universität wien

MASTERARBEIT

Titel der Masterarbeit

Integration von Risikomanagement und internen Kontrollsystem und die Anforderungen an die Integration der abbildenden Anwendungssysteme

Erstellung eines allgemein gültigen Integrationsmodells für Risikomanagement und internes Kontrollsystem sowie Ableitung der Anforderungen an die Integration unterstützenden Applikationen / Systeme

Verfasser

Kurt Berthold, BSc

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2013

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienbuchblatt:	Masterstudium Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. Dr. Erich Schikuta

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die Zitate deutlich kenntlich gemacht zu haben.

Wien, am 26. Mai 2013

Unterschrift:

_____

Kurt Berthold, BSc

Danksagung

Für die vorliegende Arbeit gilt mein Dank meinen Betreuern Univ.-Prof. Dipl.-Ing. Dr. Erich Schikuta und DDr. Alexander Hampel, Vorstand des Forschungsförderungsvereins Integration 3000 und Geschäftsführer der ADAPCON Services GmbH, für die individuelle und persönliche Betreuung im Rahmen dieser Masterarbeit.

Inhaltsverzeichnis

1 Einleitung

Durch gehobene Marktansprüche in Form von verstärkten Konkurrenzsituationen, höheren Erwartungen der Shareholder sowie komplexer werdenden Geschäftsmodellen wird es für Unternehmen immer schwieriger, Planziele zu erreichen bzw. abzusichern. Das bewusste Eingehen von Risiken und die Vermeidung von Fehlern sind in diesem Zusammenhang wichtige Faktoren für die Zielerreichung. Ein strukturiertes *Risikomanagement* ist daher ein unverzichtbares Instrument, um Wachstums- und Geschäftsziele zu erreichen. Mit dem erweiterten Ansatz des *Enterprise Risk Managements* (ERM) wird zudem die ganzheitliche Unternehmenssteuerung wahrgenommen [1, S. 328].

Das *Interne Kontrollsystem* (IKS) als ein Teil eines umfassenden ERM dient dazu, erkannte Risiken durch Kontrollen zu steuern [2, S. 31]. Interne Kontrollen sind Reaktionen auf ein identifiziertes und bewertetes Risiko. Nur durch die Integration des IKS in das Risikomanagement kann eine effektive Unternehmenssteuerung wahrgenommen werden.

In der Literatur und in vielen Unternehmen werden das Risikomanagement und IKS jedoch meistens als isolierte Systeme betrachtet.[1] Erst mit dem COSO II Framework [3, S. 502] wurde das Risikomanagement in das IKS-Modell integriert, jedoch ohne einen Kontext zwischen dem einzelnen Risiko mit einer verbundenen Kontrolle vorzusehen. Die Auswirkungen sind getrennte Einheiten in der Aufbauorganisation, isolierte Geschäftsprozesse und Artefakte sowie unterschiedliche Systeme zur Umsetzung der Risikomanagement- und IKS Prozesse. Kontrollen werden einzelnen Risiken meistens nicht oder nur intuitiv zugeordnet, da ein logisches Integrationsmodell, welches spezifische Kontrollen und Risiken miteinander verbindet, fehlt. In der vorliegenden Arbeit wird daher ein Integrationsmodell von Risikomanagement und IKS erstellt indem ein logisches Mapping zwischen einzelnen Risiken und Kontrollen vorgenommen wird.

Zur Einleitung wird in diesem Abschnitt nach der Darstellung des derzeitigen Wissens- und Forschungsstandes das Ziel der Arbeit, in Form einer kurzen Darstellung des Integrationsmodells, beschrieben. In der Folge wird die wissenschaftliche Methodik kurz dargestellt und der Aufbau der Arbeit präsentiert. Im letzten Teil dieses Abschnittes wird eine Abgrenzung zu anderen Arbeiten, welche sich mit den Themen Risikomanagement und IKS beschäftigen vorgenommen und der Mehrwert des Integrationsmodells beschrieben.

1.1 Stand des Themas, Herausforderungen

Die Hauptaufgabe eines ERM besteht darin, negative Abweichungen vom Geschäftsplan zu verhindern. Andererseits können durch eine stringente

[1] vgl. COSO I Framework, welches nur den IKS relevanten Teil darstellt [4, S. 5]

Anwendung auch Chancen wahrgenommen werden, welche das Geschäftsergebnis verbessern. Alle wesentlichen Geschäftsprozesse, die Ergebnisziele eines Unternehmens signifikant beeinflussen werden dabei in Betracht gezogen. Wo diese Wesentlichkeitsgrenze besteht ist von Unternehmen zu Unternehmen unterschiedlich.

Neben der Festlegung der Wesentlichkeiten werden die Geschäftsprozesse, welche mit Risiken behaftet sind identifiziert. Die Identifizierung wird mittels *Top-Down* oder *Bottom-Up* Ansatz [4, S. 43], [5, S. 85], welche in der Folge dargestellt werden, vorgenommen.

1.1.1 Risikoidentifikation mit dem *Top-Down* Ansatz

Beim Top-Down Ansatz geht die Initiative von der Unternehmensleitung aus indem Kontrollaktivitäten auf Unternehmensebene definiert werden [3, S. 434], [5, S. 85]. Das Top-Management bestimmt damit die Ausprägung des Risikomanagements inklusive IKS für jeden Unternehmensbereich und schafft die Möglichkeit, einer regelmäßigen Überwachung und Beurteilung

Nach [5, S. 86] ist diese Vorgangsweise besonders bei kleinen und mittleren Unternehmen vorteilhaft und kostengünstig, da die Identifikation nur durch das Top-Management durchgeführt und das Personal nicht belastet wird. Dem gegenüber sind mit dem Top-Down Ansatz bei großen Unternehmen folgende Gefahren gegeben:[2]

- Die notwendige Granularität kann aus Zeitgründen durch das Top-Management nicht gewährleistet werden.
- Es können einzelne aber wichtige Risiken in Teilbereichen übersehen werden.
- Die einseitige Vorgabe des Managements und die fehlende Involvierung des Personals erschwert das Schaffen eines Risikobewusstseins im Unternehmen.

1.1.2 Risikoidentifikation mit dem *Bottom-Up* Ansatz

Im Gegensatz zur Top-Down Vorgangsweise werden mit dem Bottom-Up Ansatz die Risiken dort identifiziert wo sie entstehen [6, S. 203], [4, S. 43]. Dies geschieht durch die Einbindung tieferer Hierarchieebenen [5, S. 85]. Risiken werden hierbei durch das Personal, welches die Prozesse ausführt, erfasst.

Nach [5, S. 86] liegt der Hauptvorteil dieser Vorgangsweise in der Schaffung des Risikobewusstseins im gesamten Unternehmen. Außerdem können die direkten

[2] vgl. [5, S. 86] – *Vor- und Nachteile einer Chancen- und Risikoidentifikation Top down vs. Bottom Up*

Erfahrungswerte des Personals genutzt werden. Als Nachteile sind folgende Punkte zu beachten:

- Hohe Kosten in der Risikoerfassung durch Einbeziehung des Personals.
- Übertriebene Detaillierung der Risiken.
- Fehlendes Gesamtbild auf Unternehmensebene durch mangelhafte Abstimmung mit der Gesamtheit an wesentlichen Geschäftsprozessen.

1.1.3 Kombination Top-Down / Bottom-Up

Bei der Kombination der beiden Ansätze werden die Vorteile beider Vorgehensweisen vereint und Nachteile kompensiert [7, S. 119]. Im ersten Schritt wird ein Risikokatalog von der Unternehmensleitung vorgegeben. Anhand des Katalogs wird das Personal zur Risikoidentifikation auf Detailebene aufgefordert. Die dafür anwendbaren Methoden sind zum Beispiel Workshops, Interviews oder schriftliche Befragungen [5, S. 87]. Abschließend werden die Risiken auf Unternehmensebene konsolidiert.

Abbildung 1 zeigt den schematischen Ansatz der Verknüpfung dieser beiden Methoden.

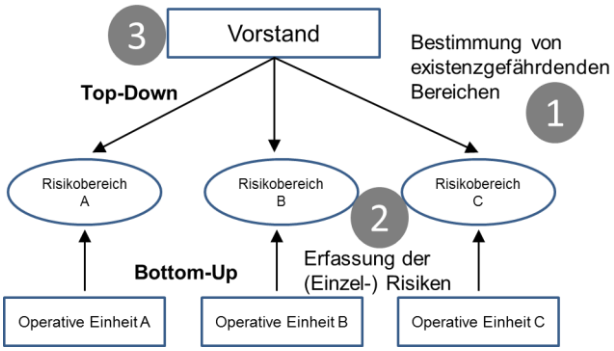

Abbildung 1: Kombinierter von Bottom-up und Top-down Ansatz [3]

1.1.4 Steuerung und Kontrolle

Kontrollen können durch Maßnahmen vorgelagert steuern oder nachgelagert kontrollieren, vermindern die Wahrscheinlichkeit von Fehlern und werden, als Reaktion auf ein Risiko, zur Steuerung von Prozessen etabliert. Es wird hierbei zwischen der Kontrolle als integrierte Maßnahme im Prozessablauf [8, S. 38] und auf Unternehmensebene [3, S. 62] unterschieden. Ein Beispiel für die Kontrolle als integrierte Maßnahme im Prozessablauf ist das vier-Augen-Prinzip bei Überweisung von größeren Geldbeträgen. Kontrollaktivitäten auf Unternehmensebene prüfen die

[3] Quelle: eigene Darstellung in Anlehnung an [63, S. 148]

Gesamtheit der Geschäftsprozesse, beispielsweise anhand von Checklisten oder Stichproben. In diesem Kontext ist auch wichtig, welche IT-Systeme für die Ausführung der Geschäftsprozesse eingesetzt werden. Die damit verbundenen Risiken und Kontrollen werden in Abschnitt vier beschrieben.

Nicht alle Risiken können mit nur einer einzigen Kontrolle gesteuert werden. In einigen Fällen sind ein Bündel an Maßnahmen und/oder Kontrollen zur Bewältigung des Risikos notwendig. Ein Beispiel dafür sind Projekte, welche eine Vielzahl an Risiken enthalten können. Bei Risiken in Projekten, wie zum Beispiel den Neubau einer Fabrik oder die Eroberung eines neuen Marktes reichen einzelne Kontrollen nicht aus. Stattdessen ist die Überwachung eines vorab definierten und bewährten Vorgehensmodells notwendig, um die angestrebten Ziele zu erreichen. Im Bereich der IT stellt beispielsweise die Ablöse einer bestehenden Software Applikation, welche wesentliche Geschäftsprozesse des Unternehmens ausführt, ein Projektrisiko dar. Abbildung 2 zeigt, welche Risiken in Projekten auftreten[4].

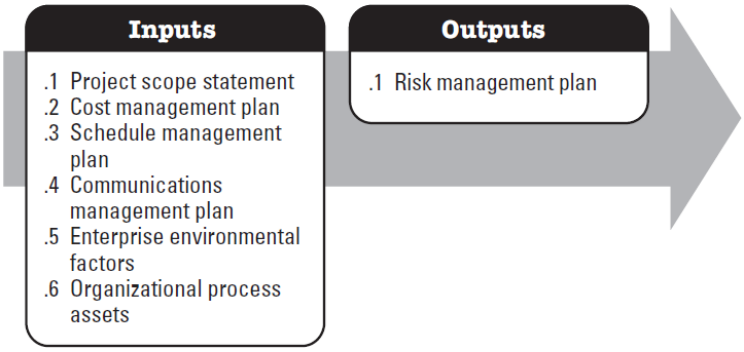

Abbildung 2: Planung von Projektrisiken[5]

Die Inputs stellen die verschiedenen Projektrisiken dar, welche einen Risikomanagementplan (Outputs), der mehrere Risiken enthält, erfordern.

Risiken in immer wiederkehrenden Prozessen werden mit Kontrollen gesteuert. Ein Prozessrisiko ist zum Beispiel Datenverlust durch eine mangelnde Durchführung von Datensicherungen.

1.1.5 Herausforderungen

Durch verschiedene Richtlinien, Standards oder Gesetzesvorgaben wie zum Beispiel Basel III [9], das GmbH-Gesetz [10] für Gesellschaften mit beschränkter Haftung (GmbH) oder das Aktiengesetz (AktG) [11] für Aktiengesellschaften (AG) sind Interne Kontroll- und Risikomanagementsysteme in den meisten Kapitalgesellschaften in verschiedensten Ausprägungen bereits vorhanden. Ein einheitliches Modell zur Durchführung im Sinne einer Handlungsanleitung wird von

[4] Beispiel von Risikomaßnahmen des *US Project Management Institute* (http://www.pmi.org/)
[5] Quelle: [81, S. 53]

der Gesetzgebung jedoch nicht vorgeschrieben. Unternehmen können die Umsetzung der Vorgaben frei gestalten. Damit verbunden ist, dass der konkrete Handlungsbedarf von Unternehmen zu Unternehmen unterschiedlich definiert und, aufgrund eines fehlenden allgemeingültigen Modells, eine einheitliche, effiziente, strukturierte und lückenlose Bearbeitung erschwert wird.

Als Basis für die Strukturierung und Vereinheitlichung stehen international anerkannte Normen und Rahmenwerke zur Verfügung. Wichtige Modelle in diesem Zusammenhang sind die Normen

- ISO/IEC 27001/02 [12], [13] für die Steuerung von IT-Risiken
- ISO/IEC 27005 [14] zur Steuerung von Risiken in der Informationssicherheit
- ISO/IEC 31000 [15] als generische Richtlinie für die Grundsätze und angemessene Umsetzung des Risikomanagement [5, S. 60]

sowie die Rahmenwerke

- COSO [4], [16], des *„Committee of Sponsoring Organizations of the Treadway Commission“* für die Strukturierung eines IKS[6]
- COBIT (*„Control Objectives for Information and related Technology“*) [17], [18] für die IT-Governance.

Diese Normen und Rahmenwerke werden im Verlauf der Arbeit näher beschrieben und stellen das Grundgerüst für das zu entwickelnde Integrationsmodell dar.

1.2 Ziel der Arbeit, Erkenntnisfortschritt

Mit der vorliegenden Arbeit werden Risikomanagement und IKS gemäß aktueller Literatur dargestellt sowie die relevanten strukturellen Aspekte der beiden Systeme erarbeitet. Mit der Beschreibung, Analyse und Kombination von Axiomen (grundlegende Gesetzesaussagen innerhalb eines Systems[7]) wird im ersten Schritt ein allgemeingültiges Integrationsmodell hergeleitet, das auch die das Risikomanagement und IKS umsetzenden IT-Systeme integriert.

Das Integrationsmodell bildet vier Ebenen wie folgt ab:

a. Risikomanagement und IKS Aufbauorganisation
b. Risikomanagement und IKS Prozesse
c. Artefakte, welche durch Risikomanagement und IKS-Prozesse erzeugt werden
d. Umsetzende Systeme, die Risikomanagement und IKS-Prozesse ausführen

[6] Die offiziellen Publikationen des COSO II Rahmenwerks setzen sich aus der Beschreibung des *Frameworks* und den *Application Techniques* zusammen
[7] vgl. http://wirtschaftslexikon.gabler.de/Archiv/1791/axiom-v7.html [Zugriff am 24.1.2013]

In der Folge wird, abgeleitet vom Integrationsmodell ein Vorgehensmodell zur Umsetzung der Integration erstellt.

Das resultierende Ziel ist die effektive Umsetzung von ERM gemäß dem Idealzustand, welcher durch das COSO-Modell [4] vorgegeben wird.

Ein weiteres wesentliches Ziel der Arbeit ist die allgemeine Definition von Anforderungen für die Integration von bestehenden IT-Applikationen und Systemen, welche die wesentlichen Risikomanagement- und IKS-Prozesse abwickeln.

Mit dem Integrationsmodell wird ein einheitliches Vorgehen bei der Implementierung und Aufrechterhaltung eines ERM, inklusive integriertem IKS, aufgezeigt. Der Mehrwert dieses Ansatzes ist, dass Risiken und Kontrollen in einer logischen Form definiert und zusammengeführt werden. Damit wird eine einheitliche, integrative und risikoorientiere Unternehmensteuerung ermöglicht.

Zur praktischen Evaluierung wird das Modell fünf erfahrenen Personen präsentiert und anschließend Interviews geführt. Die Personen, welche interviewt werden, kommen aus den Bereichen der Wirtschaftsprüfung, der Privatwirtschaft sowie öffentlicher Bereich. Diese unterschiedlichen Sichtweisen geben wertvolle Aufschlüsse über die korrekte Erstellung des Integrationsmodells.

1.3 Methodik

Für die Darstellung der Integration von Risikomanagement und IKS wird die Methode der Modellbildung angewandt. Modelle haben sich in der Softwareentwicklung bewährt und eignen sich sehr gut für die Darstellung komplexer Strukturen [19, S. 132] und somit auch für das Integrationsmodell.

Die Modellbildung, als iterativer Prozess zur Erstellung des Integrationsmodells ist von zwei grundlegenden Komponenten abhängig:

- **Fachwissen der Domäne Risikomanagement und IKS** das sich aus gesetzlichen Vorgaben, anerkannten Methoden und Rahmenwerken sowie spezifischen Risiken im Unternehmen zusammensetzt.
- **Methoden der Modellierung** in Bezug auf die Darstellung eines abstrakten Modells zur Vereinfachung der Komplexität als Grafik und textueller Beschreibung der Zusammenhänge.

Die Erstellung der Modelle wird mit der Unified Modeling Language (UML) als semantisches Klassendiagramm realisiert.

Mit der Bildung des Integrationsmodells werden gleichzeitig die Systemgrenzen definiert und eine Wechselwirkung mit der so genannten Außenwelt dargestellt. Das fertige Modell stellt eine Anregung für zukünftige Arbeiten dar, dieses weiter zu entwickeln bzw. zu optimieren.

Bei der Evaluierung des Integrationsmodells wird ein Falsifikationsversuch nach dem kritischen Rationalismus vorgenommen. Der kritische Rationalismus basiert auf Theorien von Sir Karl Popper [20] und geht davon aus, dass das menschliche Wissen fehlbar ist. Bestätigungen einer Theorie sind deshalb nicht der richtige Weg zur Gewinnung von neuen Erkenntnissen sondern vielmehr Beobachtungen mit denen sie falsifiziert oder widerlegt werden können. Eine ausführlichere Darstellung des kritischen Rationalismus wird in Abschnitt zwei dargestellt.

Das in dieser Arbeit erstellte Integrations- und Vorgehensmodell ist beobachtbar und kann jederzeit, zum Beispiel durch Erfahrung, widerlegt werden. Die Erfahrung der zu interviewenden Personen wird daher einen guten Aufschluss über die Korrektheit des Modells wiedergeben.

1.4 Aufbau der Arbeit

Nach der Einleitung werden in Abschnitt zwei die Vorgangsweise zur Erstellung der Arbeit sowie die angewandten wissenschaftlichen Methoden beschrieben.

Um die Modellierung vornehmen zu können werden in Abschnitt drei alle, für das Integrationsmodell relevanten Begriffe aus folgenden Bereichen erörtert:

- Enterprise Risk Management (ERM)
- Internes Kontrollsystem (IKS)
- Governance inklusive IT-Governance sowie
- Compliance

Abschnitt vier zeigt eine Darstellung der für Risikomanagement und IKS verbindlichen gesetzlichen Vorgaben sowie anerkannten Rahmenwerke und Normen, die ebenfalls für die Modellbildung herangezogen werden.

In Abschnitt fünf wird anhand der vorher ausgeführten theoretischen Punkte das Integrationsmodell für Risikomanagement und IKS präsentiert. Zudem wird in diesem Abschnitt auch das Vorgehensmodell zur Umsetzung der Integration dargestellt.

Vor der Zusammenfassung erfolgt in Abschnitt Sechs die Beschreibung und Analyse der Interviews mit erfahrenen Personen zur Evaluierung der Modelle.

1.5 Abgrenzung und Mehrwert

Mit dem *Enterprise Risk Management Framework COSO II* wurde 2004 ein Modell entwickelt, das eine Integration von Risikomanagementsystem und IKS vorsieht [3, S. 50]. Obwohl das Modell, welches in Abschnitt vier dargestellt ist, auch konkrete Handlungsanweisungen vorsieht fehlt jedoch der Kontext zwischen einzelnen konkreten Risiken und verbundenen Kontrollen. Bei den Kontrollaktivitäten werden

beispielsweise nur die Kontrollarten genannt ohne auf die logische Verbindung zu identifizierten Risiken einzugehen [21, S. 61-66].

Der primäre Mehrwert der vorliegenden Arbeit ist die Entwicklung eines Modells zur direkten Integration von Risikomanagement und IKS. Das resultierende Integrationsmodell ist die Basis für ein, ebenfalls in dieser Arbeit erstelltes Vorgehensmodell zur Umsetzung der Integration. Um der Ausführung von Risikomanagement und IKS Aufgaben durch IT-Systeme Rechnung zu tragen werden zudem die umsetzenden Anwendungen für Risikomanagement und IKS im Integrations- und Vorgehensmodell eingegliedert.

Das Integrationsmodell berücksichtigt unterschiedliche Bereiche und bietet folgende zusätzliche Mehrwerte:

- **Auf Organisationsebene** werden Risikomanagement und IKS-Rollen direkt miteinander verknüpft.
- **Auf Prozessebene** werden durch IKS-Prozesse konkrete Risiken mittels Mapping zwischen Risiken und Kontrollen gesteuert.
- **Artefakte** aus beiden Bereichen werden miteinander in Verbindung gebracht.
- **Umsetzende IT-Systeme** für Risikomanagement und IKS werden integriert.
- **Das Vorgehensmodell** zeigt die konkrete Umsetzung des Integrationsmodells, um den nach COSO vorgegebenen Idealzustand in der operationellen Umsetzung zu erreichen.

Der allgemeine Anspruch der Modelle ist, die Komplexität, welche sich durch die getrennte Betrachtung der beiden Welten ergeben, zu reduzieren und gleichzeitig eine ausgewogene Abstimmung von Risiken und Kontrollen zu gewährleisten.

2 Vorgangsweise und Methodik

Die Erstellung des Integrationsmodells für Risikomanagement und IKS erfolgt in vier Phasen, welche in der Folge dargestellt werden. Abbildung 3 zeigt die Vorgangsweise anhand eines Phasenmodells:

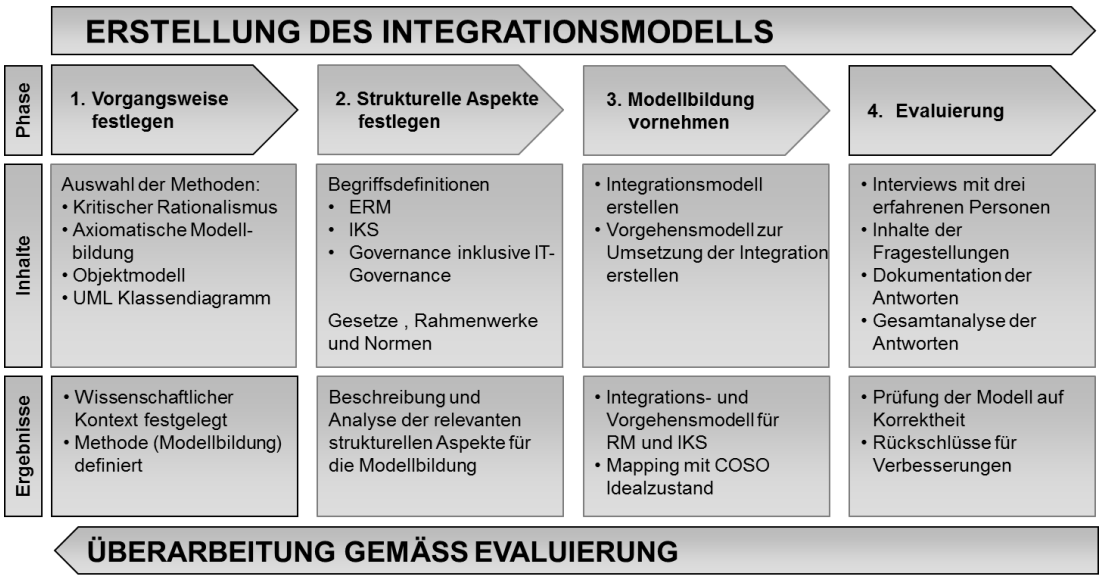

Abbildung 3: Phasen zur Erstellung des Integrationsmodells[8]

Zu Beginn wird die allgemeine Vorgangweise definiert indem wissenschaftliche Methoden ausgewählt und beschrieben werden. In der zweiten Phase werden sämtliche strukturellen Aspekte von Risikomanagement und IKS erarbeitet, um Begrifflichkeiten einzugrenzen, gesetzliche Vorgaben zu erkennen sowie anhand von anerkannten Rahmenwerken Aufschlüsse für die Modellbildung zu erhalten. In der dritten Phase erfolgen die eigentliche Modellbildung inklusive Beschreibung aller Elemente und deren Zusammenhänge. Die vierte Phase dient der Evaluierung der Modelle. Die Ergebnisse dieser Phase werden in der Zusammenfassung der Arbeit als Bestätigung oder Verbesserungsmaßnahmen eingebracht.

2.1 Kritischer Rationalismus

Der *Kritische Rationalismus* [20], [22] ist eine Wissenstheorie, die davon ausgeht, dass Theorien nicht bewiesen sondern nur widerlegt und so weiterentwickelt werden können. Das Wort *Kritisch* weist auf die Widerlegbarkeit von Theorien hin. *Rational* bedeutet in diesem Zusammenhang, dass logische Regeln zur Widerlegung angewandt werden.

[8] Quelle: eigene Darstellung

Wissenschaftliche Aussagen können demnach nicht hundertprozentig abgesichert oder *verifiziert* werden. Im Gegensatz dazu werden nur Theorien anerkannt, die widerleg- oder *falsifizierbar* sind.

Gemäß kritischem Rationalismus ist die Falsifikation daher das zentrale Merkmal jeder wissenschaftlichen Aussage. Misslingt die Falsifizierung hat sich die wissenschaftliche Theorie vorerst bewährt, da kein Fehler gefunden werden konnte. Bei erfolgreicher Falsifikation wird die bisherige Aussage verworfen.

In diesem Kontext und für die Erstellung der Modelle ist zudem das Induktionsproblem [23] von Bedeutung. Bei der Recherche und Erarbeitung der strukturellen Aspekte des Risikomanagements und IKS wurden einzelne Gesetzmäßigkeiten als Basis für das Integrationsmodell definiert. Darauf aufbauend wurde das Modell erstellt indem induktiv aus einer Reihe an Gegebenheiten auf das Gesamtmodell geschlossen wurde. Nach Sir Karl Popper und David Hume kann dieser Rückschluss jedoch nicht verifiziert werden. Es ist somit sehr wahrscheinlich, dass das Modell teilweise oder in seiner Gesamtheit widerlegt werden kann.

2.2 Axiomatische Modellbildung

In der Literatur existieren keine einheitlichen Aussagen, wie ein unternehmerisches Risiko formuliert, gesteuert und überwacht werden muss. Auch die spezifischen gesetzlichen Vorgaben, wie etwa der Sarbanes Oxley Act (SOX) [24] in den USA oder das Unternehmensrechtsänderungsgesetz [25] in Österreich enthalten hierzu keine Handlungsanweisungen. Es bleibt daher den Unternehmen selbst überlassen, welchen Stellenwert dem Risikomanagement und IKS eingeräumt wird. Ein allgemeingültiges Modell stellt die fehlende Handlungsanweisung her.

Axiome unterstützen die Modellbildung, da allgemein anerkannte und bewährte Methoden zur Anwendung kommen. Allerdings sind auch diese Axiome jeweils auch auf Ihre Gültigkeit zu hinterfragen und darauf zu achten, dass diese im Modell sinnvoll kombiniert werden.

Das Integrationsmodell kombiniert bestehende relevante Axiome zu einem ganzheitlichen System mit dem Vorteil, dass eine vereinheitlichte Vorgangsweise für jedes Unternehmen, unabhängig von Branche, Größe oder Komplexität für das Steuern von Risiken gewählt werden kann. Der Erkenntnisgewinn ist, dass jedes Unternehmen das Modell anwenden und auch die einzelnen Axiome im Sinne einer Anwendbarkeit in Frage stellen kann.

2.3 Semantisches Objektmodell

Das *Semantische Objektmodell (SOM)* stellt nach [26] eine Methodik zur Modellierung betrieblicher Systeme dar. Als betriebliche Systeme sind in diesem Zusammenhang Unternehmen, Unternehmensverbunde oder Geschäftsbereiche von Unternehmen zu verstehen [26, S. 3]. Im Integrationsmodell werden die

Geschäftsbereiche des Risikomanagements und IKS dargestellt. Abbildung 4 zeigt die allgemeine Form des SOM.

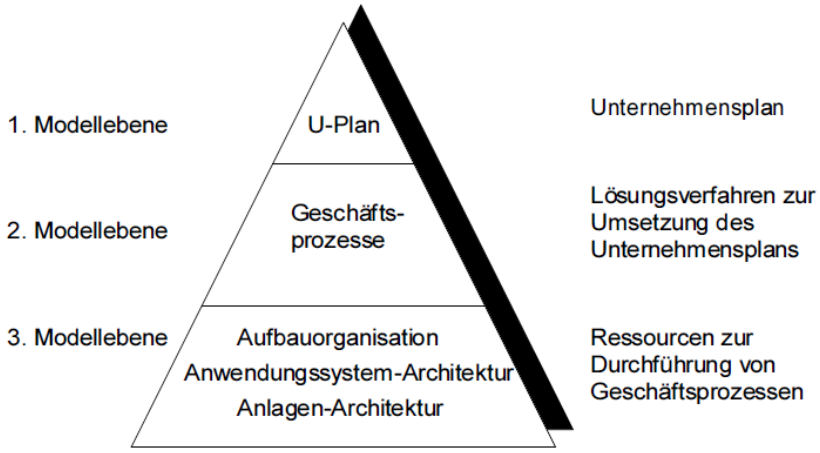

Abbildung 4: Darstellung der Unternehmensarchitektur mit dem SOM[9]

Das SOM besteht aus drei Ebenen, welche die Unternehmensarchitektur repräsentieren und in der Folge kurz beschrieben werden.

2.3.1 Erste Modellebene

Der Unternehmensplan stellt das Ergebnis der betriebswirtschaftlichen Unternehmensplanung dar. Hier wird unter anderem die Risikobereitschaft festgelegt sowie Stärken und Schwächen ermittelt. Die notwendigen Ressourcen für Risikosteuerung und interne Kontrollen werden festgelegt.

2.3.2 Zweite Modellebene

Auf dieser Ebene werden interne Geschäftsprozesse modelliert, welche den Unternehmensplan umsetzen. Die Lenkung der Prozesse im Sinne einer Überwachung und Steuerung wird definiert. Im Integrationsmodell werden hier die relevanten Risikomanagement und IKS Prozesse dargestellt.

2.3.3 Dritte Modellebene

Zu den in dieser Ebene dargestellten Ressourcen zählen das Personal und Systeme oder Anlagen. Die fachlichen Anforderungen an die Ressourcen und deren Integration in die gesamte Unternehmensarchitektur werden durch die in der darüber liegenden Ebene des Prozessmodells definiert. Jede Ressource nimmt bestimmte Aufgaben innerhalb des Systems wahr. Die Beziehungen zwischen den

[9] Quelle: [26, S. 8]

Prozessen werden dargestellt. Im Integrationsmodell werden in dieser Ebene Rollen und ausführende IT-Systeme modelliert.

2.3.4 Zusätzliche Modellebene

Für die Erstellung des Integrationsmodells ist, nach den Erfahrungen des Autors dieser Arbeit eine zusätzliche Ebene, welche die durch das Risikomanagement und IKS erstellten Artefakte enthält, vorzusehen. Als Artefakte werden in diesem Kontext die Ergebnisse der Risikomanagement und IKS Prozesse bezeichnet. Diese werden im Wesentlichen durch elektronische Dokumente in unterschiedlichen Formen repräsentiert.

2.4 Vorgehensmodell

Im Zuge der Gesetzeserlassung des *Sarbanes Oxley Acts* [24] in USA wurde auch ein eigenes behördliches Aufsichtsgremium für Wirtschaftsprüfer, das *Public Accounting Oversight Board (PCAOB)*[10] neu etabliert. Das PCAOB sowie die US-Börsenaufsichtsbehörde *Security and Exchange Commission (SEC)*[11] geben nach [27, S. 39] eine nachhaltige Empfehlung zur Etablierung des COSO [4], [16] Rahmenmodells zur Integration von Risikomanagement und IKS ab.

Der in COSO II erweiterte und integrative Ansatz des Enterprise Risk Management gibt demnach den Rahmen für das Integrationsmodell vor und wird deshalb als Vorgehensmodell für die Umsetzung der Integration gewählt.

Die Inhalte, Aufbau und Struktur von COSO I und COSO II werden in Abschnitt vier dargestellt.

[10] http://www.pcaobus.org [Zugriff am 24.1.2013]
[11] http://www.sec-oig.gov [Zugriff am 24.1.2013]

3 Begriffsdefinitionen

Für die Entwicklung des Integrationsmodells müssen auf der Detailebene eine Reihe von Einflussfaktoren und Begriffen berücksichtigt werden. In diesem Abschnitt wird auf diese näher eingegangen.

In diesem Zusammenhang ist das Zusammenwirken von *Governance*, *Risk* und *Compliance* von Bedeutung. Abbildung 5 zeigt die Beziehungen der genannten Bereiche untereinander in grafischer Form.

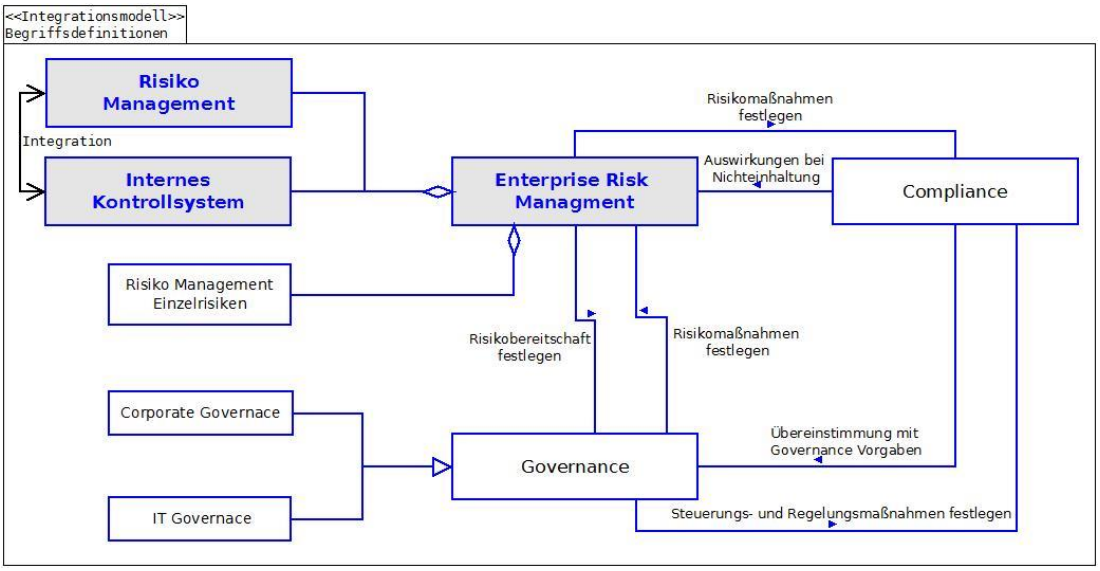

Abbildung 5: Zusammenwirken der relevanten Begriffe[12]

Der zentrale Ausgangspunkt der Integrationsüberlegungen ist das *Enterprise Risk Management*, durch welches die Bereiche des *Risikomanagements* und *Internen Kontrollsystems* integriert werden. Die Ausprägung des Enterprise Risk Managements ist von *Governance* und *Compliance* Vorgaben abhängig, welche auf das Interne Kontrollsystem wirken. Das Management der Einzelrisiken wird in der Klasse Enterprise Risk Management aggregiert. Aus dem Begriff *Governance* leiten sich die Teilbereiche der *Corporate* und *IT-Governance* ab.

3.1 Enterprise Risk Management (ERM)

In diesem Abschnitt wird aus den Begriffen *Risiko* und *Risikomanagement* die Definition des *Enterprise Risk Management (ERM)* hergeleitet.

[12] In Anlehnung an [82]

3.2 Der Risikobegriff

Der Risikobegriff wird in der Literatur unterschiedlich definiert [6, S. 1]. Der Duden beschreibt zum Beispiel ein Risiko allgemein als

> *„einen möglichen negativen Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust oder Schäden verbunden sind“*[13]

Zur Eingrenzung des Begriffs auf betriebswirtschaftliche Aspekte werden im Verlauf dieser Arbeit nur Risiken, welche in Unternehmen zum Tragen kommen betrachtet. In diesem Kontext wird nach [5, S. 29] das „*Corporate Risk Management*“ wie folgt definiert:

> *„Risiko ist die Gefahr (bzw. die Chance) einer negativen (bzw. positiven) Abweichung von den Unternehmenszielen.“*

Aus dieser Definition kann abgeleitet werden, dass ein Geschäftsplan existiert und das Risiko darin besteht, diesen Plan nicht zu erfüllen. Die Erreichung von Unternehmenszielen ist mit einer Vielzahl an Aktivitäten, welche risikobehaftet sein können, verbunden. In der Folge werden einige Beispiele dieser Einzelrisiken angeführt:[14]

- Personalrisiken: alle Risiken, welche mit der Beschäftigung von Mitarbeiter/Innen verbunden sind wie zum Beispiel Ausfall von Schlüsselpersonen, Krankheit oder auch Betrug.
- Politische Risiken: treten zum Beispiel bei Änderung von Gesetzen ein, die Nachteile für ein Unternehmen bedeuten.
- Währungsrisiko: dazu zählen alle Risiken oder Chancen, welche mit Währungsschwankungen zu tun haben.
- Kredit- oder Ausfallsrisiko: Risiken, welche allgemein durch Zahlungsausfall verursacht werden.
- IT-Risiken: alle Risiken, die mit dem Betrieb und der Anschaffung von IT-Systemen verbunden sind.

Die Definition des Risikobegriffs beinhaltet auch das Wahrnehmen von Chancen. Risiken und Chancen sind unmittelbar miteinander verbunden. Eine nicht wahrgenommene Chance stellt demnach auch ein Risiko dar. Im weiteren Verlauf der Arbeit wird der Terminus *Chance* jedoch nicht weiter betrachtet, sondern ausschließlich Risiken im Sinne eines Schadenseintritts.

[13] Siehe Begriffsdefinition nach [93]
[14] In Anlehnung an eine umfassende Darstellung von Einzelrisiken in [3, S. 164-313]

3.3 Risikomanagement - Einzelrisiken

In diesem Abschnitt wird das Risikomanagement im Sinne der Steuerung von Einzelrisiken in Form des Risikomanagementprozesses und der Unterscheidung zwischen operationellen und strategischen Risiken dargestellt. Der in Abbildung 5 dargestellte Kontext zum ERM wird hierbei vorerst noch nicht betrachtet.

3.3.1 Risikomanagementprozess

Der Risikomanagementprozess wird nach [28, S. 267-268] in vier Stufen wie folgt untergliedert:

a. Risikoidentifikation in Form einer Analyse der unternehmensspezifischen Risiken.
b. Risikobewertung durch die Entscheidung ob Maßnahmen im Hinblick auf die Verminderung des Risikos eingeleitet werden.
c. Risikosteuerung durch konkrete Maßnahmen, welche eine Vermeidung, Reduktion oder Tragung des Risikos vorsehen.
d. Erfolgskontrolle zur Überprüfung ob die angewandten Methoden zur Zielerreichung geführt haben.

Abbildung 6 zeigt den Risikomanagementprozess in grafischer Form.

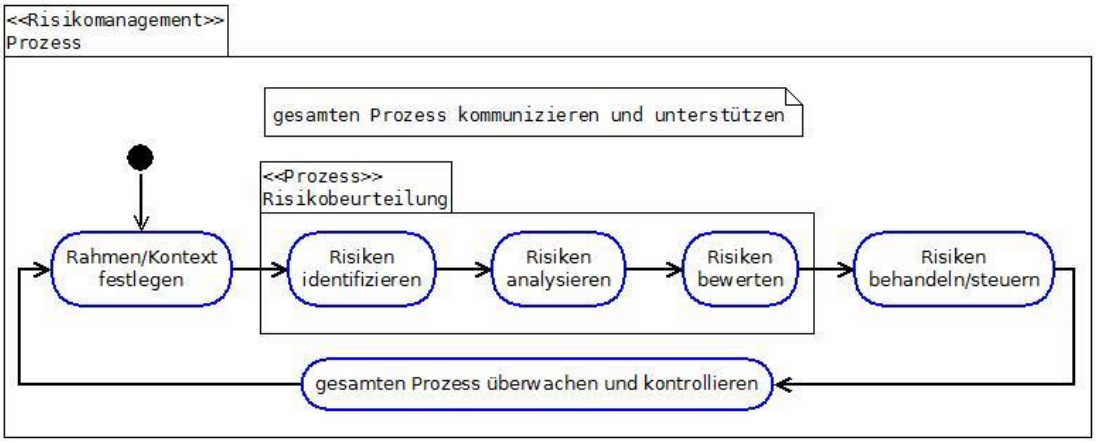

Abbildung 6: Risikomanagementprozess[15]

Diese Darstellung zeigt, dass die Bereiche *Risikomanagement* und *IKS* im Falle einer Integration zusammenfallen indem der gesamte Risikomanagementprozess überwacht und kontrolliert wird.

[15] Quelle: eigene Darstellung in Anlehnung an ISO 31000:2009 [15, S. vii], eine detailliertere Sichtweise bietet der Risikomanagementprozess nach der ISO/IEC 27005:2008 Norm, welche in Abschnitt 4.3.2 dargestellt wird

Der Risikomanagementprozess zeigt das generische Vorgehen zur Steuerung von Risiken, ohne jedoch auf konkrete Steuerungsmaßnahmen einzugehen. Die generelle Ausführung des Prozesses ist immer gleich[16], unabhängig davon ob es sich bei der Risikoart um operationelle und strategische Risiken, welche in den folgenden beiden Abschnitten dargestellt werden, handelt.

3.3.2 Operationelles Risiko

Das operationelle Risikomanagement wird hauptsächlich vom mittleren Management eines Unternehmens getragen. Eine nach [29, S. 9] lautende Definition beschreibt das operationelle Risiko wie folgt:[17]

> *„Das operationelle Risiko ist definiert als die Gefahr von Verlusten infolge unzulänglicher oder fehlgeschlagener interner Prozesse, Systeme oder Menschen sowie von externen Ereignissen. Diese Definition beinhaltet das Rechtsrisiko, schließt aber strategisches -und Reputationsrisiko aus."*

Demzufolge werden mögliche Schäden im betrieblichen Umfeld betrachtet. Das Risiko betrifft hier die Abweichung vom Geschäftsplan durch die Verfehlung von Prozesszielen oder mangelnde Effektivität von etablierten Geschäftsprozessen. Die Definition schließt auch externe Ereignisse ein, welche auf ein Unternehmen einwirken. Nach [29, S. 94] zählen zu den wesentlichen extern bedingten Risiken

- externe Kriminalität in Form von Betrug, Raub, Diebstahl oder ähnlichen,
- Elementarereignisse wie zum Beispiel ein großräumiger Ausfall der Strom oder Telekommunikationsversorgung [29, S. 65],
- Naturkatastrophen sowie
- Terror, Krieg oder politische Risiken.

Im Vordergrund stehen die Risiken aller wichtigen Produkte, Tätigkeiten, Verfahren und Systeme.[18] Das impliziert die Überwachung und kontinuierliche Verbesserung von immer wiederkehrenden Geschäftsprozessen, welche mit Risiken behaftet sind.

Die Ausrichtung der IT an den Bedürfnissen der Kunden[19] ist einer der Teilbereiche des operationellen Risikomanagements. Diese umfasst die Erhebung des Servicebedarfs sowie die Etablierung eines Prozesses für das Anforderungsmanagement zur Auswahl der geeigneten Services. Das Management der Informationssicherheit[20] im Kontext mit der Vertraulichkeit, Verfügbarkeit, und Integrität von Daten und Informationen ist ein Teilbereich des operationellen IT-

[16] Gemäß der Rahmenfestlegung in der ISO 31000:2009 [15, S. 1]
[17] Eine ähnliche Definition ist auch in [52, S. 2] und [50, S. 163] zu finden.
[18] In Anlehnung an den Grundsatz 4 in [52, S. 4] .
[19] Gemäß ITIL *Service Strategie Phase* [88]
[20] Siehe [13, S. 1]

Risikomanagements. Die anerkannte ISO Norm 27001:2005 gibt hierbei den Prozessansatz für das Management der Informationssicherheit vor [12, S. 5].

Das Eintreten eines operationellen Risikos ist mit Verlusten verbunden. Abbildung 7 zeigt die logischen Ausprägungen der Häufigkeit von Verlusten an.

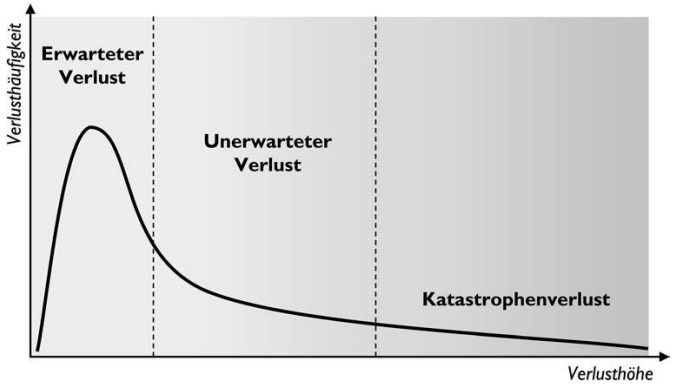

Abbildung 7: Typische Verteilung operationeller Verlustfälle[21]

Erwartete sind mit kalkulierbaren Verlusten gleichzusetzen und müssen bei der Unternehmensplanung berücksichtigt werden. Die vergleichsweise geringe Verlusthöhe ergibt sich durch die Einleitung von geeigneten Gegenmaßnahmen, welche die Schadenhöhe minimieren. Die Kurve bewegt sich in Richtung unerwartete und Katastrophenverluste sehr stak nach unten. Der Grund dafür ist, dass Kontrollschritte in Geschäftsprozessen das Risiko minimieren und ein Schadenseintritt nur in Ausnahmensituationen, wie zum Beispiel externen Ereignissen, vorkommt.

3.3.3 Strategisches Risiko

Die wesentlichen Zielsetzungen des strategischen Risikomanagements sind die Nachhaltigkeit und Überlebensfähigkeit eines Unternehmens [5, S. 160]. Um das zu erreichen werden daher langfristige Veränderungen, welche sich negativ auf das Unternehmen auswirken, minimiert oder verhindert. Im Folgenden werden einige Beispiele des strategischen Risikomanagements beschrieben.

Langfristige Fähigkeit zur Risikoübernahme in finanzieller Hinsicht

Nach [5, S. 159] treten größere Veränderungen nur über längere Zeiträume auf. Das Risiko besteht hier darin, die Veränderung korrekt zu antizipieren und richtige Entscheidungen im Hinblick auf eine finanzielle Absicherung zu treffen. Beispiele dafür sind etwa die Übernahme von Mitbewerbern oder die Investition in Forschung

[21] Quelle: [29, S. 15]

und Entwicklung. Nach den Einschätzungen des Autors werden Entscheidungen in diesem Zusammenhang im Rahmen des Strategieprozesses getroffen.[22]

Innovationsrisiko

Der Innovationsprozess geht meistens über einen längeren Zeitraum. Nach [30, S. 101] setzt sich hierbei das Gesamtrisiko aus folgenden Risikoarten zusammen:

- Technisches Risiko: basiert auf der Unsicherheit hinsichtlich des Ergebnisses des Entwicklungsvorhabens
- Zeitrisiko: entsteht durch die Überschreitung des geplanten Zeitraumes der Entwicklung
- Kostenrisiko: betrifft die Überschreitung der geplanten Kosten
- Verwertungsrisiko: beschreibt Risiken, die mit der Markteinführung der Entwicklung in Zusammenhang stehen

Bei etablierten Technologien stellt die Einschätzung der absetzbaren Kapazitäten am Markt ein Risiko dar.

Marktrisiken

Große Unternehmen agieren häufig auf internationalen Märkten mit unterschiedlichen Gesetzmäßigkeiten. Der Eintritt in einen neuen Markt ist immer mit Investitionen verbunden, welche hier das Risiko darstellen. Die Strategie, einen neuen Markt zu erobern ist nicht immer gleich, da etwa lokale Anbieter oder politische Umstände eine große Rolle spielen können.

Die präsentierten Beispiele implizieren, dass strategische Risiken von der Unternehmensführung getragen werden müssen, da langfristige Planungszyklen notwendig sind, welche die Existenzsicherung des Unternehmens sichern sollen. Langfristige Planungen sind ohne die Abschätzung von Risiken nicht möglich, da die Marktentwicklungen über einige Jahre in den meisten Fällen nicht exakt vorhersehbar ist. Eine konsequente Identifikation, Bewertung und Steuerung von strategischen Risiken ist zwar keine gänzliche Absicherung für nachhaltigen Geschäftserfolg, erhöht aber die Wahrscheinlichkeit der Verbesserung des Unternehmenswertes.

3.4 Enterprise Risk Management (ERM)

In Abbildung 5 ist die Beziehung von Einzelrisiken und ERM in Form einer Aggregation dargestellt. Diese Beziehung zeigt, dass bei der isolierten Betrachtung von Einzelrisiken immer der Kontext zum gesamten Risikoportfolio eines Unternehmens hergestellt wird. Das ERM umfasst daher das unternehmensweite Risikomanagement und unterstützt durch eine risikoorientierte Steuerung, die

[22] vgl. die Ausführungen in [4, S. 3] und [16, S. 4]

Erreichung der geplanten Unternehmensziele. Nach [21, S. 4], [3, S. 464] wird ein ERM wie folgt definiert:

> *„ERM ist ein Prozess, ausgeführt durch Überwachungs- und Leitungsorgane, Führungskräfte und Mitarbeiter einer Organisation, angewendet bei der Strategiefestlegung und innerhalb der Gesamtorganisation, gestaltet, um die Organisation beeinflussende mögliche Ereignisse zu erkennen und um hinreichende Sicherheit bezüglich des Erreichens der Ziele der Organisation zu gewährleisten."*

Gemäß dieser Definition ist das Schadensausmaß, welches sich durch die Summe aller Risiken ergibt zu minimieren bzw. die Gesamtheit an Chancen, welche sich ergeben, wahrzunehmen. Allgemein betrachtet stellt das ERM einen Rahmen für einen Prozess, der sich ununterbrochen über die gesamte Organisation erstreckt, dar und zur Erkennung von möglichen Ereignissen – die im Falle ihres Eintretens die Organisation beeinflussen – dient [31, S. 2].

Die zentralen Elemente des ERM sind daher [32, S. 1], [5, S. 34]

- das Management aller betrieblichen Risiken,
- die Integration des Risikomanagements in die Unternehmenssteuerung durch Integration von Risikozielen in die Unternehmensziele sowie
- die Berücksichtigung von Risikointerdependenzen durch Bewertung von wechselseitig abhängigen Risiken und Umsetzung von dafür geeigneten Maßnahmen.

Das Interne Kontrollsystem, welches im nächsten Abschnitt dargestellt wird, ist ein integraler Bestandteil unternehmensweiten Risikomanagements.[23]

3.5 Internes Kontrollsystem (IKS)

Unter einem *Internen Kontrollsystem* (IKS) ist nach [33, S. 7] folgendes zu verstehen:

> *„die vom Management eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen), die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements*
> - *zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),*
> - *zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie zur*

[23] vgl. [31, S. 6]

- *Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften.“*

Diese Definition kommt aus dem Bereich der Rechnungslegung in Form der Finanzberichterstattung und umfasst auch alle anderen Unternehmensbereiche. Darüber hinaus werden jedoch auch alle anderen wesentlichen Geschäftsprozesse, auch wenn diese nicht die Finanzberichterstattung betreffen, betrachtet [3, S. 24].

Die Bestandteile des IKS sind die Regelungen zur Steuerung der Unternehmensaktivitäten sowie Regelungen zu Überwachung der Einhaltung dieser Regelungen [3, S. 24], [33, S. 7]. Abbildung 8 zeigt den IKS-Aufbau in grafischer Form.

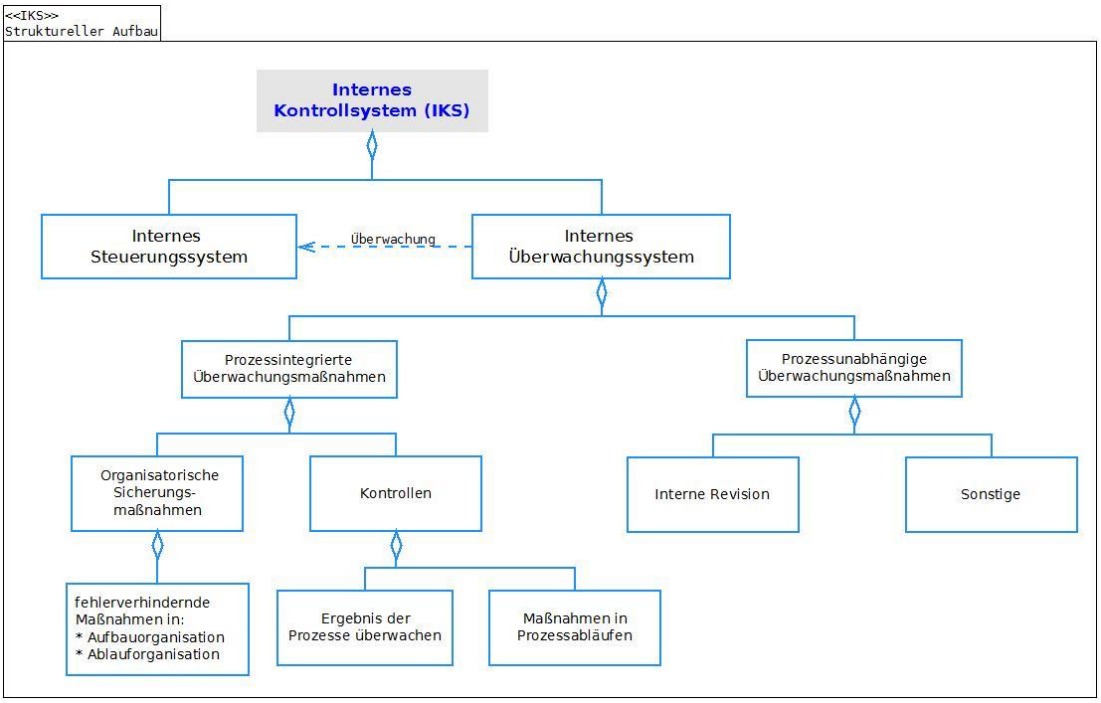

Abbildung 8: IKS-Struktur[24]

Das Modell in Abbildung 8 unterscheidet im Bereich des internen Überwachungssystems zwischen prozessintegrierten und prozessunabhängigen Maßnahmen zur Überwachung. Demnach wird unterschieden ob Kontrollen integraler Bestandteil eines Geschäftsprozesses sind oder unabhängig als Steuerungsmaßnahmen umgesetzt werden.

Unter den fehlerverhindernden Maßnahmen im Bereich der organisatorischen Sicherheitsmaßnahmen sind alle Aktivitäten zu verstehen, welche ein bestimmtes Sicherheitsniveau gewährleisten [3, S. 25], [33, S. 7]. Diese Maßnahmen betreffen entweder

[24] Quelle: eigene Darstellung in Anlehnung an [3, S. 24], [33, S. 8]

- die Aufbauorganisation im Sinne von zum Beispiel Funktionstrennungen oder
- die Ablauforganisation, zum Beispiel in Form von Zugriffs- oder Zutrittsberechtigungen zu IT-Systemen oder Räumlichkeiten

Kontrollen sind entweder durch Kontrollschritte in Prozessen oder die Überwachung von Prozesszielen geprägt. Zur Überwachung von Prozesszielen wird eine bestimmte Anzahl von mehrfach ablaufenden Prozessen beobachtet und zum Beispiel die Fehlerhäufigkeit in bestimmten Prozessschritten festgestellt. Die Verfehlung des Prozessziels führt zur Einleitung von Verbesserungsmaßnahmen.

Die Interne Revision agiert vollkommen unabhängig von jeglichen Prozessen. Nach [27, S. 19] gehört zu ihrem Arbeitsumfang auch die Prüfung und Beurteilung der Effizienz und Effektivität des IKS.

Zur Überwachung des Reifegrades eines IKS kann nach [3, S. 436] das Modell der *Capability Maturity Model Integration (CMMI)*[25] herangezogen werden. Abbildung 9 zeigt die verschiedenen Reifegrade.

Stufe	Ausprägung	Merkmale
5	Optimiert	* Ausgeprägtes Kontrollbewusstsein im ganzen Unternehmen * Weitgehende Automatisierung der Kontrollaktivitäten * Hohe Reaktionsfähigkeit auf Veränderungen durch Werkzeuge * Integriertes IKS, Revisions- und Risikomanagementsystem
4	Überwacht	* IKS Grundsätze und Richtlinien sind detailliert dokumentiert * Regelmäßige Überwachung der Kontrollen * Laufende Aktualisierung der Kontrollen * Regelmäßig IKS-Berichterstattung
3	Definiert	* IKS Grundsätze und Richtlinien sind dokumentiert * Kontrollen sind in den Prozessen integriert und dokumentiert * Nachvollziehbarkeit der Kontrollen ist gegeben * Information, Kommunikation und Schulung existieren
2	Wiederholbar	* Interne Kontrollen sind vorhanden aber nicht standardisiert * Fehlende Nachvollziehbarkeit der Kontrollen * Kontrollen sind personenabhängig und nicht dokumentiert * Fehlende Information, Kommunikation und Schulung
1	Initial	* Unstrukturiertes Kontrollumfeld im Unternehmen * Interne Kontrollen sind kaum oder nicht vorhanden * Vorhandene Kontrollaktivitäten werden fallweise ausgeführt * Vorhandene Kontrollen sind nicht verlässlich

Abbildung 9: Reifegrade eines IKS[26]

Die einzelnen Stufen des Modells bauen aufeinander auf. Die höher liegenden Stufen enthalten deshalb immer alle Eigenschaften der unteren Ebenen.

[25] Siehe Einzelheiten für das CMMI des Software Engineering Institute (SEI) [83]
[26] Quelle: eigene Darstellung in Anlehnung an [3, S. 437]

3.6 Governance

Für den englischen Begriff *Governance* existieren unterschiedliche Übersetzungen bzw. Herleitungen. Meistens wird das Wort aus dem englischen *govern (regieren)* abgeleitet oder, im Sinne der Unternehmensführung mit dem deutschen Begriff *Steuerung* übersetzt. Eine eindeutige Übersetzung ist in der Literatur jedoch nicht vorhanden. Bei der Verwendung des Begriffs ist daher eine kontextbezogene Präzisierung notwendig [34, S. 33], welche in den nächsten beiden Abschnitten mit den Themengebieten der *Corporate und IT-Governance* vorgenommen wird.

3.6.1 Corporate Governance

Die *Grundsätze für die Unternehmensführung* werden im Sprachgebrauch und in der Literatur mit dem englischen Begriff *Corporate Governance* vereinheitlicht bzw. übersetzt. Nach [35, S. 243] umfasst die Corporate Governance

> *„die grundsätzlichen Ausgestaltungen sowie die speziellen Rahmenbedingungen für die Strukturen und für die Prozesse der Führung, Verwaltung und Überwachung von Unternehmen“*

Diese Definition impliziert einen generellen Ordnungsrahmen für die Führung und Überwachung von Unternehmen sowie interne Kontrollen und hat außerdem einen starken Einfluss auf das Risikomanagement [3, S. 457].

Die grundsätzlichen Überlegungen zur Corporate Governance sind auf den Umstand der Trennung von Eigentum und Verfügungsmacht in Unternehmen, besonders in Kapitalgesellschaften, zurückzuführen. Die Eigentümer/Innen von Unternehmen sind zum Beispiel Gesellschafter oder Aktionäre. Die Verfügungsmacht wird durch die Vorstände oder Geschäftsführer/Innen ausgeübt. Das Ziel hierbei ist, die Interessen der Aktionäre zu schützen. Corporate Governance stellt sich somit als zielorientierte Führung und Überwachung von Unternehmen dar [36, S. 19].

Die spezifische Umsetzung und Vorgaben der Corporate Governance sind in eigenen Regelwerken enthalten. In Österreich wird dieses Regelwerk durch den am 1.10.2002 erstmals öffentlich vorgestellten *Österreichischen Corporate Governance Kodex* repräsentiert.[27] Der Kodex umfasst neben wichtigen gesetzlichen Bestimmungen auch international übliche Vorschriften [37, S. 13]. Die Regeln des Kodex sind wie folgt kategorisiert [37, S. 14] :

- **Legal Requirement (L):** Regel beruht zwingend auf Rechtsvorschriften und muss demnach zwingend eingehalten werden.
- **Comply or Explain (C):** Regel soll eingehalten werden; eine Abweichung muss erklärt und begründet werden, um ein kodexkonformes Verhalten zu erreichen.

[27] vgl. [94] und [37]

- **Recommendation (R):** Regel mit Empfehlungscharakter; Nichteinhaltung ist weder offenzulegen noch zu begründen.

Das Risikomanagement ist in insgesamt sechs Regelungen enthalten, welche in der Folge kurz dargestellt werden.

a. Regel 9 (L) [37, S. 18] besagt unter anderem, dass der Vorstand den Aufsichtsrat über die Entwicklung der Risikolage und des Risikomanagements der Gesellschaft informieren muss.
b. Regel 37 (C) [37, S. 28] beschreibt den Informationsaustausch zwischen Aufsichtsrats- und Vorstandsvorsitzende zu den Themen Strategie, Geschäftsentwicklung und Risikomanagement.
c. Regel 40 (L) [37, S. 29] definiert die Einrichtung eines Prüfungsausschusses, welcher die Wirksamkeit des Risikomanagements und IKS überwachen soll.
d. Regel 69 (L) [37, S. 41] legt verbindlich fest, dass das Unternehmen einen Konzernlagebericht vorlegen muss, welcher auch die wesentlichen Merkmale des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess enthält.
e. Regel 70 (C) [37, S. 41] besagt, dass das Unternehmen im Konzernlagebericht wesentliche Risikomanagement-Instrumente in Bezug auf nicht-finanzielle Risiken beschreiben soll.
f. Regel 83 (C) [37, S. 46] schreibt vor, dass der Abschlussprüfer die Funktionsfähigkeit des Risikomanagements beurteilen muss.

Wie erwähnt werden durch die Einhaltung der Corporate Governance im Sinne des Österreichischen Corporate Governance Kodex die Interessen der Aktionäre gewahrt.

3.6.2 IT-Governance

Durch die steigende Anzahl von systemunterstützten Geschäftsprozessen hat die IT einen hohen Stellenwert in Unternehmen erreicht. Keine Organisation kann heutzutage auf den Einsatz von IT-Systemen verzichten und der Einfluss der IT auf den Unternehmenserfolg wird immer größer [38], [39, S. 6].

Das IT-Governance Institute [40] definiert den Begriff *IT-Governance* daher wie folgt [39, S. 11] :

> "*IT Governance liegt in der Verantwortung des Vorstands und des Managements und ist ein wesentlicher Bestandteil der Unternehmensführung. IT Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt.*"

Mit dieser Definition wird festgelegt, dass die IT so ausgerichtet werden muss, dass ein höchstmöglicher Wertbeitrag zur Erreichung der Unternehmensziele gewährleistet wird.

Mit der ISO/IEC 38500 Norm [41] wurde die IT-Governance im Jahr 2008 standardisiert. Die Norm gibt den Rahmen für einen verantwortungsvollen IT-Servicebetrieb vor und richtet sich an die Unternehmensführung [42, S. 24]. Abbildung 10 zeigt den strukturellen Aufbau der Norm in grafischer Form.

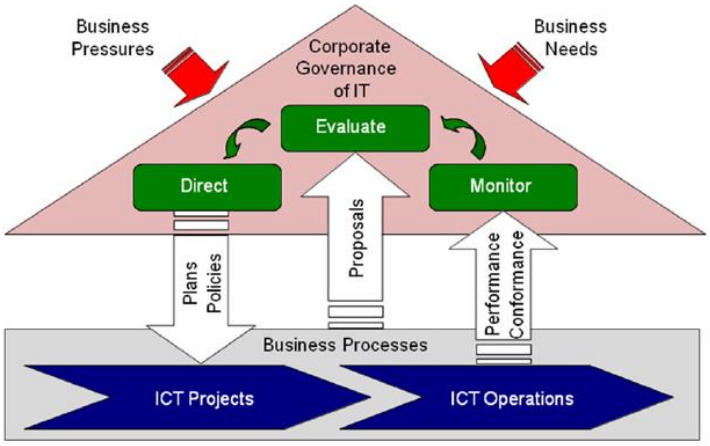

Abbildung 10: Aufbau und Struktur der ISO/IEC Norm[28]

Die Grafik in Abbildung 10 zeigt das Zusammenspiel der drei Grundsätze der Norm in Form der Einleitung von Maßnahmen (*Direct*), der Bewertung (*Evaluate*), und der Überwachung der Auswirkung (*Monitor*). Dabei sind sowohl IT-Projekte als auch die IT-Operation betroffen.

Die sechs Leitsätze der Norm [42, S. 25] zeigen die allgemein gültigen Prinzipien der IT-Governance auf und lauten wie folgt[29]:

a. **Verantwortlichkeit:** alle Verantwortlichkeiten zur Umsetzung und Nutzung der IT sind festgelegt.
b. **Strategie:** die strategische Planung der IT wird an der Unternehmensstrategie ausgerichtet.
c. **Investitionen:** der Nutzen der IT bedingten Anschaffungen steht in einem ausgewogenen Verhältnis zu damit einhergehenden Kosten und Risiken.
d. **Leistungsfähigkeit und Effektivität:** Qualität und Nutzen der IT erfüllen die Anforderungen an das Geschäft des Unternehmens.
e. **Konformität:** gesetzliche Erfordernisse werden eingehalten.

[28] Grafik, Quelle: http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-2-April-2011.aspx [Zugriff am 5.2.2013]
[29] Die Inhalte der erwähnten Quelle wurden, aufgrund der Erfahrungswerte des Autors leicht adaptiert

f. **Verhalten und Bedürfnisse der Mitarbeiter:** bei den IT Abläufen werden die Bedürfnisse der betroffenen Personen respektiert.

Die IT stellt demnach keinen Selbstzweck dar. Der größte Nutzen der IT wird daher weniger durch den Einsatz von neuer Technologie sondern vielmehr durch die konsequente Ausrichtung aller Aktivitäten an die Unternehmensziele erreicht.

3.7 Compliance Management System (CMS)

Unter dem Begriff *Compliance* ist im betriebswirtschaftlichen Kontext allgemein die Einhaltung von Regeln zu verstehen [43, S. 3]. Im deutschen Corporate Governance Kodex ist unter Kapitel 4.1.3 folgendes nachzulesen [44, S. 6] :

> *„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).“*

Damit wird darauf hingewiesen, dass neben den gesetzlichen Vorschriften auch interne Regelungen oder Richtlinien einzuhalten sind.

Der IDW EPS 980 Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland führt im Anhang einige spezifische Rahmenkonzepte für ein Compliance Management System an [43, S. 30]. Für Österreich sind in diesem Zusammenhang die *Grundsätze ordnungsmäßiger Compliance* der Finanzmarktaufsicht (FMA) von Bedeutung [45]. Diese regelt die Compliance Maßnahmen in Kreditinstituten; die Inhalte sind jedoch auch für andere Unternehmen anwendbar.

Die ganzheitliche Steuerung der Compliance und den damit verbundenen Risiken wird im Compliance Management System (CMS) dargestellt. Dabei sind folgende Gegebenheiten zu beachten:

- Die Anforderungen an die Compliance variieren je Unternehmen [46, S. 49]. Es existiert daher keine einheitliche Handlungsanweisung.
- Unterschiedliche gesetzliche, unternehmensinterne und externe Vorschriften können innerhalb eines Unternehmens Gültigkeit haben. Um diese Anforderungen erfüllen zu können, werden in verschiedenen Organisationseinheiten eines Unternehmens interne Kontroll- und Steuerungssysteme implementiert[30].
- Ein weitgehendes Zusammenwirken von Compliance Tätigkeiten mit der Internen Revision und dem Risikomanagement ist anzustreben[31].

[30] vgl. In Anlehnung zu den *Grundsätzen der ordnungsgemäßen Compliance, Kapitel 2.4* [45, S. 2]

[31] vgl. In Anlehnung zu den *Grundsätzen der ordnungsgemäßen Compliance, Kapitel 6* [45, S. 3]

Die im vorigen Absatz genannten Voraussetzungen für ein CMS zeigen, dass eine Integration mit dem Risikomanagement und IKS gegeben ist. Das CMS versteht sich demnach auch als Teil des Risikofrüherkennungs- und Überwachungssystems [46, S. 35].

4 Enterprise Risk Management (ERM) Rahmenbedingungen

In diesem Abschnitt werden die allgemein gültigen Rahmenbedingungen, die für ein ERM beachtet werden müssen oder einen Rahmen für die Implementierung vorgeben, in Form von gesetzlichen Vorgaben und anerkannten Rahmenwerken, dargestellt.

4.1 Gesetzliche Vorgaben, Richtlinien, Standards und Verordnungen

Wirtschaftliche Katastrophen wie zum Beispiel die Konkursfälle von Enron [47] oder Worldcom [48] in den USA bzw. Parmalat [49] in Europa haben die Behörden dazu veranlasst, eigene Gesetze zur Verhinderung derartiger Vorfälle zu erlassen. Die Ursachen dieser Konkurse waren falsche Finanzdaten, fehlendes oder unzulängliches Risikomanagement und, durch mangelhafte interne und externe Kontrollen nicht aufgedecktes, betrügerisches Vorgehen. Als Beispiel werden in der Folge die Ereignisse des US-Energiekonzerns Enron kurz analysiert.

Verursacher	Konkursauslöser	Schwachstellen
• Management • Wirtschaftsprüfer • Aufsichtsrat[32]	• Bilanzfälschung[33] • Bereicherung des Managements[34] • Korruption[35] • Interessenskonflikte[36]	• Wirtschaftsprüfer[24] • Fehlende Kontrolle des Managements durch den Aufsichtsrat

Tabelle 1: Analyse der Ursachen des Enron Konkurses

Der dargestellte Fall zeigt die Notwendigkeit der Gesetzgebungen exemplarisch auf. Wirtschaftsprüfer müssen unabhängiger werden und dürfen in wirtschaftlicher Hinsicht in keiner Abhängigkeit zu Ihren Klienten stehen. Das Management muss in Bezug auf die Korrektheit der Finanzdaten mehr Verantwortung übernehmen und dafür transparente Prozesse im Hinblick auf interne Kontrollen einrichten.

Das Ziel dieser Gesetzgebungen ist daher, das Vertrauen in die Jahres- und Konzernabschlüsse von bedeutenden Unternehmen zu stärken. Bedeutende

[32] Indirekt, da durch die fehlende Aufdeckung die Vorkommnisse nicht verhindert wurden
[33] Siehe dazu in [47, S. 186] über die Fälschungen zwecks Gewinnoptimierung und Erfüllung der Erwartungshaltung der Finanzmärkte
[34] Die Manager konnten durch die Manipulationen ihr Jahreseinkommen auf 100 Millionen US-Dollar und mehr steigern in [47, S. 187]
[35] Von US-Politikern gebilligte und durch Gesetze geförderte Scheingeschäfte führten zu einer künstlichen Verknappung Elektrizität [47, S. 187-188]
[36] Siehe dazu in [47, S. 188] über die Abhängigkeit des Wirtschaftsprüfers zu seinen Auftraggebern

Unternehmen in diesem Zusammenhang sind Firmen, welche von öffentlichem Interesse sind. Dies kann entweder durch eine Börsennotierung oder eine gewisse Unternehmensgröße gegeben sein[37]. Unternehmen dieser Kategorie werden mit den Gesetzen vom Staat angehalten, ihrer Verantwortung als Arbeitgeber und in der Verwaltung des Kapitals der Anleger nachzukommen.

In der Folge werden die einzelnen relevanten Gesetze dargestellt und im Hinblick auf die Einrichtung eines ERM analysiert.

4.1.1 Basel II

Mit Basel II wurden vom *Basler Ausschuss für Bankenaufsicht*[38] die Eigenkapitalanforderungen von Banken einheitlich geregelt [50]. Die Umsetzung in nationale Gesetzgebungen erfolgte stufenweise im Jahr 2008[39].

Zuvor wurde bereits im Jahr 1988 der Baseler Akkord, der später als *Basel I* [51] bezeichnet wurde, veröffentlicht. Dieser gab eine nach wie vor geltende Regelung der Eigenkapitalanforderungen vor. Gemäß dieser Anforderung muss die Bank über ein Eigenkapital von mindestens 8% der risikogewichteten Aktiva verfügen [50, S. 2]. Risiken bei der Kreditvergabe, welche die Bonitäten der Kreditnehmer berücksichtigen sah Basel I nicht vor, wodurch die schlechten durch die besseren Kreditnehmer subventioniert wurden. Die zunehmende Dynamik des Kreditgeschäftes und ungerechte Verteilung der Risiken zwischen Kunden und Banken führte daher im Jahr 2007/2008 mit Basel II zur Erweiterung der Vorgaben.

Obwohl die Regelungen in Basel II nur für den Finanzsektor maßgebend sind, können die Inhalte im Hinblick auf die enthaltenen Ausführungen zum operationellen Risikomanagement [50, S. 163-176] in angepasster Form auch die Basis für die risikoorientierte Steuerung von Unternehmen darstellen. In [52, S. 3-5] werden in diesem Kontext konkrete Praxisempfehlungen zum Management operationeller Risiken beschrieben. In der Folge werden die Hauptpunkte dieser Empfehlungen, welche auch für Nicht-Finanzdienstleister Gültigkeit haben, angeführt:

- Entwicklung geeigneter Rahmenbedingungen für das Risikomanagement
- Erkennung, Bewertung, Überwachung und Minderung/Begrenzung von Risiken
- Externe Prüfung durch die Bankenaufsicht
- Offenlegung des Ansatzes des operationellen Risikomanagements

Abbildung 11 zeigt, in struktureller Form zusammengefasst, die wichtigsten Punkte der Mindestanforderungen des operationellen Risikomanagements aus Basel II.

---

[37] Siehe Artikel 2, Abs. 13 der 8. EU-Richtlinie [67]

[38] Siehe dazu eine Information des Bundesministeriums für Finanzen unter http://www.bmf.gv.at/Finanzmarkt/BaslerAusschussfrBa_11398/_start.htm [Zugriff am 7.2.2013]

[39] Siehe [50, S. 1]

Abbildung 11: Operationelles Risiko nach Basel II[40]

Die Mindestanforderungen enthalten keine konkreten Handlungsanweisungen zur Umsetzung stellen jedoch ein Grundgerüst für ein Basis Risikomanagementsystem dar.

4.1.2 Kreditwesengesetz (KWG)

Das deutsche Kreditwesengesetz (KWG) [53] bezieht sich auf Kreditinstitute und Finanzdienstleistungsinstitute. Nach den Erfahrungen des Autors können die im Gesetz verankerten, detaillierten Vorschriften für Risikomanagement und IKS jedoch auch für Unternehmen, welche nicht aus dem Finanzsektor kommen sinnvoll angewandt werden.

Mit dem KWG wird in Deutschland Basel II umgesetzt. Durch die, im Gesetz vorgegebene, Aufsichtstätigkeit der *Bundesanstalt für Finanzdienstleistungsaufsicht* wird Missständen im Kredit- und Finanzdienstleistungswesen, welche erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können, entgegengewirkt.[41] Das Gesetz enthält, unter anderem, umfangreiche Vorschriften im Hinblick auf die Eigenmittelausstattung und das Eingehen von Risiken im Kreditgeschäft[42]. Diese Vorschriften betreffen ablauforganisatorische Maßnahmen zur Risikobegrenzung.

§25a des KWG [53, S. 87-89] regelt die die organisatorischen Voraussetzungen im Sinne einer Aufbauorganisation für das interne Risikomanagement und IKS und der Beschreibung von Kontrollverfahren. Abbildung 12 zeigt die, in diesem Zusammenhang stehende, organisatorische Struktur.

[40] Quelle: eigene Darstellung in Anlehnung an [50, S. 163-176]
[41] vgl. §6 Abs. 2 – Aufgaben der Bundesanstalt für Finanzdienstleistungsaufsicht [53, S. 27]
[42] Siehe *Zweiter Abschnitt* des KWG [53]

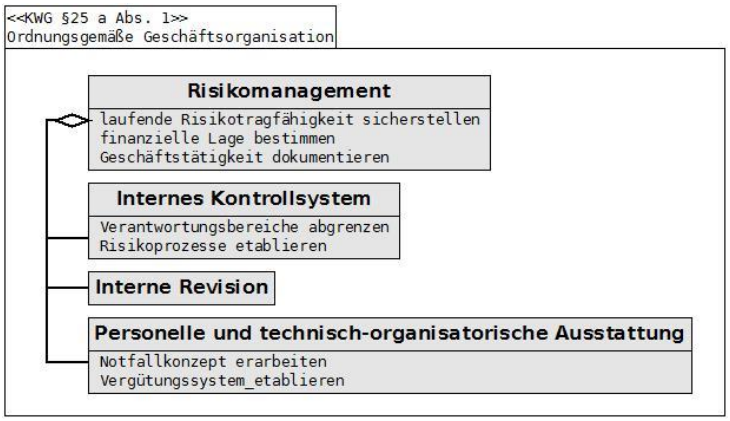

Abbildung 12: Organisatorische Risikomanagement- und IKS Struktur[43]

Die Geschäftsführung oder der Vorstand, welche die Gesellschaft führen sind für die ordnungsgemäße Geschäftsorganisation verantwortlich.[44] Der Bereich des IKS umfasst Risikoprozesse im Sinne der Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken[45]. Bei der personellen und technisch-organisatorischen Ausstattung der Gesellschaft wird im Bereich des Notfallkonzepts die IT eigens erwähnt.[46] Das angemessene, transparente und auf eine nachhaltige Entwicklung des Instituts ausgerichtete Vergütungssystem bezieht sich auf die Geschäftsführung und Mitarbeiter der Gesellschaft.[47]

4.1.3 Mindestanforderungen an das Risikomanagement (MaRisk)

Mit den *Mindestanforderungen an das Risikomanagement (MaRisk)* [54] wird durch die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Ausgestaltung des Risikomanagements für Banken im Sinne des §25a Abs. 1 des KWG vorgegeben.[48] Damit wurde ein praxisnaher Rahmen [54, S. 3, AT 1 - Vorbemerkung] für die Implementierung geschaffen. Die Vorgaben setzen sich aus einem allgemeinen und einem besonderen Teil zusammen. Der allgemeine Teil (AT) beschreibt die Grundsätze des Risikomanagements. Im besonderen Teil (BT) sind spezifische Anforderungen im Hinblick auf die konkrete Umsetzung des Risikomanagements enthalten.

Der mit Basel II [50] geschaffene Rahmen, der eine ganzheitliche Betrachtung für das Management aller relevanten Risiken vorsieht, stellt die Basis für die MaRisk dar [55, S. 5]. Das qualitative Risikomanagement im Sinne der Darstellung von Risikoprozessen und eine für das Risikomanagement geeignete Aufbauorganisation stehen hierbei im Vordergrund.

[43] Quelle: eigene Darstellung in Anlehnung an § 25a Abs. 1 des KWG [53, S. 87-88]
[44] Gemäß §25a Abs. 1 des KWG [53, S. 87, 2. Satz]
[45] Gemäß §25a Abs. 1 des KWG [53, S. 87, Punkt 1b]
[46] Gemäß §25a Abs. 1 des KWG [53, S. 87, Punkt 3]
[47] Gemäß §25a Abs. 1 des KWG [53, S. 87, Punkt 4]
[48] Siehe dazu die Vorbemerkung des Rundschreibens vom 14.12.2013 [54, S. 3]

Die detaillierte Sichtweise des allgemeinen Teils (AT) der MaRisk eignet sich sehr gut für die Darstellung von allgemeingültigen Anforderungen an ein Risikomanagement inklusive IKS. Abbildung 13 zeigt daher die für das Risikomanagement und IKS relevanten Teile in strukturierter Form[49].

Die Hauptpunkte des besonderen Teils (BT) beschreiben die *besonderen Anforderungen* an das IKS und die Ausgestaltung der Internen Revision. Beide Bereiche stellen die Risikoorientierung in den Vordergrund. So wird zum Beispiel für die Interne Revision folgendes definiert [54, S. 35, BT 2.1]:

> *„Die Prüfungstätigkeit der Internen Revision hat sich auf der Grundlage eines risikoorientierten Prüfungsansatzes grundsätzlich auf alle Aktivitäten und Prozesse des Instituts zu erstrecken."*

Alle anderen Punkte des besonderen Teils (BT) betreffen spezifische Anforderungen an das Geschäft einer Bank und werden daher in dieser Arbeit nicht näher betrachtet.

[49] Inklusive Darstellung operationeller Risiken aus dem besonderen Teil (BT) [54, S. 35]

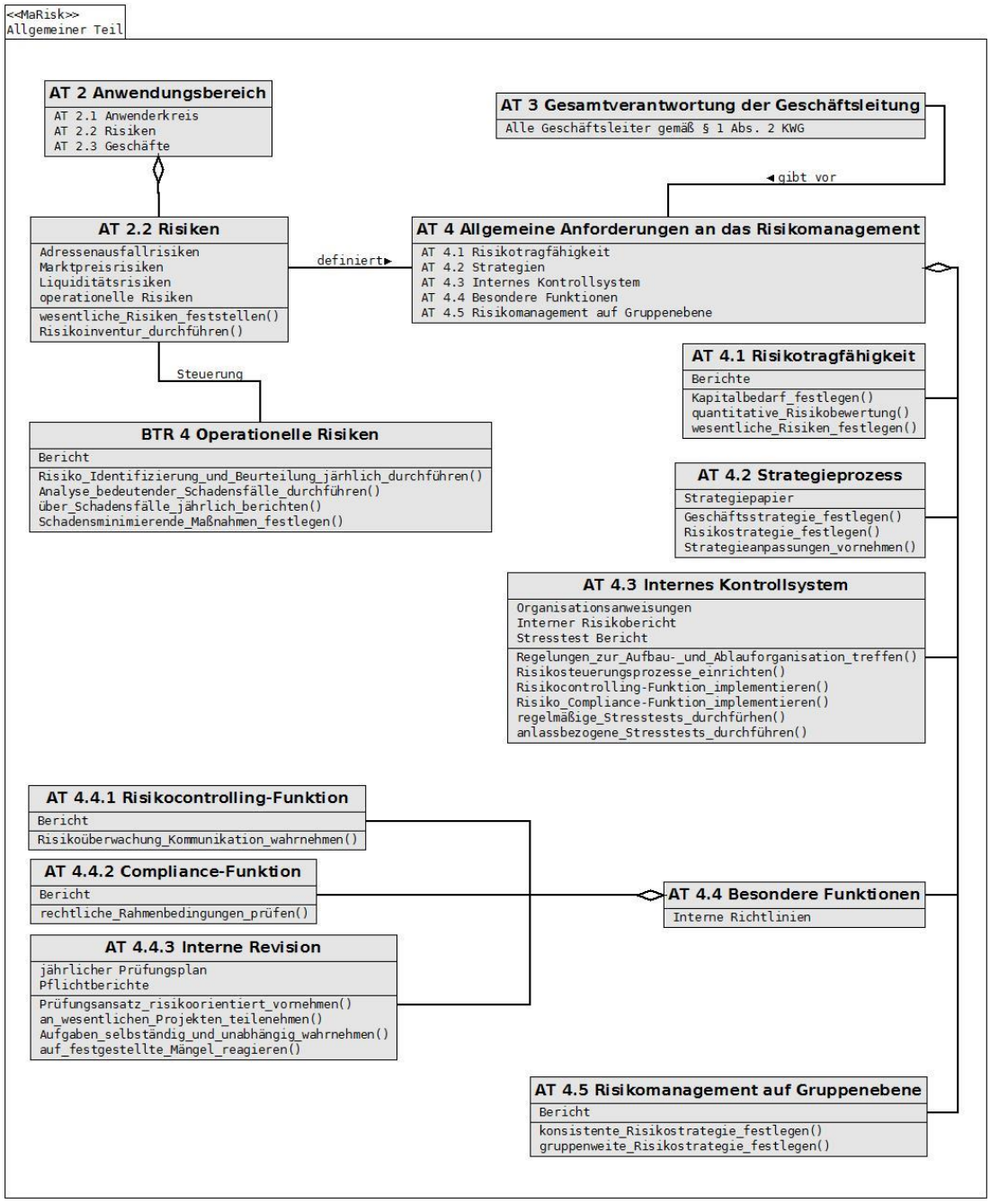

Abbildung 13: Strukturelle Darstellung des Risikomanagements nach MaRisk[50]

[50] Quelle: eigene Darstellung in Anlehnung an [54, S. Allgemeiner Teil]

4.1.4 Solvency II

Für Versicherungen wurden mit Solvency II [56] im Rahmen eines Projektes der Europäischen Union eigene Richtlinien verabschiedet, welche im Bereich des operationellen Risikomanagements Ähnlichkeiten zu Basel II aufweisen.

Der Schutz von Versicherungsnehmern und -gebern soll gemäß der Richtlinie gleichermaßen gewährleistet werden[51], indem die Solvenz Anforderungen an das Versicherungsunternehmen reguliert werden. Unter Solvenz Anforderungen sind jene Forderungen gegen das Versicherungsunternehmen zu verstehen, welche im Schadensfall an Versicherungsnehmer zu begleichen sind[52]. Damit verbunden sind Eigenkapitalvorschriften, welche die Zahlungsfähigkeit der Versicherung im Schadensfall sicherstellen.

Die Richtlinie basiert auf drei Säulen, welche in Abbildung 14 dargestellt werden.

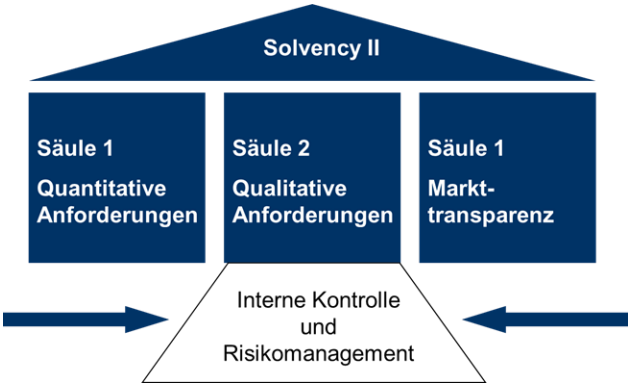

Abbildung 14: Solvency II Säulenmodell[53]

- Die erste Säule beschreibt die Kapitalanforderungen an Versicherungsunternehmen, die durch eine Formel konkret festgelegt wird[54].
- In der zweiten Säule wird das qualitative Risikomanagement dargestellt, das hauptsächlich in Form von transparenter Risikosteuerung realisiert werden muss[55].
- Die dritte Säule beinhaltet die Berichtserstattungspflichten für Versicherungsunternehmen, welche den *International Financial Reporting Standards* (IFRS) [57] angeglichen werden sollen.

[51] Siehe Artikel 17 in [56, S. L 335/3]
[52] Unter Solvenz ist die Fähigkeit einer Person oder einer Unternehmung, ihre fälligen Verbindlichkeiten sofort bzw. innerhalb absehbarer Zeit zu erfüllen, zu verstehen – vgl. [99]
[53] Quelle: eigene Darstellung in Anlehnung an [84]
[54] Siehe ANNEX IV in [56, S. L 335/124] – „Calculation of the Basic Solvency Capital Requirement“
[55] Siehe Ausführungen in [56, S. L 335/34]

Zur Berechnung der *Solvenz Kapital Anforderung* wird auch das operationelle Risiko berücksichtigt[56]. Versicherungen mit einer höheren Risikobereitschaft müssen über ein höheres Eigenkapital verfügen [58, S. 3].

Nach den Erfahrungen des Autors schließt das operationelle Risikomanagement einer Versicherung auch die Analyse des versicherten Unternehmens mit ein. Kann ein Unternehmen ein gut geführtes Risikomanagementsystem vorweisen, ist das Ausfallsrisiko der Versicherung bei Vertragsabschluss geringer. Durch die, damit verbundenen, geringeren Risikokosten sinken in der Regel auch die Prämienzahlungen.

4.1.5 Sarbanes-Oxley Act of 2002 (SOX)

Im Juli 2002 wurde der *Sarbanes-Oxley Act of 2002 (SOX)* [24] vom US-Kongress als Bundesgesetz verabschiedet. Den Anlass für diese Gesetzgebung bildeten vor allem, die, durch Bilanzmanipulationen verursachten, Finanzskandale der Firmen Enron [47] und Worldcom [48]. Das Hauptziel des Gesetzes ist, die Vertrauenswürdigkeit der veröffentlichten Finanzzahlen von Unternehmen wieder herzustellen und das Vertrauen der Investoren zu stärken [59]. Das Gesetz betrifft alle öffentlichen in- und ausländische Unternehmen, welche an US-Börsen notiert sind [60, S. 3].

Der Großteil der im Gesetz verankerten Maßnahmen betrifft das Management und den Abschlussprüfer. Das Verhältnis zwischen dem Abschlussprüfer und dem Unternehmen ist genau geregelt. Im Zuge der Gesetzeserlassung wurde deshalb auch ein eigenes behördliches Aufsichtsgremium für Wirtschaftsprüfer, das *Public Accounting Oversight Board* (PCAOB) neu etabliert[57]. Wirtschaftsprüfer waren in der Vergangenheit für die, auch vom Gesetz vorgeschriebene, externe Qualitätskontrolle zuständig. Diese Zuständigkeit wurde an das PCAOB übertragen. Die dafür vorgesehenen Regelungen sind in der SOX Section 101 [24] festgeschrieben, in welcher der Aufsichtsbehörde PCAOB umfangreiche Befugnisse zugeteilt wurden. Es soll damit verhindert werden, dass Unternehmen und Wirtschaftsprüfer aufgrund von wirtschaftlichen Abhängigkeiten zusammenarbeiten, um Bilanzpositionen bewusst oder unbewusst verfälscht darstellen.

Die *Security and Exchange Commission* (SEC) als US Börsenaufsichtsbehörde ist für die Prüfung des PCAOB zuständig und hat dahingehend weitreichende Befugnisse. Damit ist sichergestellt, dass die oberste US-Behörde des Börsenwesens für die Einhaltung aller Gesetze verantwortlich ist [61, S. 91].

Die wichtigsten Teile des Gesetzes in Zusammenhang mit Risikomanagement und IKS sind die Abschnitte (Sections) 302 und 404 [24], welche im Folgenden dargestellt werden.

[56] Siehe [56, S. L 335/51] – *Article 101 Calculation of the Solvency Capital Requirement*
[57] Siehe *Section 101* in [24]

- **Section 302** beschreibt die Verantwortungen des Vorstandes. Die Unternehmensführung hat die Pflicht zur Etablierung von Offenlegungskontrollen und –verfahren. Zudem wird eine zeitgerechte Veröffentlichung von wichtigen finanziellen und nichtfinanziellen Berichten verlangt. Gleichzeitig muss ein internes Frühwarnsystem eingeführt werden, welches ermöglicht, dass Existenz bedrohende Szenarien abgewehrt oder frühzeitig in Erfahrung gebracht werden können. Der Chief Executive Officer (CEO) und der Chief Financial Officer (CFO) müssen eidesstattliche Erklärungen über die Korrektheit der Darstellung der finanziellen Situation des Unternehmens abgeben[58].
- **Section 404** betrifft direkt das IKS und soll verhindern, dass aufgrund von mangelnden Kontrollen die Finanzberichtserstattung nicht korrekt ist. Auch hier sind CEO und CFO persönlich verantwortlich, indem von ihnen verlangt wird, dass sie die Effektivität des IKS überprüfen und über die Inhalte Bescheid wissen[59]. Der Jahresbericht des Unternehmens muss demnach auch eine Beschreibung des IKS enthalten, welche vom Abschlussprüfer testiert werden muss[60].

Nach [61, S. 112] ist das wichtigste Element des Gesetzes die Delegierung von speziellen Verfügungsvollmächten des US-Kongresses an das PCAOB, da dieses Regeln schneller anpassen und auf Anfragen von Interessensvertretungen flexibler reagieren kann.

4.1.6 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Das Gesetz für Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [62] trat am 1.5.1998 in der Bundesrepublik Deutschland in Kraft und enthält umfangreiche Änderungen des deutschen Aktien- und Handelsgesetzes [63, S. 37].

Die wichtigste Neuerung betrifft die Änderung des §91 Abs. 2 [62, S. 787] des deutschen Aktiengesetzes mit folgender Forderung an den Vorstand [63, S. 39], [64, S. 31] :

> *„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“*

Diese Definition impliziert die Führung eines Risikomanagementsystems („*den Fortbestand gefährdende Entwicklungen“*) und IKS (*„Überwachungssystem“*). In diesem Zusammenhang sind folgende Neuregelungen von Bedeutung [63, S. 38] :

[58] In Anlehnung an [85, S. 92-93]
[59] Siehe Section 404/subsection (a)/(1) und (2) in [24]
[60] Siehe Section 404/subsection (b) in [24]

- Die Einrichtung eines Risikomanagementsystems durch *„die Verpflichtung des Vorstands, für ein angemessenes Risikomanagement und für eine angemessene interne Revision zu sorgen“* wird verdeutlicht [65, S. 15]
- Erwähnung der zukünftigen Risikoentwicklungen im Lagebericht der Gesellschaft [65, S. 7].
- Änderungen in der Abschlussprüfung durch den Wirtschaftsprüfer im Hinblick auf eine stärker risikoorientierte Prüfung [65, S. 11] sowie der Beurteilung von erforderlichen Verbesserungsmaßnahmen des internen Überwachungssystems [62, S. 790]. Durch die neue Art der Prüfung soll der Aufsichtsrat Aufschlüsse zu bestehenden oder drohenden Risiken für das Unternehmen erhalten und damit in die Lage versetzt werden, verbesserte Kontrollmöglichkeiten einzuleiten [65, S. 11].

Der Grund der Gesetzgebung in Deutschland weist Ähnlichkeiten zum *Sarbanes Oxley Act of 2002* in den USA auf. Auch hier waren Unternehmenskrisen der vergangenen Jahre der Gesetzgebung vorausgegangen [63, S. 37].

4.1.7 Die 8. EU-Richtlinie

EU-Richtlinien geben seitens der Europäischen Union einen Rahmen für die Erlassung von neuen Gesetzen in den EU-Mitgliedsstaaten vor. In der *konsolidierten Fassung des Vertrags zur Gründung der europäischen Gemeinschaft* wird der Terminus einer *Richtlinie* in Artikel 288 [66, S. C 326/172] wie folgt definiert:

> *„Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. „*

Demnach müssen EU-Richtlinien in nationales Recht umgesetzt werden, die konkrete Umsetzung bleibt jedoch dem Mitgliedsstaat vorbehalten.

Die 8. EU-Richtlinie mit der offiziellen Bezeichnung *2006/43/EG* [67] wurde am 17.5.2006 vom Europäischen Parlament und Rat beschlossen. Die Umsetzung in nationales Recht musste von allen 27 EU Mitgliedsstaaten bis spätestens 29.6.2008 vollzogen werden[61].

Nach [67, S. L 157/91] werden mit der Richtlinie folgende Ziele verfolgt:

- Verbindliche Vorgabe eines Satzes internationaler Prüfungsstandards
- Aktualisierung der Ausbildungsvoraussetzungen für Wirtschaftsprüfer
- Festlegung von Berufsgrundsätzen für Wirtschaftsprüfer

[61] Siehe Artikel 53 der 8. EU-Richtlinie [67, S. L 157/107]

- Verbesserung und Harmonisierung der Qualität der Abschlussprüfung
- Stärkung des Vertrauens in die Abschlussprüfung

Im Hinblick auf das Risikomanagement und IKS weist die Richtlinie in abgeschwächter Form einige Ähnlichkeiten mit der *Section* 404 des *Sarbanes Oxley Act of 2002* auf [3, S. 26]. So ist zum Beispiel ein IKS einzurichten [67, S. L157/90], welches die Wirksamkeit der internen Kontrollen, des Risikomanagements und der Internen Revision überwachen soll.

Die Richtlinie wird auch als „*Abschlussprüferrichtlinie*" bezeichnet, da besonders auf die Rolle der Unabhängigkeit des Wirtschaftsprüfers eingegangen wird und das Vertrauen in die Abschlussprüfung von Unternehmen gestärkt werden soll[62]. Von der Richtlinie betroffen sind Unternehmen von öffentlichem Interesse, wie zum Beispiel Banken, Versicherungen oder börsennotierte Unternehmen[63].

Eine der Besonderheiten ist die Einführung eines Prüfungsausschusses[64] mit bestimmten Pflichten, wie die Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des IKS, der Internen Revision und des Risikomanagements sowie der Unabhängigkeit des Abschlussprüfers. Der Abschlussprüfer selbst muss dem Prüfungsausschuss über die wesentlichen Erkenntnisse der Prüfung und Schwächen des IKS berichten[65].

In Bezug auf Risikomanagement und IKS ist folgender Passus in der Richtlinie von Bedeutung [67, S. L 157/90] :

> *„Prüfungsausschüsse und ein wirksames internes Kontrollsystem tragen dazu bei, finanzielle und betriebliche Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmaß zu begrenzen und die Qualität der Rechnungslegung zu verbessern."*

Damit ist eine verbindliche Verankerung des Risikomanagements inklusive IKS gegeben, welche sich in den nationalen Gesetzen wiederfinden muss. In Österreich erfolgte diese Umsetzung mit dem Unternehmensrechtsänderungsgesetz 2008, welches im nächsten Abschnitt vorgestellt wird.

4.1.8 Unternehmensrechtsänderungsgesetz 2008 (URÄG)

Das Unternehmensrechtsänderungsgesetz 2008 (URÄG) [25] trat allgemein am 1.6.2008 in Kraft und gilt für Geschäftsjahre, die nach dem 31.12.2008 beginnen. Es gilt in vollem Umfang für börsennotierte Unternehmen und teilweise für kapitalmarktorientierte Unternehmen, nicht kapitalmarktorientierte Aktiengesellschaften, nicht kapitalmarktorientierte Europäische

[62] Siehe [67, S. L 157/87] – die Beschreibung der Gründe der Richtlinie
[63] Siehe [67, S. L 157/92] – Artikel 2 (*Begriffsbestimmungen*), Abs. 13
[64] Siehe [67, S. L 157/103] – Artikel 41 (*Prüfungsausschuss*)
[65] Siehe [67, S. L 157/103] – Artikel 41 (*Prüfungsausschuss*), Abs. 4

Aktiengesellschaften, Ges.m.b.Hs und Genossenschaften soweit es sich bei diesen um Unternehmen im öffentlichen Interesse handelt[66].

Unternehmen im öffentlichen Interesse sind Kapitalgesellschaften, die kapitalmarktorientiert sind oder das Fünffache der in Euro ausgedrückten Merkmale einer großen Gesellschaft überschreiten[67]. Im Zuge der Erlassung des Gesetzes wurden die Schwellenwerte für kleine, mittelgroße und große Kapitalgesellschaften angehoben [25, S. 1]. Die Anhebung wurde notwendig, um den administrativen Aufwand für kleinere Unternehmen, welche sich mit dem Gesetz ergeben, in Grenzen zu halten. Tabelle 2 zeigt, wie sich die einzelnen Werte je Unternehmenskategorie verändert haben.

	Unternehmen in Österreich		
Unternehmenskategorie	**Kleine**	**Mittelgroße**	**Große**
Kriterien	2 der 3 Merkmale nicht überschreiten	2 der 3 Merkmale der kleinen überschreiten und 2 der 3 nicht überschreiten	2 der 3 Merkmale der mittelgroßen überschreiten
Merkmale alt:			
1. Bilanzsumme	€ 3,65 Mio	€ 14,6 Mio	
2. Umsatzerlöse	€ 7,3 Mio	€ 29,2 Mio	
3. Anzahl Arbeitnehmer/Innen im Jahresschnitt	50	250	
Merkmale neu:			
1. Bilanzsumme	€ 4,84 Mio	€ 19,25 Mio	
2. Umsatzerlöse	€ 9,68 Mio	€ 38,5 Mio	
3. Anzahl Arbeitnehmer/Innen im Jahresschnitt	50	250	

Tabelle 2: Gegenüberstellung der alten und neuen Schwellenwerte gemäß URÄG[68]

Hinsichtlich Bilanzsumme und Umsatzerlöse fallen daher Unternehmen unter das URÄG, welche folgende Kriterien aufweisen[69]:

- Höhe der Bilanzsumme > **96,25** Millionen Euro
  - da 19,25 Millionen Euro Bilanzsumme x 5 = **96,25** Millionen Euro
- Höhe der Umsatzerlöse > **192,5** Millionen Euro
  - da 38,5 Millionen Euro Umsatzerlöse in den letzten zwölf Monaten vor dem Abschlussstichtag x 5 = **192,5** Millionen Euro

Im Hinblick auf das Risikomanagement und IKS sieht das URÄG folgende relevante Punkte vor:

- Ausweitung der Aufgaben des Prüfungsausschusses durch[70]:

[66] In Anleitung an die Regierungsvorlage zum URÄG 2008 [86, S. 5]
[67] In der Regierungsvorlage zum URÄG 2008 [86, S. 5] wird diesbezüglich auf § 271a Abs.1 des Unternehmensgesetzbuchs (UGB) verwiesen, welcher Unternehmen von gesamtwirtschaftlicher Bedeutung beschreibt
[68] Quelle: eigene Darstellung in Anleitung an Artikel I (*Änderung des Unternehmensgesetzbuchs*) Abs.2 des URÄG [25, S. 1]
[69] Als Basis dienen die Schwellenwerte für große Unternehmen gemäß Tabelle 2
[70] Gemäß URÄG [25] , Artikel II, III, IV, V

1. die Überwachung des Rechnungslegungsprozesses
2. die Überwachung der Wirksamkeit des IKS, gegebenenfalls des internen Revisionssystems und Risikomanagementsystems der Gesellschaft
3. die Überwachung der Abschlussprüfung und Konzernabschlussprüfung
4. die Prüfung und Überwachung der Unabhängigkeit des Abschlussprüfers (Konzernabschlussprüfers), insbesondere im Hinblick auf die für das geprüfte Unternehmen erbrachten zusätzlichen Leistungen
5. die Prüfung des Jahresabschlusses
6. gegebenenfalls die Prüfung des Konzernabschlusses und Konzernlageberichtes sowie die Erstattung des Berichtes über die Prüfungsergebnisse an den Aufsichtsrat
7. die Vorbereitung des Vorschlages des Aufsichtsrates für die Auswahl des Abschlussprüfers (Konzernabschlussprüfers)

- Dem Prüfungsausschuss muss weiterhin ein Finanzexperte angehören.
- Jährlich verpflichtende Corporate Governance Erklärung

  Der Abschussprüfer und der Prüfungsausschuss müssen überprüfen, ob der Bericht erstellt wurde. Die Inhalte selbst werden hierbei nicht bewertet.
- Gesetzliche Schwerpunkte zum Begriff des Internes Kontrollsystems

  Das URÄG 2008 enthält keine exakte gesetzliche Definition zum IKS-Begriff.

  Die in §82 des Aktiengesetzes und §22 des GmbH Gesetzes erwähnten Inhalte geben keine verbindlichen Regelungen sondern eher Standards vor[71].

  In der Regierungsvorlage zum Insolvenzrechtsänderungsgesetz (IRÄG) 1997 findet sich folgender Passus, welcher den Terminus IKS am exaktesten beschreibt [68, S. 64]:

  > *„Unter einem internen Kontrollsystem sind sämtliche aufeinander abgestimmte Methoden, um das Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten sowie die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen, zu verstehen.“*

  Diese weite Definition schließt auch Risikomanagement im Unternehmen und die Interne Revision mit ein.

[71] Die diesbezüglichen Gesetzestexte im Aktien- und GmbH Gesetz sind exakt gleich und lauten wie folgt: *„Die Vorstände (AG) bzw. Geschäftsführer (GmbH) haben dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“* [11], [10]

Mit dem URÄG 2008 wurden die Inhalte der 8. EU-Richtlinie umgesetzt[72] sowie einige Gesetze, wie zum Beispiel das Unternehmensgesetzbuch, das Aktiengesetz 1965 oder das GmbH-Gesetz geändert.

4.1.9 SAS 70

Der *Statement on Auditing Standards No. 70* (SAS 70) [69] ist ein Standard des *American Institute of Certified Public Accountants* (AICPA) als Berufsverband der US Wirtschaftsprüfer. Mit diesem Standard werden die wesentlichen Bestandteile des IKS über einen Zeitraum von 6 Monaten detailliert getestet [69, S. 24].

Durch eine Zertifizierung kann zum Beispiel die Qualität der IT-Services von Unternehmen nachweislich dargestellt werden. Dies ist besonders bei der Auslagerung von Geschäftsprozessen relevant. Der SAS 70 Report besteht aus zwei Typen wie folgt [70] :

- Der Typ I ist eine Bescheinigung über die Angemessenheit der Kontrollen und Nachvollziehbarkeit des IKS
- Durch den Typ II erfolgt eine Bescheinigung über die Wirksamkeit und Funktionsfähigkeit der Kontrollen

Nach den Erfahrungen des Autors eignet sich der SAS 70-Report besonders als Qualitätskriterium für Rechenzentren, Service Organisationen und die unternehmensinterne IT-Abteilung in Ihrer Rolle als interner Dienstleister.

4.1.10 Zusammenfassung der gesetzlichen Vorgaben, Richtlinien und Standards

Im Zuge des Worldcom Skandals büßten Investoren im Jahr 2002 insgesamt 180 Milliarden US-Dollar ein.[73] Ein Jahr zuvor verloren Anleger mit dem Konkurs beim Mischkonzern Enron weitere 61 Milliarden [71, S. 3]. Diese Ereignisse waren unter anderem die Auslöser umfassender Gesetzgebungen in USA, und nachfolgend, in Europa. All diese neuen Gesetze wurden notwendig, da klassische, quantitativ geprägte, aufsichtsratsrechtliche Instrumentarien in Bezug auf das Risikomanagement nicht mehr ausreichten, Schäden zu verhindern.[74]

Eine Gruppe der, in diesem Abschnitt vorgestellten, Vorgaben in Form von Gesetzen, Richtlinien, Verordnungen oder Standards betrifft Kreditinstitute und Versicherungen. Wie bereits erwähnt sind diese, meist sehr detaillierten, einhergehenden Anforderungen auch für Unternehmen anwendbar. Abbildung 15

[72] Siehe Artikel XI (Hinweis auf Umsetzung) §1 des URÄG [25]
[73] vgl. [96]
[74] vgl. MaRisk – „Beweggründe und Historie“ in [55, S. 5]

veranschaulicht diese Vorgaben und deren Umsetzung in Form des Säulenmodells von Basel II.[75]

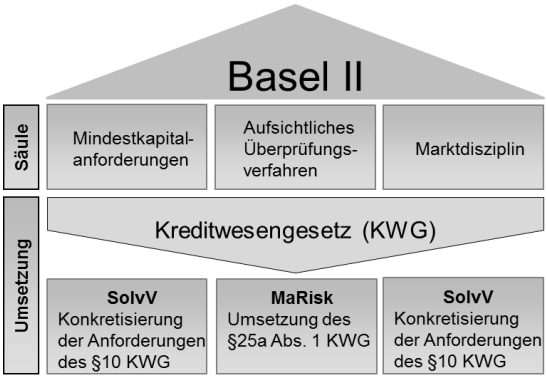

Abbildung 15: Darstellung der Vorgaben für Kreditinstitute[76]

Die Anforderungen von Basel II müssen von den Mitgliedsstaaten der Europäischen Union in nationales Recht umgesetzt werden.[77] Abbildung 15 zeigt, beispielhaft, die Umsetzung in der Bundesrepublik Deutschland in Form des Kreditwesengesetzes (KWG). Die Solvabilitätsverordnung (SolvV) [72] sowie die MaRisk [54] unterstützen hierbei die Umsetzung des KWG durch konkrete Maßnahmen.

Die Umsetzung der Anforderungen der Solvency II Richtlinie ist zum Zeitpunkt der Erstellung der vorliegenden Arbeit noch nicht vollzogen. In der Bundesrepublik Deutschland liegt dafür ein *Regierungsentwurf für das Zehnte Gesetz zur Änderung des Versicherungsaufsichtsgesetzes* vor, welcher vorsieht, dass die Solvency II Richtlinie ab dem 1. Jänner 2014 in vollem Umfang anzuwenden ist.[78]

Die zweite Gruppe der Vorgaben betrifft die Umsetzung von Gesetzen für große Unternehmen von öffentlichem Interesse. Abbildung 16 zeigt in diesem Kontext die Entstehung des Unternehmensrechtsänderungsgesetzes (URÄG) in Österreich.

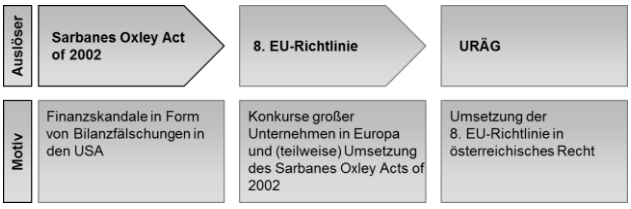

Abbildung 16: Umsetzung des URÄG in Österreich[79]

Der Anfang der Gesetzgebungen erfolgte in den USA mit dem Sarbanes Oxley Act of 2002. Anschließend wurde im Jahr 2006 in 8. EU-Richtlinie verabschiedet,

[75] vgl. Teile 2 bis 4 in Basel II [50], welche das Säulenmodell beschreiben
[76] Quelle: eigene Darstellung
[77] vgl. [50, S. 1, 2. Absatz]
[78] vgl. [95]
[79] Quelle: eigene Darstellung

welche mit dem URÄG in Österreich 2008 umgesetzt wurde. In der Bundesrepublik Deutschland wurden mit dem *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*, welches umfangreiche Änderungen des Aktien- und Handelsgesetzes enthält, bereits im Jahr 1998 Maßnahmen für die Einführung eines unternehmensweiten Risikomanagements gesetzt.

Mit der Ausnahme der MaRisk enthalten die angeführten Gesetze, Richtlinien, Verordnungen oder Standards keine konkreten Handlungsanweisungen zur Umsetzung von Risikomanagement und IKS. Anerkannte Rahmenwerke oder Normen, welche in den nächsten Abschnitten beschrieben werden, helfen, die Ziele der Gesetzgebungen umzusetzen.

4.2 Rahmenwerke

Zur Umsetzung der im vorigen Abschnitt beschriebenen gesetzlichen Vorgaben und Richtlinien stehen allgemein anerkannte Rahmenwerke für Risikomanagement, IKS und IT zur Verfügung. Der Vorteil beim Einsatz von Rahmenwerken ist, dass durch eine allgemeingültige, vorgegebene Struktur eine transparente Darstellung der notwendigen Maßnahmen vorgegeben wird. In diesem Abschnitt werden die Rahmenwerke COSO [4], [16], COBIT [17], [18] und ITIL [73] als Grundlage für die Einführung und Aufrechterhaltung eines ERM in Unternehmen dargestellt.

COSO II [21] stellt den Rahmen für das allgemeine, unternehmensweite Risikomanagement (ERM) dar. Die IT-spezifischen Vorgaben werden durch das COBIT Rahmenwerk definiert. COBIT gibt demnach im Rahmen von COSO II die Anforderungen an die Steuerung der IT-Governance vor [18, S. 8]. Konkrete Prozessschritte und Anweisungen zur Umsetzung der Vorgaben sind in COBIT nicht enthalten, da lediglich definiert wird, *was* gemacht werden muss [74, S. 11]. ITIL unterstützt COBIT in diesem Kontext indem aufgezeigt wird, *wie* die Vorgaben umgesetzt werden [74, S. 6]. Durch das Zusammenwirken der erwähnten Rahmenwerke und den in Abschnitt 4.3 dargestellten Normen wird das unternehmensweite Risikomanagement unter Berücksichtigung der IT-relevanten Prozesse umgesetzt. Abbildung 17 veranschaulicht diese Zusammenhänge.

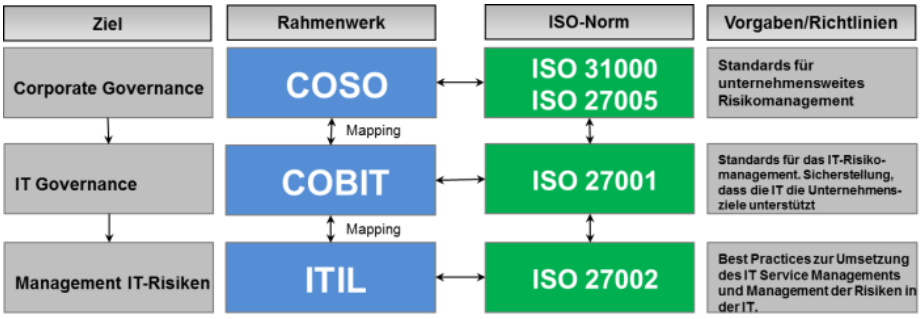

Abbildung 17: Zusammenhang zwischen den verwendeten Rahmenwerken[80]

[80] Quelle: eigene Darstellung in Anlehnung an [74], [18]

4.2.1 COSO II - ERM

Die COSO Rahmenwerke werden vom *"Committee of Sponsoring Organizations of the Treadway Commission" (COSO)*, einer freiwilligen privatwirtschaftlichen Organisation in USA [4], [16], publiziert. Das Hauptziel dieser Organisation ist, die Finanzberichterstattung und das ethische Handeln von Unternehmen durch interne Kontrollen zu verbessern. Die erste COSO Version wurde bereits im Jahr 1992 veröffentlicht [75, S. 1]. Der nunmehr erhöhte Stellenwert in den USA kann als Reaktion auf die Einführung des Sarbanes Oxley Acts of 2002 [24] im Jahr 2002 mit besonderem Augenmerk auf die bereits beschriebene *Section 404* gesehen werden [75, S. 1]. In diesem Kontext wurde das COSO Modell 2004, unter besonderer Berücksichtigung der Anwendbarkeit für ein unternehmensweites Risikomanagement (ERM) überarbeitet.[81]

COSO-ERM versteht sich allgemein als dreidimensionales Modell [3, S. 49]. Die erste Dimension beinhaltet vier Zielkategorien, welche mit acht Aktivitäten der zweiten Dimension im direkten Verhältnis zueinander stehen [3, S. 49]. In der dritten Dimension werden vier allgemeine Unternehmensbereiche dargestellt. Das IKS ist damit für einzelne Geschäftsbereiche oder das gesamte Unternehmen relevant [3, S. 49]. Es gibt eine direkte Beziehung zwischen Zielen, die wiedergeben, was eine Organisation erreichen will, und Komponenten des unternehmensweiten Risikomanagements, die wiedergeben, was zu ihrem Erreichen erforderlich ist [21, S. 23]. Diese Beziehungen werden in Form eines Würfels dargestellt [21, S. 7].

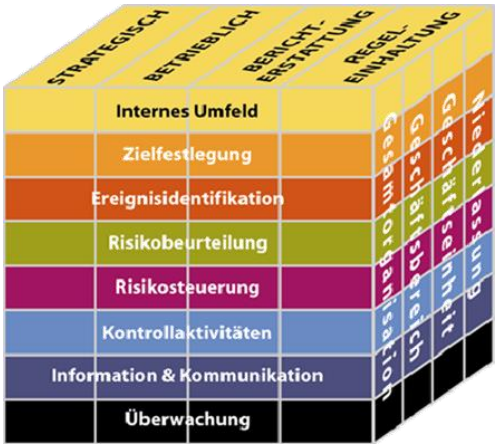

Abbildung 18: COSO-Würfel[82]

Die vier Zielkategorien - strategisch, betrieblich, Berichterstattung und Regeleinhaltung – welche in den vertikalen Spalten zu finden sind [21, S. 23] und die erste Dimension darstellen beziehen sich auf folgende Ziele[83]:

[81] Siehe dazu die Bemerkungen im *Foreword* in [4]
[82] Quelle: [21, S. 7]
[83] In Anlehnung an [4, S. 5]

1. **Strategisch:** Definition und Einhaltung von „high-level“ Zielen zur Unterstützung der Mission.
2. **Betrieblich:** Sicherstellung des effektiven und effizienten Einsatzes der Ressourcen.
3. **Berichterstattung:** Zuverlässigkeit der Finanzberichterstattung.
4. **Regeleinhaltung:** Einhaltung der geltenden Gesetze und Vorschriften (Compliance)

Die zweite Dimension enthält die Aktivitäten des ERM, auf welche in der Folge kurz eingegangen wird.

- **Internes Kontrollumfeld:** Diese Komponente stellt die Basis für alle weiteren Komponenten des ERM dar und umfasst die Festlegung der Strategie und Ziele des Unternehmens sowie die Identifikation, Beurteilung und Steuerung von Risiken [3, S. 468], [21, S. 27].
- **Zielfestlegung:** Mit der Festlegung von Zielen wird die Voraussetzung für die Ereignisidentifikation sowie die Beurteilung und Steuerung von Risiken hergestellt. Im ersten Schritt werden strategische Ziele festgelegt, welche die Ausgangsbasis für die Unterziele darstellen [3, S. 469], [21, S. 35].
- **Ereignisidentifikation:** Hierzu zählt die Identifikation von Ereignissen, die sich positiv (als Chance) oder negativ (als Risiko) auf das Unternehmen auswirken [3, S. 470], [21, S. 41].
- **Risikobeurteilung:** Ereignisse werden im Hinblick auf Ihre Auswirkung auf die Zielerreichung beurteilt. Die Beurteilung der Ereignisse erfolgt nach ihrer Eintrittswahrscheinlichkeit und der Ergebnisauswirkung [3, S. 470], [21, S. 49].
- **Risikosteuerung:** Mit dieser Komponente werden folgende Maßnahmen zur Risikosteuerung festgelegt [21, S. 55]:
    - Risikovermeidung durch beenden von risikobehafteten Aktivitäten
    - Risikoreduktion durch Maßnahmen zur Verminderung der Eintrittswahrscheinlichkeit und/oder Ergebnisauswirkung
    - Risikoteilung, zum Beispiel durch Versicherungen oder das Outsourcing von Tätigkeiten
    - Risikoakzeptanz durch die Unterlassung jeglicher Tätigkeiten, welche das Risiko reduzieren oder vermeiden
- **Kontrollaktivitäten:** Mit Richtlinien und Verfahren wird sichergestellt, dass die Risikosteuerungsmaßnahmen tatsächlich und korrekt durchgeführt werden [3, S. 471], [21, S. 61].
- **Information und Kommunikation:** Relevante Informationen aus internen und externen Quellen werden erfasst und so kommuniziert, dass alle verantwortlichen Personen ihre Aufgaben im Rahmen des ERM wahrnehmen können. Alle betroffenen Stellen innerhalb und außerhalb des

Unternehmens müssen sämtliche notwendigen Informationen zum richtigen Zeitpunkt erhalten [3, S. 472], [21, S. 27].

- **Überwachung:** Das ERM muss laufend überprüft und gegebenenfalls verbessert werden. Im Vordergrund steht hierbei die Frage, ob das Risikomanagement- und IKS operativ effektiv ist und den Anforderungen des Unternehmens genügt [3, S. 472], [21, S. 75]. Diese Komponente wird zudem in verschiedenen gesetzlichen Vorgaben verlangt.[84]

Mit der dritten Dimension besteht die Möglichkeit, das COSO Modell auf die Gesamtorganisation oder nur bestimmte Geschäftsbereiche anzuwenden.

Das COSO Rahmenwerk beschreibt zudem Rollen und Verantwortlichkeiten in Unternehmen [4, S. 83-91]. Mit der groben Unterscheidung zwischen den internen (*Entity Personnel*) und externen (*External Parties*) Beteiligten werden unter anderem die Einflussfaktoren zwischen dem Unternehmen und der Außenwelt dargestellt. Bei der Gruppe der internen Beteiligten umfasst die Darstellung das gesamte Personal des Unternehmens und es wird davon ausgegangen, dass jede einzelne Person seinen Beitrag zum effektiven ERM leisten kann [4, S. 83]. In Abbildung 19 ist die Rollen- und Aufgabenaufteilung gemäß COSO ersichtlich.

[84] zum Beispiel gemäß §91 Abs. 2 KonTraG [62, S. 787]

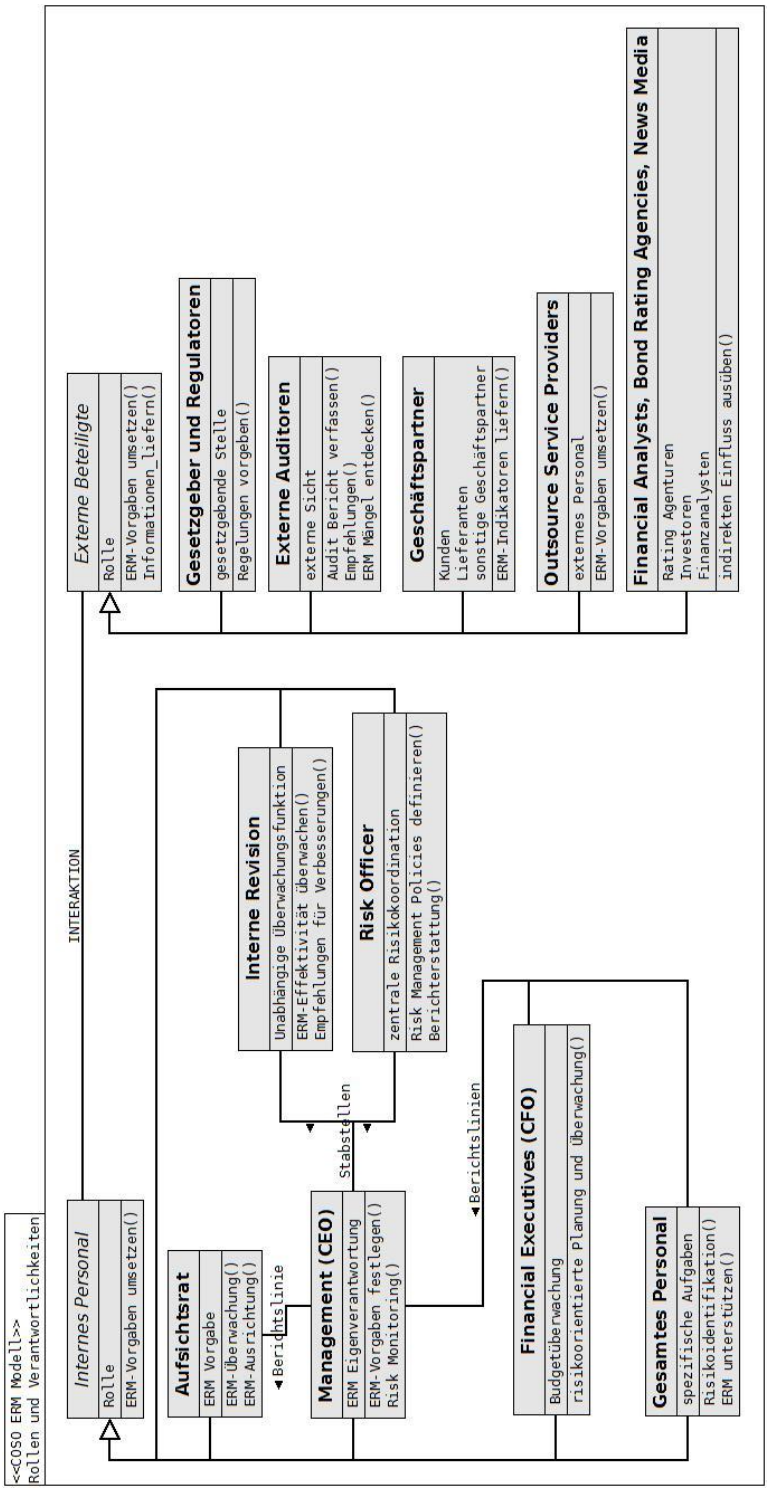

Abbildung 19: Rollen und Verantwortlichkeiten gemäß COSO Model (grober Überblick)[85]

[85] Quelle: eigene Darstellung in Anlehnung an [4, S. 83-91]

Der Bereich des internen Personals in Abbildung 19 in Verbindung mit den dargestellten ERM Aktivitäten zeigt, dass mit dem COSO ERM Rahmenwerk das IKS, die Interne Revision und das Risikomanagement in einen ganzheitlichen Ansatz eingebunden und integriert werden [3, S. 501].

4.2.2 COBIT

Der Wertbeitrag der IT in Unternehmen ist ein wichtiges Element zur Erreichung von Geschäftszielen. Der Grund dafür ist, dass eine Vielzahl an wesentlichen Geschäftsprozessen durch IT-Systeme unterstützt werden [17, S. 13], [18, S. 5]. Außerdem steigt mit der Integration von Prozessen und IT über die Unternehmensgrenzen hinaus die Komplexität von Strukturen und Abläufen [76, S. 24]. Die Risiken und Steuerung der IT, als wesentliche Bestandteile der *IT-Governance*, sind in diesem Kontext von besonderer Bedeutung.

Mit den, auf Basis von COSO entwickelten [76, S. 77], *Control Objectives for Information and Related Technology* (COBIT)[86] , steht ein umfassendes Rahmenwerk zur Verfügung, welches die Eingliederung der IT Governance in die Corporate Governance gewährleistet [17, S. 14]. Zu diesem Zweck stellt COBIT so genannte „Good Practices*"* zur Verfügung, mit welchen die Entwicklung von klaren Richtlinien für die Steuerung der IT in der gesamten Organisation ermöglicht wird [17, S. 26].

Zur Etablierung der Richtlinien wurden einige Komponenten für unterschiedliche Interessensgruppen definiert und in drei Ebenen wie folgt gegliedert[87]:

Ebene	Ausprägung	Interessensgruppe	COBIT Komponenten[88]
1	strategisch	Vorstand, Geschäftsführung, Aufsichtsrat	Board Briefing on IT-Governance
2	operativ	Linien- und IT-Management	Management Guidelines und Maturity models
3	spezialisiert[89]	Spezialisiertes Personal der Bereiche Governance, Assurance, Control und Security	Spezifische Komponenten zur Umsetzung von COBIT

Tabelle 3: Darstellung der COBIT Interessensgruppen

[86] Die Basis für die Ausführungen in diesem Abschnitt stellt die COBIT Version 5 dar [17] , zur Darlegung einzelner Fakten wird in diesem Abschnitt teilweise auch auf die Version 4.1 [18] verwiesen

[87] In Anlehnung an [18, S. 7]

[88] Auf die detaillierte Beschreibung der Komponenten, welche in COBIT 4.1 dargestellt sind [18, S. 7] wird im Rahmen dieser Arbeit verzichtet. Die Aufstellung zeigt lediglich, dass für unterschiedliche Interessensgruppen verschiedene Werkzeuge im Sinne der „Good Practices" in Form der COSO Komponenten zur Verfügung stehen

[89] Im Hinblick auf die Anwendung des COBIT Modells

Abbildung 20 zeigt den Zusammenhang der verschiedenen Elemente, die auf Basis der COSO Komponenten entstanden sind.

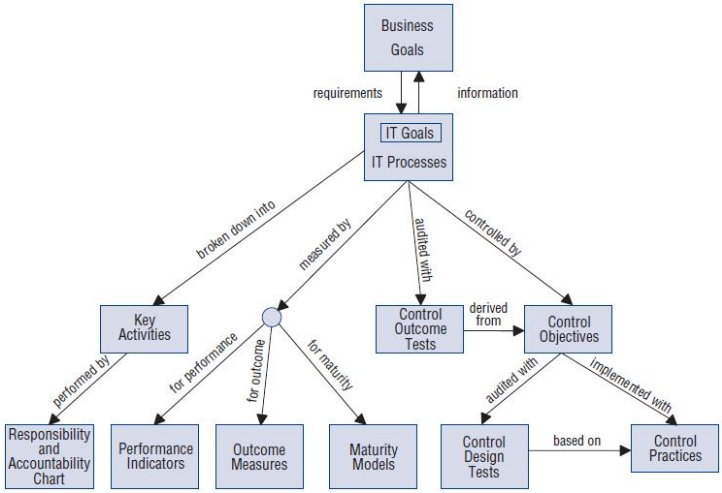

Abbildung 20: Zusammenhang der COSO Komponenten[90]

Die Grafik in Abbildung 20 verdeutlicht auf der obersten Ebene den Kontext zwischen den Zielen des Unternehmens und der IT. Von den IT Zielen ausgehend werden unterschiedliche Aktivitäten zur Einhaltung der IT Governance im Sinne von Risikosteuerung und Kontrollen dargestellt. In diesem Zusammenhang sind folgende vier Grundprinzipien von COBIT gut zu erkennen[91]:

1. Ausrichtung der IT auf die Unternehmensziele und den damit verbundenen geschäftlichen Anforderungen
2. Steuerungs- und Kontrollmaßnahmen im Hinblick auf das IT Risikomanagement
3. Orientierung an Messwerten im Sinne der konkreten Überprüfbarkeit von Zielen
4. Definition von und Orientierung an IT Prozessen

Die in Abbildung 20 dargestellten Komponenten werden durch das generische COBIT Prozessmodell unterstützt. Dieses sieht in der Version 5 insgesamt 37 Governance- und Managementprozesse vor, welche in fünf Domänen unterteilt werden [17, S. 33]. Abbildung 21 zeigt das COBIT 5 Prozess Referenzmodell mit allen Prozessen.

[90] Quelle: [18, S. 8]
[91] In Anlehnung an [87, S. 21]

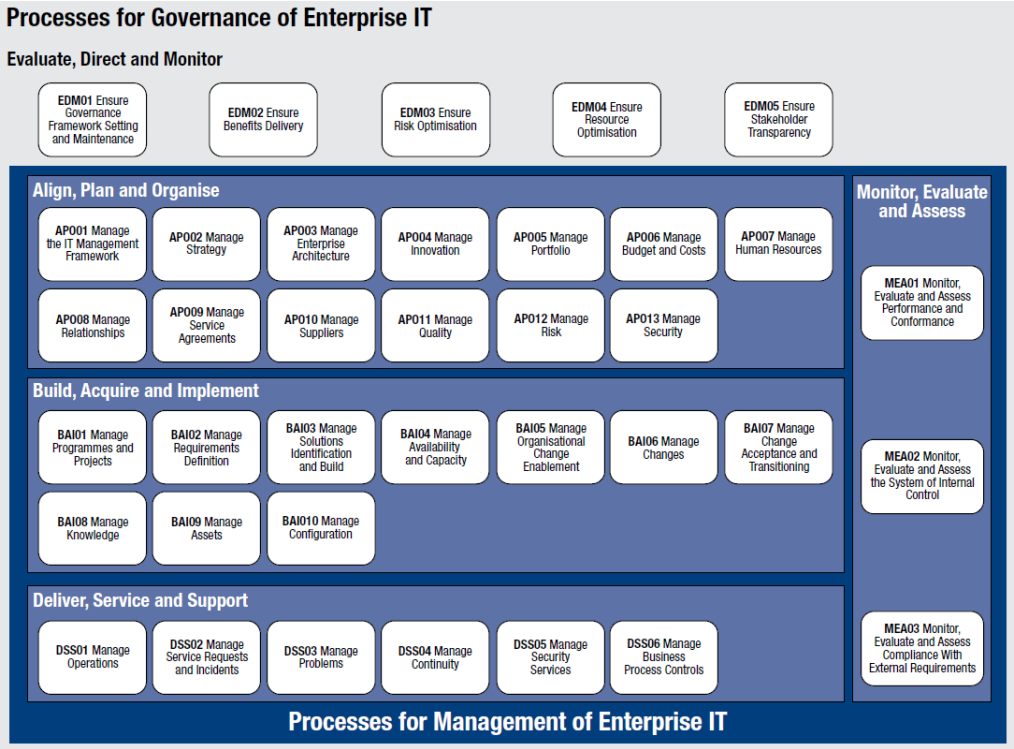

Abbildung 21: COBIT 5 – Prozess Referenzmodell[92]

Mit der *Software Process Improvement and Capability Determination (SPICE)* innerhalb der ISO/IEC 15504 Norm [77] erfolgt die Messung der Prozessfähigkeit (*Process Capability*) der definierten COBIT 5 Prozesse. Abbildung 22 zeigt das *COBIT 5 Process Capability Model* in einer stark vereinfachten Form.

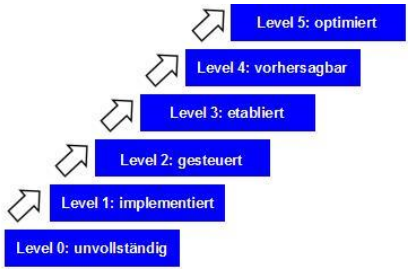

Abbildung 22: COBIT 5 Process Capability Model (stark vereinfachte Form)[93]

Die einzelnen Stufen (*Levels*) des Modells werden wie folgt interpretiert[94]:

- Level 0 *Incomplete Process*: Der Prozess ist nicht implementiert oder verfehlt das Prozessziel.

[92] Quelle: [17, S. 33]
[93] Quelle: eigene Darstellung in Anlehnung an [97]
[94] In Anlehnung an [17, S. 44], [97]

- Level 1 *Performed Process*: Der Prozess ist implementiert und erreicht das Prozessziel.
- Level 2 *Managed Process*: Der Prozess wird nun in einer kontrollierten Art und Weise umgesetzt (geplant, überwacht und angepasst). Die Prozessergebnisse werden in geeigneter Weise ermittelt, kontrolliert und aufrechterhalten.
- Level 3 *Established Process*: Der Prozess wird gesteuert und die Ergebnisse werden spezifiziert, kontrolliert und aufrechterhalten.
- Level 4 *Predictable Process*: Der Prozess wird konsistent innerhalb definierter Grenzen ausgeführt.
- Level 5 Optimising Process: Der Prozess wird kontinuierlich verbessert, um aktuelle und prognostizierte Geschäftsziele zu erreichen.

Mit der Publizierung von COBIT 5 wurden folgende fünf grundlegende Prinzipien für die Governance und das Management der IT in Unternehmen festgelegt[95]:

- Erfüllung der Bedürfnisse der Stakeholders durch die Erzielung von Mehrwerten unter Berücksichtigung der Balance zwischen der Nutzenrealisierung und Optimierung von Risiken.
- Erfassen der gesamten Unternehmensbereiche durch die Integration der IT-Governance in die Corporate Governance.
- Anwendung eines einzigen integrierten Rahmenwerkes durch die Deckung mit anderen, relevanten Standards und Frameworks auf einer hohen Ebene. COBIT 5 stellt demnach den übergreifenden Rahmen für die Leitung und Verwaltung der IT dar.
- Ermöglichung eines ganzheitlichen Ansatzes durch die Definition von so genannten *Enablers* zur Unterstützung bei der Umsetzung eines umfassenden Governance- und Managementsystems für die IT. In COBIT 5 sind folgende sieben dieser Enablers, welche helfen, Unternehmensziele zu erreichen, definiert:
    - Grundsätze, Richtlinien und Frameworks
    - Prozesse
    - Organisatorische Strukturen
    - Kultur, Ethik und Verhalten
    - Informationen
    - Services, Infrastruktur und Anwendungen
    - Menschen, Fähigkeiten und Kompetenzen
- Trennung von Governance[96] und Management durch die klare Unterscheidung von Aktivitäten, Organisationsstrukturen und Zielen. Das

[95] In Anlehnung an [17, S. 14]
[96] Siehe Abschnitt 3.6

Management setzt hierbei die Governance Vorgaben durch die Planung, Umsetzung und Überwachung von dafür erforderlichen Aktivitäten um.

Beim Vergleich von COBIT 5 mit der Vorgängerversion 4.1 fällt auf, dass sich das Rahmenwerk stark in Richtung der Corporate Governance entwickelt hat. Zudem ist, nach der Auffassung des Autors, eine stärkere Integration von Risikomanagement und IKS erkennbar. Demgemäß stellt COBIT 5 eine sehr gute Grundlage für die Abbildung des ERM dar. Für die Erstellung des Integrationsmodells[97], welches die Gesamtsicht von Organisationen abbildet ist dieser, von der IT stark geprägte, Ansatz allerdings nicht geeignet, da die Initiative für ein ERM vom Vorstand oder der Geschäftsführung ausgehen muss und, Top-Down, alle Bereiche umfasst.[98] Zudem fehlt in COBIT 5 ein detailliertes Mapping mit dem COSO Rahmenwerk was die Abbildung eines unternehmensweiten Risikomanagements erschwert.[99] Demgegenüber stellt COBIT 4.1 umfangreiche Informationen für das Mapping mit COSO [18, S. 173] zur Verfügung. Darüber hinaus existiert eine Reihe an weiteren Publikationen für das Mapping mit weiteren Normen oder Rahmenwerken[100] was COBIT 4.1, nach der Meinung des Autors, für die aktuell geeignetste Variante zur Integration der IT in das gesamte Integrationsmodell von Risikomanagement und IKS macht.

4.2.3 ITIL

Die *Information Technology Infrastructure Library* (ITIL) [73], welche vom *Office of Governance Commerce*, einer britischen Regierungsbehörde, veröffentlicht wurde beschreibt mit insgesamt fünf Büchern und einer zusammenfassenden Publikation so genannte „Good Practices“ [73, S. 4] für das IT-Service Management. Mit der konsequenten Anwendung des ITIL Rahmenwerks werden hochwertige IT-Dienstleistungen realisiert, welche die folgenden Ziele unterstützen[101]:

- Abstimmung der Services auf die Anforderungen des Geschäfts und der Nutzer
- Einhaltung von gesetzlichen Vorschriften
- Effektiv und effizient in der Serviceauslieferung sowie der Beschaffung und Planung der dafür benötigten Ressourcen
- Kontinuierliche Überprüfung und Verbesserung der Leistungen

Der kontinuierliche Verbesserungsprozess erfolgt gemäß dem so genannten *PDCA-Deming Kreis* [73, S. 13] mit den Phasen

- Plan: Erkennen vor Verbesserungspotenzialen

[97] Siehe Abschnitt fünf
[98] vgl. §22 GmbH Gesetz und §82 Aktiengesetz [10], [11]
[99] In der aktuellen Publikation von COBIT 5 [17] wird COSO lediglich zweimal als eines unter einigen anderen Rahmenwerken erwähnt
[100] vgl. zum Beispiel [74], [87]
[101] In Anlehnung an [74, S. 14]

- Do: Umsetzung der Planung
- Check: Erfolgskontrolle
- Act: Optimierung und Verbesserung sowie Beseitigung von Mängel und Schwächen

Die fünf Bücher der derzeit aktuellen Version 3 (ITIL v3) umfassen Inhalte zu den einzelnen Phasen der IT Dienstleistungen und stellen in ihrer Gesamtheit einen Lebenszyklus dar, welcher sich an der Erbringung von IT-Dienstleistungen orientiert und einen kontinuierlichen Verbesserungsprozess ermöglicht. Folgende Phasen werden in ITIL v3 beschrieben:

Phase	Titel	Inhalt	Ziel
1	Service Strategie[102]	Festlegung, welche IT-Services angeboten werden und welche internen oder externen Kunden den Service in Anspruch nehmen	Ausrichtung des Services an den Bedürfnissen der Kunden
2	Service Design[103]	Festlegung des Umfangs und Inhalts der Services gemäß den Geschäftserfordernissen inklusive der Berücksichtigung von Risiken und Gestaltung von Methoden zur Messung der Leistungserbringung	Serviceentwurf gemäß den geschäftlichen Anforderungen
3	Service Transition[104]	Sicherstellung und Bereithaltung der vereinbarten Services	Auslieferung und Inbetriebnahme der Services
4	Service Operation[105]	Eigentliche Erbringung der Services inklusive Service Level Agreements und Überwachung und Optimierung des Betriebes	Erbringung von effizienten und effektiven Services
5	Continual Service Improvement[106]	Festlegung von Maßnahmen für einen kontinuierlichen Verbesserungs-prozess wie zum Beispiel Messung der Kundenzufriedenheit oder Evaluierung und Verbesserung der Service-prozesse	kontinuierliche Verbesserung

Tabelle 4: Kurzschreibung der ITIL v3 Phasen

Abbildung 23 zeigt den ITIL Lebenszyklus inklusive der fünf Phasen, welche die einzelnen Bücher repräsentieren.

[102] Inhalt und Ziel in Anlehnung an [73, S. 25-41], [88]
[103] Inhalt und Ziel in Anlehnung an [73, S. 45-72], [89]
[104] Inhalt und Ziel in Anlehnung an [73, S. 75-89], [91]
[105] Inhalt und Ziel in Anlehnung an [73, S. 93-122], [90]
[106] Inhalt und Ziel in Anlehnung an [73, S. 125-141], [92]

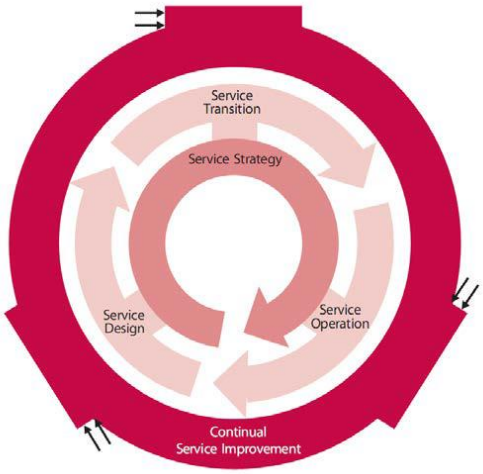

Abbildung 23: ITIL Lebenszyklus mit fünf Phasen[107]

4.2.4 Zusammenfassung der Rahmenwerke

Die dargestellten Rahmenwerke COSO, COBIT und ITIL adressieren ähnliche Ziele. Wie bereits erwähnt basiert das COBIT Rahmenwerk auf dem COSO Modell [76, S. 77]. Andererseits können zur Umsetzung von Maßnahmen spezifische ITIL Prozesse den 34 COBIT Prozessen zugeordnet werden [74, S. 7]. Zudem werden in den drei Rahmenwerken ähnliche Rollen und Verantwortlichkeiten definiert.

Mit der zusammenfassenden Darstellung in Tabelle 5 wird ein Mapping der Rahmenwerke COSO und COBIT durchgeführt. Dieses zeigt eine Bewertung der Beziehungen zwischen den COSO Aufgaben und den COBIT Prozessen. Es zeigt sich, dass COBIT im Bereich der *Kontrollaktivitäten* am stärksten durch das COSO Rahmenmodell unterstützt wird, während der Bereich der *Risikobeurteilung* den schwächsten Beziehungsgrad aufweist.

Diese grobe Sichtweise inklusive der Berücksichtigung der weiteren Unterstützung der beiden Rahmenmodelle durch ITIL sowie der Berücksichtigung von Rollen und unterstützenden Systemen stellt das Grundgerüst für das in dieser Arbeit erstellte Integrationsmodell dar.

[107] Quelle: [73, S. 19]

COSO Aufgaben	COBIT (Domänen)																																					
	Planung und Organisation (PO)											Beschaffung und Implementierung (AI)										Auslieferung und Unterstützung (DS)													Überwachung und Evaluierung (ME)				Summe
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2	AI3	AI4	AI5	AI6	AI7	DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9	DS10	DS11	DS12	DS13	ME1	ME2	ME3	ME4	
Kontrollumfeld	0	0	0	2	0	2	2	2	0	1	0	0	0	0	0	0	0	1	2	0	1	0	0	2	1	0	0	0	0	0	0	0	0	0	2	**18**
Risikobeurteilung	2	0	1	0	1	0	0	0	2	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	**11**
Kontrollaktivtäten	0	2	2	0	2	0	0	2	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	2	2	2	2	2	0	0	2	0	0	**48**
Information und Kommunikation	1	2	1	1	0	2	1	1	0	0	0	0	0	1	0	0	1	1	0	0	1	1	0	1	2	0	1	0	0	1	1	0	1	1	2	**22**
Überwachung	1	0	0	1	0	0	0	2	0	1	0	0	0	0	0	1	1	1	1	1	0	1	0	0	2	0	1	0	0	0	2	2	1	2	0	**21**

Begriffserklärung	
Starke Beziehung	2
Schwache Beziehung	1
Keine Beziehung oder marginal	0

Tabelle 5: COSO/COBIT Mapping auf Prozessebene[108]

[108] Quelle: eigene Darstellung in Anlehnung an [18, S. 173]

4.3 Normen

Dieser Abschnitt enthält die Darstellung von verschiedenen Normen, welche für das ERM von Bedeutung sind. Alle vorgestellten Normen wurden von der *Internationalen Organisation für Normung* (ISO)[109] bzw. der für Elektrik und Elektronik zuständigen *International Electronical Commission* (IEC)[110] erarbeitet.

Der Nutzen bei der Anwendung von Normen ist, dass unternehmensintern ein allgemeingültiger Leitfaden für die Umsetzung von spezifischen Aufgaben vorliegt und der Außenwelt ein Nachweis für eine standardisierte Umsetzung erbracht werden kann. Zudem stellt, nach den Erfahrungen des Autors, die Anwendung von Normen in der Außenwirkung eines Unternehmens einen anerkannten Qualitätsfaktor dar.

Im Zuge der Recherchen für die vorliegende Arbeit wurden die für das ERM anwendbaren Normen ISO/IEC 27001:2005 [12], ISO/IEC 27005:2008 [14] sowie ISO 31000:2009 [15] identifiziert, welche in der Folge dargestellt werden.

4.3.1 ISO/IEC 27001:2005

Im Vordergrund der ISO/IEC 27001:2005 Norm [12] steht der Begriff eines Managementsystems für die Informationssicherheit (ISMS für Information Security Management System). Die Norm gibt, ähnlich wie bei COBIT vor, *was* zur Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines ISMS umgesetzt werden muss [12, S. v]. Dabei gelangt die Methode *Plan, Do, Check, Act* (PDCA) zur Anwendung, welche in Abbildung 24 als Schema dargestellt ist.

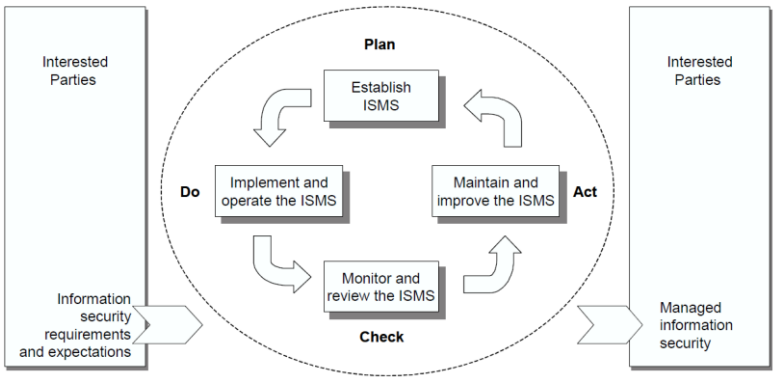

Abbildung 24: PCDA Modell der ISO/IEC 27001:2005[111]

[109] http://www.iso.org/ [Zugriff am 22.2.2013]
[110] http://www.iec.ch/ [Zugriff am 22.1.2013]
[111] Quelle: [12, S. vi]

Die bewährte PDCA Methode wurde von der ISO 9001:2008 Norm [78, S. vi] abgeleitet und stellt sich in der ISO/IEC 27001:2005 Norm wie folgt dar:

Phase	ISMS-Aufgabe	ISMS-Inhalt	Ergebnis
Plan	etablieren	• Umfang und Grenzen definieren • Allgemeine Richtlinie festlegen • Risikobewertungskonzept definieren • Risiken identifizieren, bewerten und Kontrollziele festlegen	Allgemeine Angaben zu Schutzzielen und Steuerung von Risiken
Do	implementieren und betreiben	• Risikosteuerungsverfahren inklusive Zuteilung von Verantwortungen definieren • Kontrollaktivitäten implementieren • Effektivität der Kontrollen messbar machen • Betrieb und Ressourcen steuern • Verfahren für Sicherheitsvorfälle definieren	Konkrete Angaben zum Betrieb und zur Risikosteuerung
Check	überwachen und überprüfen	• Überwachungs- und Überprüfungsaktivitäten durchführen • Regelmäßige Überprüfung der Effektivität inklusive Messen der Wirksamkeit von Kontrollen • Überprüfung der Risikobewertungen • Ereignisse, die eine Auswirkung auf die Effektivität und Performance haben könnten, dokumentieren	Dokumentation und Umsetzung der Kontrollaktivitäten
Act	aufrechterhalten und verbessern	• Identifizierte Verbesserungsmaßnahmen umsetzen • Vorbeugenden und korrektive Maß-nahmen umsetzen • Verbesserungsmaßnahmen kommunizieren • Sicherstellung, dass die Verbesserungsmaßnahmen zum angestrebten Ziel führen	Dokumentation und Umsetzung von verbessernden Maßnahmen inklusive Überprüfung der Wirksamkeit

Tabelle 6: Darstellung der ISO/IEC 27001:2005 PCDA Methode

Wie aus dem Namen *ISMS* abzuleiten ist wird mit der ISO/IEC 27001:2005 Norm das Thema *Informationssicherheitsmanagement* fokussiert. Konkrete Handlungsanleitungen zur Umsetzung der Norm sind in der ISO/IEC 27001:2005 Dokumentation nicht enthalten [79, S. 9]. Das *deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI)* hat daher mit dem *BSI-Standard 100-1* (Managementsysteme für die Informationssicherheit) [79] eine allgemein gültige

Vorgangsweise für den Aufbau des ISMS veröffentlicht. Dieser Standard sieht, unter anderem, folgende Kategorien des ISMS vor[112]:

- Übergeordnete Aspekte, welche zum Beispiel die Organisation oder das Personal betreffen
- Infrastruktur in Form von Gebäuden oder Räumlichkeiten des Rechenzentrums
- Hardware der IT-Systeme wie zum Beispiel Server, Clients oder Netzkomponenten
- IT-Netzwerk inklusive der Aktivitäten des Systemmanagements
- IT-Anwendungen

Im Anhang A der Norm werden mit der Beschreibung von Kontrollen und Kontrollzielen konkrete Maßnahmen für spezifische Bereiche des ISMS vorgegeben [12, S. 13-29]. Für die Umsetzung dieser Vorgaben wird auf die ISO 27002 Norm referenziert [13], welche eine Sammlung an Empfehlungen für diese Maßnahmen enthält.

4.3.2 ISO/IEC 27005:2008

Mit der ISO/IEC 27005:2008 Norm [14] werden Vorgaben zum Risikomanagement in der Informationssicherheit definiert. Zudem werden die Anforderungen an ein ISMS nach ISO/IEC 27001:2005 [12] unterstützt.

Das zentrale Element der ISO/IEC 27005 Norm ist der Risikomanagementprozess in Bezug auf die Informationssicherheit, welcher durch umfassende Begriffserklärungen unterlegt wird [14, S. 1-2]. Der Prozessablauf zeigt in weiten Teilen große Ähnlichkeiten zur Vorgangsweise der Risikosteuerung des COSO II Rahmenwerkes.[113] Der Detaillierungsgrad ist jedoch durch die Einfügung von zwei Risikoentscheidungspunkten höher.

Abbildung 25 veranschaulicht die grundlegenden Elemente des Risikomanagementprozesses nach ISO/IEC 27005.

[112] In Anlehnung an [79, S. 37]
[113] Siehe Abbildung 18

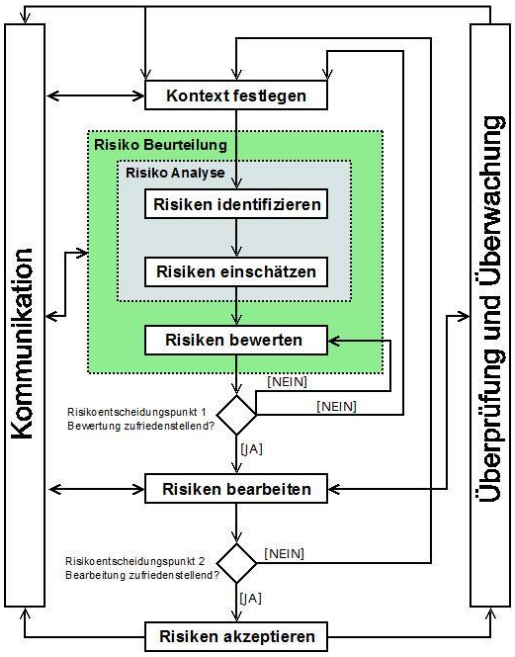

Abbildung 25: Risikomanagementprozess nach ISO/IEC 27005:2008[114]

Im Anhang der Norm [14, S. 39-40] werden zudem zur Hilfestellung umfangreiche Anleitungen für die Bedrohungsanalyse dargestellt indem einzelne Szenarien beschrieben und wie folgt klassifiziert werden:

- Vorsätzlichkeit wie zum Beispiel Diebstahl, Manipulationen von Hard- und/oder Software und dergleichen
- Versehentliche oder unbeabsichtigte Ereignisse, welche zu Schäden führen
- Umwelteinflüsse, zum Beispiel bedingt durch Naturkatastrophen

Der dargestellte Risikomanagementprozess ist universell verwendbar und kann für eine Organisation als Ganzes, einzelne Bereiche, ein spezifisches Informationssystem oder bestimmte Aspekte, wie zum Beispiel der Notfallplanung, angewandt werden [14, S. 4].

4.3.3 ISO 31000:2009 - Risiko Management

Die ISO 31000:2009 Norm [15] definiert Vorgaben für das Risikomanagement und behandelt alle Arten von Abweichungen im Sinne einer positiven oder negativen Auswirkung [3, S. 493], [5, S. 60]. Die Rahmenbedingungen sind jenen des COSO-ERM Modells [4] sehr ähnlich und beinhalten ebenso das unternehmensweite

[114] Quelle: eigene Darstellung in Anlehnung an [14, S. 5 ff]

Risikomanagement. Der nachfolgende Vergleich der ISO 31000:2009 mit dem COSO II ERM Rahmenwerk verdeutlicht die Ähnlichkeit[115]:

COSO Komponente	Korrespondierende Prozesse nach ISO 31000:2009
Internes Umfeld Information & Kommunikation	Kommunikation und Konsultation
Internes Umfeld Zielfestlegung	Erstellen des Zusammenhangs
Ereignisidentifikation Risikobeurteilung	Risikobeurteilung durch • Risikoidentifikation • Risikoanalyse • Risikobewertung
Risikosteuerung Kontrollaktivitäten	Risikobewältigung
Überwachung	Überwachung und Überprüfung

Tabelle 7: Vergleich COSO II Rahmenwerk und ISO 31000:2009

Es sind demnach keinerlei Neuerungen oder Ergänzungen zu COSO erkennbar, was den Schluss zulässt, dass bei konsequenter Anwendung des COSO Rahmenwerkes die Bedingungen der ISO 31000:2009 Norm ebenso erfüllt werden [3, S. 497]. Zur Veranschaulichung werden in Abbildung 26 die Elemente und Prozesse der Norm dargestellt.

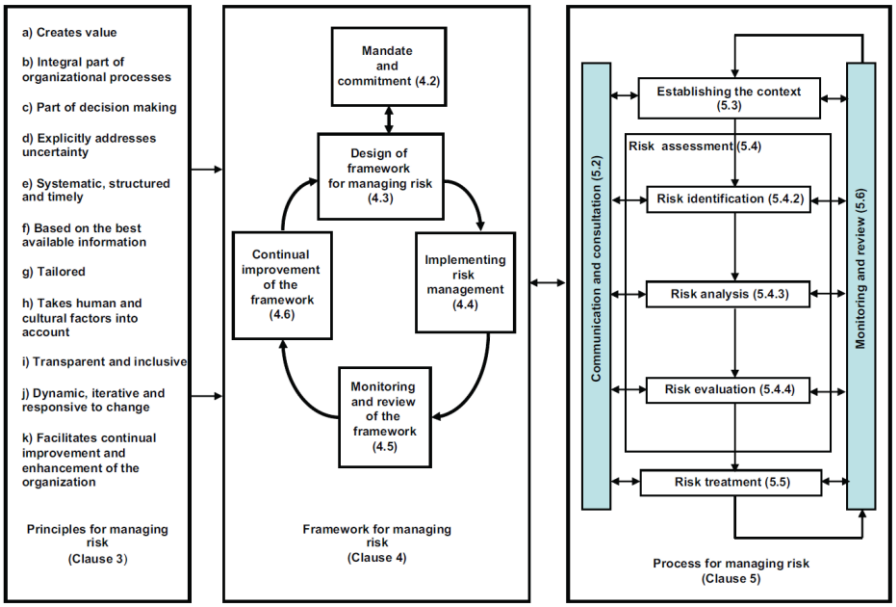

Abbildung 26: ISO 31000:2009 Rahmenwerk[116]

[115] In Anlehnung an [3, S. 496]
[116] Quelle: [15, S. vii]

Der Risikomanagementprozess [15, S. 14] orientiert sich sehr stark an der ISO/IEC 27005:2008 Norm indem auch hier im ersten Schritt ein allgemeiner Kontext festgelegt wird und anschließend Methoden zur Risikobewertung und -behandlung dargestellt sind. Inhaltlich werden jedoch ein allgemeiner gehaltenes Risikomanagement Rahmenwerk sowie ein dazu passender Prozess zur Umsetzung definiert.

Die ISO/IEC 31000:2009 Norm versteht sich als generischer Standard [5, S. 62] und es wurde darauf geachtet, dass die Inhalte nicht zu technisch und detailliert sind [3, S. 497], sodass ein breiter Anwendungsbereich gewährleistet werden kann.

4.3.4 Zusammenfassung der Normen

Die in diesem Abschnitt vorgestellten und einander ergänzenden Normen der Reihe ISO 27000 stellen die Grundlage für ein Informationssicherheitsmanagementsystem dar, während die ISO 31000 Norm den Ansprüchen eines generellen Risikomanagementansatzes genügt. Abbildung 27 zeigt den Zusammenhang der erwähnten Normen als grobe Übersicht.

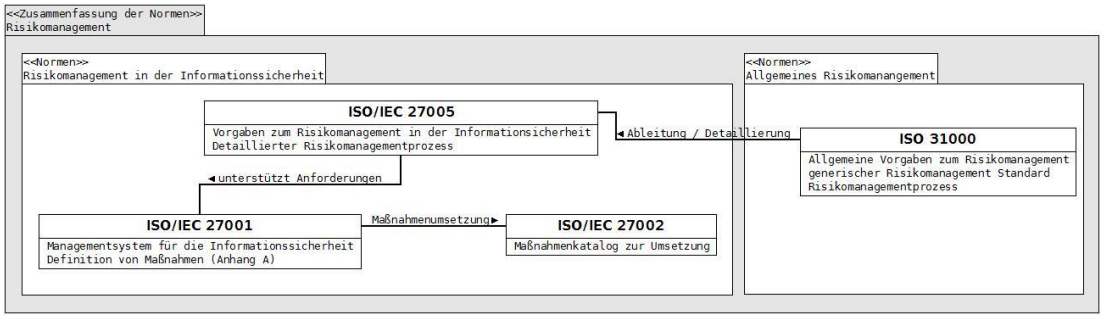

Abbildung 27: Zusammenhang der ISO 27000 Familie und der ISO 31000 Norm (grobe Übersicht)[117]

Die ISO/IEC 27005 Norm unterstützt durch detaillierte Vorgaben in Bezug auf den Risikomanagementprozess die Anforderungen an ein Managementsystem für die Informationssicherheit im Sinne der ISO/IEC 27001. Die ISO/IEC 27002 steht in Beziehung zur ISO/IEC 27001 Norm indem ein Maßnahmenkatalog für die Umsetzung des Managementsystems für die Informationssicherheit zur Verfügung gestellt wird. Die Beziehung zwischen den Normen ISO 31000 und ISO/IEC 27005 zeigt, dass die allgemeinen Vorgaben an das Risikomanagement in beiden Normen enthalten sind und in der ISO/IEC 27005 Norm detailliert werden.

[117] Quelle: eigene Darstellung

5 Integrationsmodell

Dieser Abschnitt umfasst die Erstellung des Integrationsmodells für Risikomanagement und IKS inklusive der Anforderungen an die ausführenden Systeme. Die Vorgangsweise orientiert sich hierbei an den Ausführungen zum semantischen Objektmodell und der axiomatischen Modellbildung in Abschnitt zwei. Zudem werden die Begriffsdefinitionen in Abschnitt drei sowie die ERM Rahmenbedingungen, welche in Abschnitt vier dargestellt wurden, berücksichtigt. In der Folge werden die statischen Aspekte des Modells dargestellt.

5.1 Integrationsmodell – Mapping von Risikomanagement und Internen Kontrollsystem

Abbildung 28 zeigt ein grobes Zielschema mit den für die Modellierung notwendigen Aktivitäten in jeder Ebene.

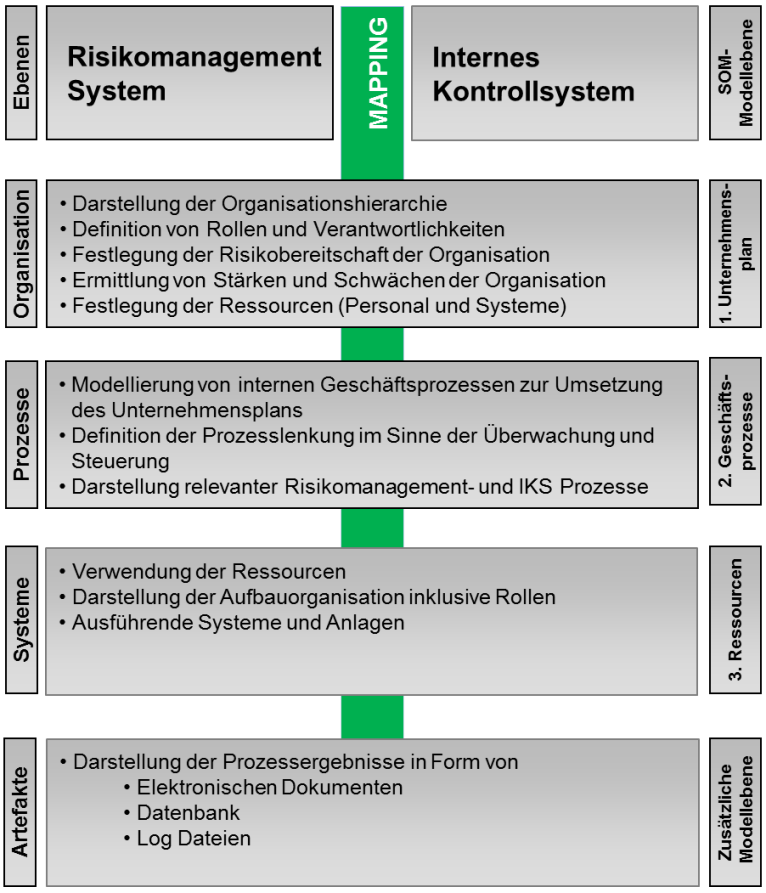

Abbildung 28: Grobstruktur des Integrationsmodells[118]

[118] Quelle: eigene Darstellung

Das Ziel bei der Modellbildung ist das Mapping von Risikomanagement- und Internem Kontrollsystem auf allen, in Abbildung 28, dargestellten Ebenen. Abbildung 29 veranschaulicht das Integrationsvorhaben im Überblick.

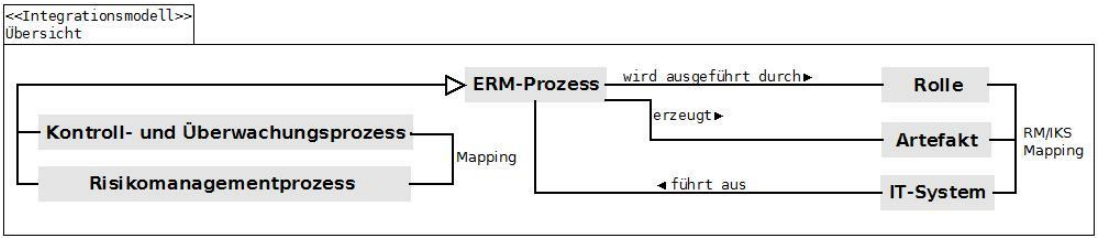

Abbildung 29: Mapping von Risikomanagement und IKS durch das Integrationsmodell[119]

In den folgenden Abschnitten wird die vom Autor gewählte allgemeine Vorgangsweise zur Erstellung des Modells dargestellt. Zudem erfolgen anhand dieser Vorgehensweise die konkrete Modellierung der einzelnen Ebenen sowie die Zusammenfassung zu einem Integrationsmodell.

5.1.1 Vorgangsweise

Im ersten Schritt werden die in Abschnitt drei beschriebenen Begriffe wie folgt harmonisiert (vereinfachte Darstellung):

- Das *Enterprise Risk Management (ERM)* umfasst die Steuerung der unternehmensweiten Risiken.
- Das *Risikomanagement* ist Teil des ERM und befasst sich nur mit der Identifikation, Beurteilung und Steuerung von Risiken.
- Das *Interne Kontrollsystem* prüft, ob die Steuerung der Risiken tatsächlich vorgenommen wird.

Abbildung 30 zeigt die Harmonisierung der Begriffe in einer, stark vereinfacht dargestellten, Form.

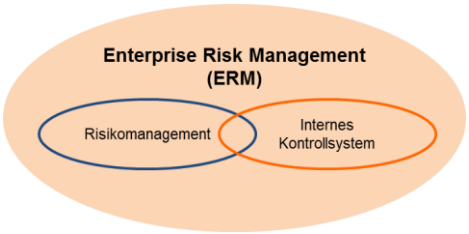

Abbildung 30: Integration von ERM, Risikomanagement und IKS[120]

[119] Quelle: eigene Darstellung
[120] Quelle: eigene Darstellung

Zur Erlangung der notwendigen Fakten auf Detailebene wurden die verwendeten Rahmenwerke und Normen eingehend analysiert und die, nach den Einschätzungen des Autors, wesentlichsten Elemente in Tabellenform gebracht. Die Modellierung erfolgte unter Zuhilfenahme dieser Elemente und, zusätzlich identifizierten, Aspekten zur Darstellung des Zusammenwirkens von Risikomanagement und IKS. Abbildung 31 zeigt das beschriebene Vorgehen in grafischer Form.

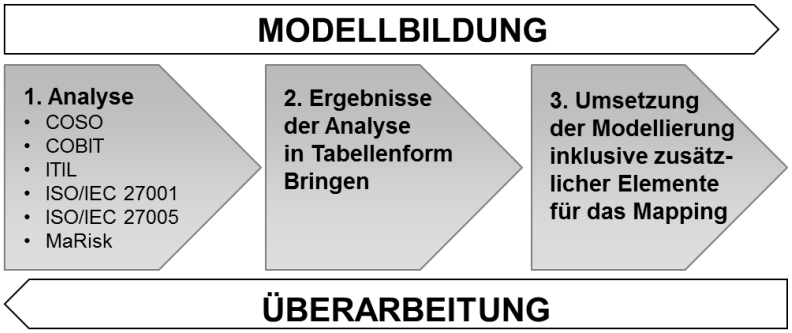

Abbildung 31: Vorgansweise zur Modellbildung[121]

Die zur Umsetzung der dargestellten Vorgangsweise notwendige Analyse der Rahmenmodelle und Normen wurde wie folgt vorgenommen:

- Analyse sowie Hervorhebung der relevanten Teile für Rollendefinitionen und Prozesse.
- Prüfung von Überschneidungen und Ergänzungen durch Abgleich von Rollen und Prozessen.
- Analyse, welche Rollen und Prozesse für die Bereiche Risikomanagement und IKS zusammengeführt werden können.
- Spezielle Betrachtung der IT durch eine detaillierte Analyse der COBIT Rollen und Prozesse.
- Vereinheitlichung von Begriffen und Konzepten, um den Anspruch der allgemeinen Gültigkeit gerecht zu werden.
- Überlegungen, welche IT-Systeme die identifizierten Risikomanagement- und IKS Prozesse ausführen.
- Allgemeine Betrachtung und Darstellung der, durch die ausführenden Systeme und Prozesse erstellten Artefakte.

Für die Bildung des Integrationsmodells wurden die Inhalte der Rahmenwerke COSO II [16], [4], [21], COBIT [18], [17], und ITIL [73] (nicht detailliert) sowie die Normen ISO/IEC 27001/5 [12], [14] und die MaRisk [54] herangezogen. Die Ausgangsbasis der Überlegungen zur Modellierung stellte die COSO II Struktur dar. Diese Sichtweise wurde in der Folge durch die, nach den Einschätzungen des

[121] Quelle: eigene Darstellung

Autors, wesentlichen Elemente der übrigen genannten Rahmenwerke und Normen ergänzt. Zuerst wurden die Rollen und Verantwortlichkeiten identifiziert und analysiert. Im Zuge dieser Analyse wurden jeder Rolle konkrete Aufgaben zugeteilt. Die Wahrnehmung der Aufgaben erfolgt durch die Umsetzung von Prozessen. Die identifizierten Aufgaben stellen daher die Basis für die abgeleiteten Prozesse dar. In der Folge wurden Systeme identifiziert, welche die Prozesse ausführen und Artefakte, die durch die Ausführung der Prozesse erzeugt werden. Abbildung 32 zeigt die eben erwähnte Vorgangsweise in grafischer Form.

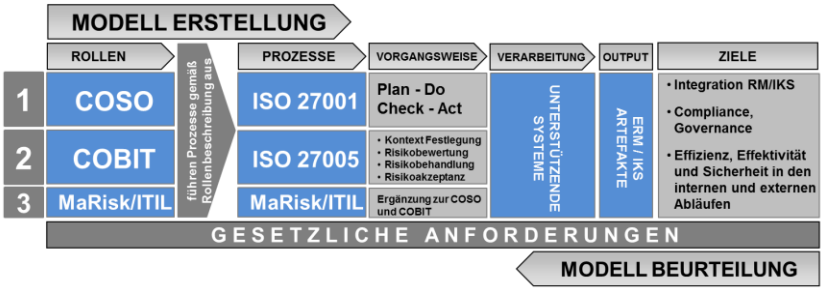

Abbildung 32: Komponenten/Elemente des Integrationsmodells[122]

Das entwickelte Integrationsmodell erhebt keinen Anspruch auf Vollständigkeit auf Detailebene, sondern zeigt eine generalisierte und allgemein gültige Darstellung der wesentlichen Elemente. Je nach Ausprägungsgrad und Anwendungsfall kann das Modell im Bedarfsfall durch die Hinzunahme von weiteren Detailbetrachtungen erweitert werden.

In den folgenden Abschnitten wird anhand der beschriebenen Vorgangsweise die Modellierung der einzelnen Ebenen durchgeführt.

5.1.2 Ebene Organisation

In dieser Ebene werden im Wesentlichen die Rollen und Verantwortlichkeiten betrachtet und in Form einer, für Risikomanagement und IKS geeigneten Aufbauorganisation dargestellt. Zudem werden je Rolle Aufgaben definiert, welche die Basis für die Identifikation von Risikomanagement und IKS Prozesse darstellen.

Im ersten Schritt wurden die Rollen und Verantwortlichkeiten von COSO II analysiert und tabellarisch mit folgenden Komponenten dargestellt: [123]

- Die Spalte *Rolle* umfasst die in COSO II allgemein definierten Rollen samt den dazu gehörenden Ausprägungen.
    - Die Rolle Management besteht demnach zum Beispiel aus dem Vorstand/Geschäftsführung und dem Senior Management.

[122] Quelle: eigene Darstellung
[123] Siehe dazu die Ausführungen zu Rollen und Verantwortlichkeiten in [21, S. 82-91]

- In der Spalte *Aufgaben und Verantwortlichkeiten* sind die, nach der Auffassung des Autors, wesentlichen Aktivitäten innerhalb einer Organisation, welche mit einer Referenznummer versehen sind, den Rollen zugeordnet.
- Die Spalte COSO Komponente zeigt, welcher Phase des COSO Modells die jeweilige Aufgabe zugeordnet wird.
- In den Spalten *ERM* und *IKS* wird anhand eines Mappings dargestellt, welche Aktivitäten im Sinne des Risikomanagements und IKS miteinander verbunden sind. Die grüne Unterlegung weist auf Aktivitäten des ERM hin, während die blauen Felder IKS Aufgaben hervorheben. Einer ERM Aufgabe muss jeweils eine IKS Aktivität zugeordnet sein und umgekehrt. Die Referenznummern zeigen jeweils auf die zugeordneten Aufgaben.
- Die Spalte *RACI*[124] weist auf das Verständnis der Rollen und Verantwortlichkeiten hin. Die Abkürzung *RACI* steht hierbei für folgende Begriffe:
    - *Responsible* definiert die Zuständigkeit für die Durchführung von Aktivitäten.
    - *Accountable* bedeutet verantwortlich und definiert, dass die Rolle die Richtung vorgibt, Aktivitäten genehmigt, die Letztverantwortung trägt und rechenschaftspflichtig ist.
    - *Consulted* heißt, dass die Rolle zur Ausführung der Aktivität hinzugezogen wird und den Prozess unterstützt.
    - *Informed* weist darauf hin, dass die Rolle über die Aktivität in Kenntnis gesetzt wird und den Prozess unterstützt.

Das Mapping der ERM- und IKS Aufgaben gibt Aufschluss über die Absicherung durch das IKS von Aufgaben, welche im Risikomanagement definiert sind. Zudem wird aufzeigt, welche Rollen Risikomanagement- und Überwachungstätigkeiten wahrnehmen. In der Folge werden die Details der einzelnen Ebenen dargestellt und kurz analysiert.

Tabelle 8 zeigt die Verantwortungsbereiche des Aufsichtsrates (AR)[125] und des Managements[126]. Eine der wichtigsten Aufgaben des Aufsichtsrates ist die Bestellung der Mitglieder des Vorstandes. Hier wird bereits ein wichtiger Schritt im Risikomanagement gesetzt indem geeignete Personen ausgewählt werden. Durch seine allgemeinen Aufsichtstätigkeiten wird diesbezüglich festgestellt, ob richtige Entscheidungen getroffen wurden [21, S. 82]. Die Aufgaben des Aufsichtsrates im Kontext mit dem ERM und IKS betreffen hauptsächlich strategische Punkte, wie zum Beispiel die Risikobereitschaft oder den Umfang des Risikomanagements.

Der in COSO II definierte Bereich des Managements umfasst die Rollen des *Chief Executive Officers (CEO)* und des *Senior Managements (SM)* [4, S. 9]. Das

[124] In Anlehnung an COBIT 4.1 [18, S. 15]
[125] Siehe dazu die Ausführungen in [21, S. 82-83]
[126] Siehe dazu die Ausführungen in an [21, S. 83-85]

Management ist direkt für alle Aktivitäten des Unternehmens verantwortlich, einschließlich des unternehmensweiten Risikomanagements (ERM)[127]. Die leitenden Führungskräfte, welche in der Tabelle als Senior Management bezeichnet werden, tragen die Verantwortung für den Umgang mit Risiken, welche mit den Zielen ihres Unternehmensbereiches verbunden sind[128]. Das IKS- und ERM Mapping in diesem und den folgenden Bereichen verweist auf Aktivitäten, welche in den zusätzlichen Ebenen dargestellt werden. Bei der Gesamtansicht in Tabelle 11 ist dieser Zusammenhang direkt sichtbar.[129]

[127] vgl. [21, S. 83]
[128] vgl. [21, S. 84]
[129] Die Mapping Tabellen in Abschnitt 5.1 umfassen insgesamt knapp 250 Zeilen und veranschaulichen die Vorarbeit zur Erstellung des Integrationsmodells. Da die primäre Aufgabenstellung der vorliegenden Arbeit die Modellentwicklung ist, werden die Mapping Tabellen nur zur Übersicht dargestellt.

Rolle	Aufgaben und Verantwortlichkeiten	#	COSO Komponente: Internes Umfeld	Zielfestlegung	Ereignis-identifikation	Risiko-bewertung	Risikosteuerung	Kontroll-aktivitäten	Information & Kommunikation	Überwachung	ERM: RACI	ERM: IKS Mapping	IKS: RACI	IKS: ERM Mapping
Aufsichtsrat	hat Kenntnis über den Umfang des Risikomanagements	CS.1								●	A/I	CS.4 CS.5		
	hat Kenntnis über die Risikobereitschaft	CS.2								●	A/I	CS.6		
	hat Kenntnis über die signifikanten Risiken	CS.3								●	A/I	CS.7		
	überprüft das Risikoportfolio	CS.4								●			A	CS.1
	wiegt das Risikoportfolio gegen die Risikobereitschaft ab	CS.5								●			A	CS.2
	stimmt der Risikobereitschaft zu	CS.6								●			A	CS.2
	prüft die Steuerung der signifikanten Risiken durch das Management	CS.7								●			A	CS.3
Management: Vorstand Geschäftsführung (CEO)	CEO verantwortet das unternehmensweite Risikomanagement durch:	CS.CEO	●	●	●	●	●	●	●	●	A/R	[1]	A/R	[1]
	* Festlegung und Abstimmung der Risikobereitschaft und Risikotoleranzen	CS.8	●	●							A/R	CS.6		
	* Erstellung des Risikoportfolios	CS.9		●							A/R	CS.4		
	* Festlegung der Risikomanagement Philosophie und Verhaltenskodex	CS.10	●								A/R	CS.6		
	* Definition und Überwachung der signifikanten Risiken	CS.11			●			●		●	A/R	CS.7		
	* Festlegung der Strategieziele und Steuerung und Kontrolle des Senior Managements	CS.12		●						●	A/R		A/R	CS.14 CS.15 CS.16 CS.17
	CEO stellt sicher, dass alle ERM Komponenten vorhanden sind	CS.13	●								A/R	CS.47		
Management: Senior Manager (SM)	SM pflegt den Umgang mit Risiken, die mit den verantworteten Zielen zusammenhängen	CS.14			●	●	●	●	●	●	A/R	CS.12		
	SM steuert die Elemente des Risikomanagements im verantworteten Bereich	CS.15			●	●	●	●	●	●	A/R	CS.12		
	SM stellt die Einhaltung der definierten Risikotoleranz sicher	CS.16			●	●	●	●	●	●	A/R	CS.12		
	SM hat Rechenschaftspflicht gegenüber der nächsthöheren Ebene	CS.17		●							R	CS.12		

[1] Zusammenfassung zu einer Referenznummer

Tabelle 8: COSO II: Verantwortungsbereich - Aufsichtsrat und Management[130]

[130] Quelle: eigene Darstellung in Anlehnung an [21, S. 82-85], [4, S. 83-86], [16, S. 95-100]

In Tabelle 9 ist der übrige Bereich des verblebenden internen Personals zusammengefasst. Die Führungskräfte des Finanz- und Rechnungswesens, welche auch zum Management zählen, werden, nach den Einschätzungen des Autors, aufgrund ihrer besonderen Aufgaben, einer eigenen Kategorie zugewiesen. In der Folge werden die einzelnen Gruppen des verbleibenden internen Personals beschrieben.

- Führungskräfte des Finanz- und Rechnungswesens[131]: Die Hauptaufgaben bestehen aus der Budgeterstellung und Überwachung sowie der Analyse und Verfolgung der Performance in Hinblick auf die Erreichung von betriebswirtschaftlichen Kennzahlen sowie Compliance- und Berichterstattungsperspektiven.

  Ein besonders wichtiger Punkt ist die Gleichstellung mit dem übrigen Seniormanagement und eine weitgehende Unabhängigkeit von internen und externen Einflüssen, welche die Tätigkeiten dieser Rollen einengen.

- Risikomanagement: Eine Ausprägung dieser Rolle ist der so genannte *Chief Executive Officer*, welcher eine zentrale Koordinationsstelle zur Unterstützung des unternehmensweiten Risikomanagements repräsentiert [21, S. 85].

- Interne Revision[132]: Diese stellt durch die laufenden Prüfungstätigkeiten fest, ob das unternehmensweite Risikomanagement funktionsfähig ist. Außerdem ergeben sich aus den Erkenntnissen der Prüfungsergebnisse Empfehlungen für Verbesserungsmaßnahmen.

- Sonstiges Personal[133]: Dieses besteht aus den Fachkräften des Unternehmens. Teilweise werden in diesen Positionen auch Führungsaufgaben wahrgenommen. Dieser Teilbereich ist vor allem für die Identifikation von Risiken und Durchführung von Kontrollaktivitäten zuständig. Falls mit diesen Positionen mit Führungsaufgaben verbunden sind können diese Tätigkeiten auch delegiert werden.

[131] In Anlehnung an [21, S. 86-87]
[132] In Anlehnung an [21, S. 87-88]
[133] In Anlehnung an [21, S. 88]

Rolle	Ausprägungen	Aufgaben und Verantwortlichkeiten	#	COSO Komponente: Internes Umfeld	Zielfestlegung	Ereignis-identifikation	Risiko-bewertung	Risikosteuerung	Kontroll-aktivitäten	Information & Kommunikation	Überwachung	ERM: RACI	ERM: IKS Mapping	IKS: RACI	IKS: ERM Mapping
Führungskräfte im Finanz- und Rechnungswesen	Leitung Finanzen (CFO) Leitung Controlling Leitung Rechnungswesen	erstellen und planen das Budget inklusive Risiken und Chancen	CS.18		●	●	●	●			●	A/R	CS.19		
		überwachen die Performance (betrieblich, gesetzlich, Berichterstattung)	CS.19								●			A/R	CS.18
		verhindern manipulative Berichterstattung und decken Unregelmäßigkeiten auf	CS.20								●			R	CS.18
		überwachen und überprüfen beschlossene Maßnahmen im Hinblick auf:	CS.CFO						●		●	A/R	[2]	A/R	[2]
		* betriebswirtschaftliche Zieldefinitionen	CS.21						●		●	R	CS.21	R	CS.18
		* Strategieentscheidungen	CS.22						●		●	R	CS.22	R	CS.8
		* Risikoanalysen	CS.23						●		●	R	CS.23	R	CS.11
Risikomanagement	Risk Officer (CRO)	entwickelt die Grundsätze des Risikomanagements	CS.24	●		●						R	CS.CEO		
		entwickelt einen Rahmen von Befugnissen	CS.25	●								R	CS.CFO		
		fördert die Risikomanagement Kompetenz	CS.26	●								R	CS.CEO		
		Integriert das ERM in Management- und Geschäftsplanungsprozesse	CS.27	●								R	CS.CFO		
		entwickelt eine Sprachregelung für das Risikomanagement	CS.28	●								R	CS.CFO		
		legt einheitliche Messgrößen fest	CS.29			●						R	CS.CFO		
		entwickelt die internen und externen Berichtsanforderungen für das ERM	CS.30								●	R	CS.CFO	C	CS.23
		überwacht den offiziellen Berichtserstattungsprozesses	CS.31								●			C	CS.23
		berichtet an den CEO über Fortschritte und Hindernisse	CS.32							●					
		empfiehlt erforderliche Maßnahmen	CS.33							●		R	CS.CEO		
Interne Revision		beurteilt die Funktionsfähigkeit des ERM	CS.34								●			C	CS.CEO
		empfiehlt Verbesserungsmaßnahmen	CS.35							●		R	CS.CEO		
		beurteilt die Verlässlichkeit des Berichtswesens	CS.36								●			R	CS.CFO
		beurteilt die Effizienz und Effektivität der Geschäftsabläufe	CS.37								●			R	CS.CEO
		überprüft die Einhaltung von Gesetzen und internen Regelungen	CS.38								●			C	CS.19
Sonstiges Personal	Fach- und Hilfs-personal mit/ohne Führungsaufgabe	Risikomanagements ist direkt oder indirekt Teil der Stellenbeschreibung	CS.39			●	●	●	●			C/I	CS.CEO		
		Druck von Vorgesetzten zur Beteiligung an unsauberen Aktivitäten wird widerstanden	CS.40							●				C	CS.18
		Meldung von Unregelmäßigkeiten wird durchgeführt	CS.41						●					R	CS.18
		Rollen und Verantwortlichkeiten in Bezug auf ERM sind klar definiert und effektiv kommuniziert	CS.42	●								C/I	CS.CEO		
		Erzeugen Informationen zur Identifizierung und Bewertung von Risiken	CS.43			●	●	●				C	CS.14		
		Unterstützen den Informations- und Kommunikationsfluss in Bezug auf das ERM	CS.44							●		C	CS.15		

[2] Zusammenfassung zu einer Referenznummer

Tabelle 9: COSO II: Verantwortungsbereich - verbleibendes internes Personal[134]

[134] Quelle: eigene Darstellung in Anlehnung an [21, S. 86-88], [4, S. 86-89]

Der in Tabelle 10 veranschaulichte Bereich stellt die externen Gruppen dar, welche einen Einfluss auf das ERM ausüben. Folgende Ausprägungen sind hierbei relevant:

- Externe Prüfer[135]: Die wesentliche Aufgabe von externen Prüfungen bezieht sich auf die Korrektheit der Finanzberichterstattung. Falls gesetzliche Anforderungen vorliegen beinhaltet diese Prüfung auch die Beurteilung des unternehmensweiten Risikomanagements. Ein Beispiel für eine derartige Vorgabe ist im *IDW Prüfungsstandard 261 des Instituts der Wirtschaftsprüfer in Deutschland* mit folgender Regelung enthalten [33, S. 9]:

  > *„Nach § 317 Abs. 4 HGB hat der Abschlussprüfer bei börsennotierten Aktiengesellschaften bei der Abschlussprüfung auch zu beurteilen, ob der Vorstand im Rahmen des Risikomanagements geeignete Maßnahmen getroffen hat, insb. ein Überwachungssystem eingerichtet hat, damit den Fortbestand des Unternehmens gefährdende Entwicklungen früh erkannt werden (Risikofrüherkennungssystem), und ob dieses Risikofrüherkennungssystem seine Aufgaben erfüllen kann.*
  >
  > *Die Prüfung des Risikofrüherkennungssystems geht insoweit über die Prüfung des rechnungslegungsbezogenen internen Kontrollsystems hinaus als auch nicht rechnungslegungsbezogene Feststellungen zu treffen sind.“*

- Gesetzgeber und Aufsichtsbehörden[136]: Diese beeinflussen das unternehmensweite Risikomanagement durch gesetzliche Vorgaben.
- Geschäftspartner des Unternehmens und Outsourcing Partner[137]: Die wichtigsten Gruppen in diesem Kontext stellen, nach den Einschätzungen des Autors, Kunden, Lieferanten und Outsourcing Partner dar. Die einher gehenden Risiken betreffen zum Beispiel Umsatzrückgänge, Ausfall von wichtigen Rohstofflieferanten oder eine mangelnde Prozessqualität bei Outsourcing Partnern. Zudem liefern diese Partner wichtige Informationen aus externer Sicht, welche in das ERM einfließen.
- Finanzanalysten, Rating Agenturen und Nachrichtenmedien[138]: Nach den Erfahrungen und Einschätzungen des Autors werden im Umgang mit dieser Gruppe hauptsächlich Risiken gesteuert, welche das Image des Unternehmens betreffen.

Die Darstellung der externen Gruppen erfolgte, um die Gesamtheit an Rollen und Verantwortlichkeiten aufzuzeigen. Bei der Entwicklung des Integrationsmodells wurden diese jedoch aus Gründen der Übersichtlichkeit nicht berücksichtigt.

Tabelle 11 stellt, die für COSO II maßgeblichen Rollen in seiner Gesamtheit dar. Es wurden insgesamt 11 Rollen und 55 konkrete Aufgabenstellungen identifiziert.

[135] In Anlehnung an [21, S. 88-89]
[136] In Anlehnung an [21, S. 89-90]
[137] In Anlehnung an [21, S. 90]
[138] In Anlehnung an [21, S. 91]

Rolle	Ausprägungen	Aufgaben und Verantwortlichkeiten	#	COSO Komponente: internes Umfeld	Zielfestlegung	Ereignis-identifikation	Risiko-bewertung	Risikosteuerung	Kontroll-aktivitäten	Information & Kommunikation	Überwachung	ERM: RACI	ERM: IKS Mapping	IKS: RACI	IKS: ERM Mapping
Externe Prüfer	Wirtschafts-prüfer	prüfen die Finanzberichterstattung	CS.45								●			C	CS.19
		berichten über Prüfungsfeststellungen, Analyseergebnisse und geben Empfehlungen ab	CS.46								●			C	CS.19
		berichten über Feststellungen von IKS- und Risikomanagement-Mängel	CS.47								●			C	CS.19
Gesetzgeber Aufsichtsbehörden	Behördliche Prüfer	Geben den Rahmen für das ERM vor	CS.48	●	●							C	CS.CEO		
		Führen externe Prüfungen durch (z.B. die Finanzmarktaufsicht bei Banken)	CS.49								●	C		C	CS.CFO
		Sprechen Empfehlungen aus und setzen Zwangsmaßnahmen	CS.50	●	●						●	C	CS.CEO		
Geschäfts-partner	Kunden, Liefer-firmen Kooperationen	stellen wichtige Quellen für das ERM dar	CS.51							●		C	CS.CEO		
		das Unternehmen definiert Maßnahmen zwecks Erhalts von wichtigen Informationen	CS.52							●		C	CS.CEO		
Outsourcing Partner		liefern Leistungen zu ausgelagerten Geschäftsprozessen	CS.53	●	●	●	●	●	●	●		C	CS.14		
Finanzanalysten Rating Agenturen Nachrichtenmedien		liefern externe Ansichten zur Verbesserung des ERM	CS.55							●		C	CS.CEO		

Tabelle 10: COSO II: Darstellung der externen Gruppen[139]

[139] Quelle: eigene Darstellung in Anlehnung an [21, S. 88-91], [4, S. 89-91]

				COSO Komponente								ERM		IKS	
Rolle	Ausprägungen	Aufgaben und Verantwortlichkeiten	#	Internes Umfeld	Zielfestlegung	Ereignis-identifikation	Risiko-bewertung	Risikosteuerung	Kontroll-aktivitäten	Information & Kommunikation	Überwachung	RACI	IKS Mapping	RACI	ERM Mapping
Aufsichtsrat		hat Kenntnis über den Umfang des Risikomanagements	CS.1								●	A/I	CS.4 CS.5		
		hat Kenntnis über die Risikobereitschaft	CS.2								●	A/I	CS.6		
		hat Kenntnis über die signifikanten Risiken	CS.3								●	A/I	CS.7		
		überprüft das Risikoportfolio	CS.4								●			A	CS.1
		wiegt das Risikoportfolio gegen die Risikobereitschaft ab	CS.5								●			A	CS.2
		stimmt der Risikobereitschaft zu	CS.6								●			A	CS.2
		prüft die Steuerung der signifikanten Risiken durch das Management	CS.7								●			A	CS.3
Management	Vorstand Geschäftsführung (CEO)	CEO verantwortet das unternehmensweite Risikomanagement durch:	CS.CEO	●	●	●	●	●	●	●	●	A/R	1)	A/R	1)
		* Festlegung und Abstimmung der Risikobereitschaft und Risikotoleranzen	CS.8		●							A/R	CS.6		
		* Erstellung des Risikoportfolios	CS.9		●							A/R	CS.4		
		* Festlegung der Risikomanagement Philosophie und Verhaltenskodex	CS.10	●								A/R	CS.6		
		* Definition und Überwachung der signifikanten Risiken	CS.11			●			●		●	A/R	CS.7		
		* Festlegung der Strategieziele und Steuerung und Kontrolle des Senior Managements	CS.12		●				●		●			A/R	CS.14 CS.15 CS.16 CS.17
		CEO stellt sicher, dass alle ERM Komponenten vorhanden sind	CS.13	●								A/R	CS.47		
	Senior Management (SM)	SM pflegt den Umgang mit Risiken, die mit den verantworteten Zielen zusammenhängen	CS.14			●	●	●	●	●	●	A/R	CS.12		
		SM steuert die Elemente des Risikomanagements im verantworteten Bereich	CS.15			●	●	●	●	●	●	A/R	CS.12		
		SM stellt die Einhaltung der definierten Risikotoleranz sicher	CS.16			●	●	●	●	●	●	A/R	CS.12		
		SM hat Rechenschaftspflicht gegenüber der nächsthöheren Ebene	CS.17		●							R	CS.12		
1) Zusammenfassung zu einer Referenznummer															
Führungskräfte im Finanz- und Rechnungswesen	Leitung Finanzen (CFO) Leitung Controlling Leitung Rechnungswesen	erstellen und planen das Budget inklusive Risiken und Chancen	CS.18		●	●	●	●				A/R	CS.19		
		überwachen die Performance (betrieblich, gesetzlich, Berichterstattung)	CS.19						●		●			A/R	CS.18
		verhindern manipulative Berichterstattung und decken Unregelmäßigkeiten auf	CS.20						●		●			R	CS.18
		überwachen und überprüfen beschlossene Maßnahmen im Hinblick auf:	CS.CFO						●		●	A/R	2)	A/R	2)
		* betriebswirtschaftliche Zieldefinitionen	CS.21						●		●			R	CS.18
		* Strategieentscheidungen	CS.22						●		●			R	CS.8
		* Risikoanalysen	CS.23						●		●			R	CS.11
Risikomanagement	Risk Officer (CRO)	entwickelt die Grundsätze des Risikomanagements	CS.24	●		●						R	CS.CEO		
		entwickelt einen Rahmen von Befugnissen	CS.25	●								R	CS.CFO		
		fördert die Risikomanagement Kompetenz	CS.26	●								R	CS.CEO		
		Integriert das ERM in Management- und Geschäftsplanungsprozesse	CS.27	●								R	CS.CFO		
		entwickelt eine Sprachregelung für das Risikomanagement	CS.28	●								R	CS.CFO		
		legt einheitliche Messgrößen fest	CS.29			●						R	CS.CFO		
		entwickelt die internen und externen Berichtsanforderungen für das ERM	CS.30								●	R	CS.CFO		
		überwacht den offiziellen Berichtserstattungsprozesses	CS.31								●			C	CS.23
		berichtet an den CEO über Fortschritte und Hindernisse	CS.32							●				C	CS.23
		empfiehlt erforderliche Maßnahmen	CS.33							●		R	CS.CEO		
Interne Revision		beurteilt die Funktionsfähigkeit des ERM	CS.34								●			C	CS.CEO
		empfiehlt Verbesserungsmaßnahmen	CS.35							●		R	CS.CEO		
		beurteilt die Verlässlichkeit des Berichtswesens	CS.36								●			R	CS.CFO
		beurteilt die Effizienz und Effektivität der Geschäftsabläufe	CS.37								●			R	CS.CEO
		überprüft die Einhaltung von Gesetzen und internen Regelungen	CS.38								●			C	CS.19
Sonstiges Personal	Fach- und Hilfs-personal mit/ohne Führungsaufgabe	Risikomanagements ist direkt oder indirekt Teil der Stellenbeschreibung	CS.39			●	●	●	●			C/I	CS.CEO		
		Druck von Vorgesetzten zur Beteiligung an unsauberen Aktivitäten wird widerstanden	CS.40							●				C	CS.18
		Meldung von Unregelmäßigkeiten wird durchgeführt	CS.41						●					R	CS.18
		Rollen und Verantwortlichkeiten in Bezug auf ERM sind klar definiert und effektiv kommuniziert	CS.42	●								C/I	CS.CEO		
		Erzeugen Informationen zur Identifizierung und Bewertung von Risiken	CS.43			●	●	●				C	CS.14		
		Unterstützen den Informations- und Kommunikationsfluss in Bezug auf das ERM	CS.44							●		C	CS.15		
2) Zusammenfassung zu einer Referenznummer															
Externe Prüfer	Wirtschafts-prüfer	prüfen die Finanzberichterstattung	CS.45								●			C	CS.19
		berichten über Prüfungsfeststellungen, Analyseergebnisse und geben Empfehlungen ab	CS.46								●			C	CS.19
		berichten über Feststellungen von IKS- und Risikomanagement-Mängel	CS.47								●			C	CS.19
Gesetzgeber Aufsichtsbehörden	Behördliche Prüfer	Geben den Rahmen für das ERM vor	CS.48	●	●							C	CS.CEO		
		Führen externe Prüfungen durch (z.B. die Finanzmarktaufsicht bei Banken)	CS.49								●			C	CS.CFO
		Sprechen Empfehlungen aus und setzen Zwangsmaßnahmen	CS.50	●	●						●	C	CS.CEO		
Geschäfts-partner	Kunden, Liefer-firmen Kooperationen	stellen wichtige Quellen für das ERM dar	CS.51							●		C	CS.CEO		
		das Unternehmen definiert Maßnahmen zwecks Erhalts von wichtigen Informationen	CS.52							●		C	CS.CEO		
Outsourcing Partner		liefern Leistungen zu ausgelagerten Geschäftsprozessen	CS.53	●	●	●	●	●	●	●	●	C	CS.14		
Rating Agenturen Nachrichtenmedien		liefern externe Ansichten zur Verbesserung des ERM	CS.55							●		C	CS.CEO		

Tabelle 11: Überblick über Rollen und Verantwortlichkeiten von COSO II[140]

[140] In Anlehnung an [21], [4], [16]

Neben der Sichtweise von COSO II sind eine Reihe von zusätzlichen Rollen und Verantwortlichkeiten in weiteren Rahmenwerken oder Richtlinien definiert. Um den hohen Stellenwert der IT Rechnung zu tragen wird in diesem Zusammenhang in der Folge das COBIT-Modell analysiert und mit dem COSO II Rahmenwerk in Verbindung gebracht.

COBIT sieht für alle Aktivitäten in den IT-Prozessen eine detaillierte Zuordnung von Rollen vor. In dieser Hinsicht ist COBIT detaillierter als COSO und liefert weitere Aufschlüsse für mögliche ERM-Rollen. Zudem ist in COBIT 4.1 eine Mapping Tabelle enthalten [18, S. 173], welche die IT-Prozesse den Komponenten von COSO I zuordnet. Anhand dieser Zuordnung kann festgestellt werden, welcher COSO Phase die jeweiligen IT-Prozesse entsprechen. Im Zuge der Analyse der COBIT Rollen wurde wie folgt vorgegangen:

- Feststellung, welche Rollen COBIT 4.1 vorsieht, anhand des RACI-Charts, welches in Abbildung 33 dargestellt ist.
- Analyse der 34 IT-Prozesse und Auswahl jener Aufgaben, welche nach der Einschätzung des Autors mit dem ERM in Zusammenhang stehen.
- Zuteilung von Aktivitäten zu Rollen. Dabei wurden nur jene Aktivitäten übernommen für welche die Rolle zuständig (*Responsible*) oder letztverantwortlich (*Accountable*) ist.
- Feststellung ob die Aufgabe das Risikomanagement oder IKS betrifft.
- Zuordnung der identifizierten Aufgaben zu COBIT Domänen und Prozessen.
- Definition einer, nach den Einschätzungen des Autors, maßgeblichen Rolle, welche die Aufgabe und den daraus resultierenden Prozess überwacht.
- Darstellung des Mappings der Aufgaben zu den COSO Komponenten anhand der Mapping Tabelle in COBIT 4.1 [18, S. 173] zur Einordnung in das ERM.
- Analyse von verteilten Verantwortungen, da einige der COBIT Aktivitäten gleichzeitig von verschiedenen Rollen wahrgenommen werden.

RACI Chart — **Functions**

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Abbildung 33: Beispiel eines RACI-Charts[141]

[141] Quelle: [18, S. 31]

Das Ergebnis der Analyse in Tabellenform umfasst alle COBIT Rollen mit zugeteilten Aufgaben und besteht aus folgenden Komponenten:

- Darstellung der COBIT 4.1 Rollen und zugeteilten Aufgaben.
- Jede Aufgabe ist mit einer Referenznummer versehen, um die mehrfache Rollenzuteilung zu Aufgaben zu gewährleisten.
- Jeder Aufgabe ist der jeweilige COBIT Prozess zugeordnet.
- In der Spalte *IKS* sind die überwachenden Rollen den Aufgaben zugeordnet.
- Der Bereich des COSO Mappings zeigt den bereits erwähnten Zusammenhang der Aufgaben und den COSO Komponenten. Hierbei steht
    - *P* für einen primären und
    - *S* für einen sekundären Zusammenhang
- In der Spalte Wichtigkeit steht
    - *H* für eine hohe
    - *M* für eine mittlere und
    - *L* für eine geringe Wichtigkeit der Unterstützung des COSO Rahmenwerkes.
- Darstellung von verteilten Verantwortungen je Aufgabe, um die Notwenigkeit der Zusammenarbeit sowie Teambildung aufzuzeigen.

Es wurden insgesamt 16 Rollen und 67 konkrete Aufgaben analysiert. Eine inhaltliche Beschreibung der Rollen ist in COBIT 4.1 nicht enthalten[142]. Da das COBIT Prozessmodell sehr detailliert ausgeführt ist, ergeben sich die Inhalte der Rollenbeschreibungen durch die zugeteilten Aufgaben.

Die folgenden Tabellen 12 bis 15 veranschaulichen das Ergebnis dieser Analysenphase.

[142] Siehe dazu die Ausführungen in COBIT 4.1 [18, S. 28] - Es wird lediglich erwähnt, welche Rollen das RACI-Chart enthält, ohne auf die inhaltlichen Ausprägungen einzugehen

Rolle	Hauptaufgaben und Verantwortlichkeiten (Prozesse)	#	Domäne	Prozess	IKS: Überwachung (Rolle)	COSO-Mapping: Kontrollumgebung	Risiko Beurteilung	Kontroll Aktivitäten	Information Kommunikation	Monitoring	Wichtigkeit	verteilte Verantwortung: Designierte Rolle bearbeitet die Aufgabe gemeinsam mit: (als Aufschlüsse zur Prozessbildung)
Aufsichtsrat (AR)	Wahrnehmung von Überwachungsaktivitäten des CEO	CO.1	ME	1-4		P	S	P	S	P	H	
Vorstand oder Geschäftsführung (CEO)	Entwicklung von Verträgen, welche das Interesse den Unternehmens schützen	CO.2	AI	5	CIO			P			M	
	Ermöglichung der Aufsichtstätigkeiten durch den Aufsichtsrat	CO.3	ME	4	AR	P	S		S	P	H	
	Überwachung der IT-Performance, Ressourcen und RM im Einklang mit der Unternehmensstrategie	CO.4	ME	4	AR	P	S		S	P	H	
	Periodische Beauftragung von externen Audits zur Beurteilung der Performance und Compliance	CO.5	ME	4	AR	P	S		S	P	H	
	Umsetzung der Beobachtungen und Empfehlungen der externen Audits	CO.6	ME	4	AR	P	S		S	P	H	
	Erstellung eines IT-Governance Reports	CO.7	ME	4	AR	P	S		S	P	H	CIO
Leitung Finanzen (CFO)	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CIO BPE
	Entwicklung eines allgemeinen Monitoring Ansatzes	CO.9	ME	1	CEO				S	P	H	
Business Process Executive (BPE)	Identifizierung der kritischen Abhängigkeiten und Performance	CO.10	PO	1	CIO		P		S	S	H	
Senior Management	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CFO CIO
	Berichterstattung über die IT-Performance	CO.11	ME	1	CIO				S	P	H	
Leitung Informatik (CIO)	Verfinkung der Kerngeschäftsziele mit IT Zielen	CO.12	PO	1	BPE		P		S	S	H	
	Erstellung eines strategischen IT-Plans	CO.13	PO	1	CEO		P		S	S	H	
	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CFO BPE
	Definition, Erstellung und Aufrechterhaltung eines Qualitätsmanagementsystems	CO.14	PO	8	CIO	P		P	S	P	H	
	Erstellung und Kommunikation eines Qualitätsstandards	CO.15	PO	8	CIO	P		P	S	P	H	
	Erstellung und Management eines Qualitätsplans für kontinuierliche Verbesserung	CO.16	PO	8	CIO	P		P	S	P	H	
	Messung, Überwachung und Überprüfung der Compliance mit Qualitätszielen	CO.17	PO	8	CIO	P		P	S	P	H	
	Unterhaltung und Überwachung eines Risikomaßnahmenplans	CO.18	PO	9	CEO		P				H	
	Definition eines Portfolio- und Programmmanagement Rahmenwerks für IT-Investitionen	CO.19	PO	10	BPO	S	S	P		S	H	
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	BPO LB LE PMO
	Überwachung der Service Leistungen von externen Partnern	CO.21	DS	2	BPO	P	S	P		S	N	
	Erstellung einen Ansatzes zur Überwachung von IT-Risiken	CO.22	ME	1	CEO				S	P	H	
	IT-Performance, IT-Strategie, Ressourcen und RM in Einklang mit der Geschäftsstrategie bringen	CO.23	ME	4	AR	P	S		S	P	H	
	Erstellung eines IT-Governance Reports	CO.7	ME	4	AR	P	S		S	P	H	CEO
Business Process Owner (BPO)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO	P			S	S	H	LB LE
Fach- und Hilfspersonal	Priorisierung und Planung von Kontrolltätigkeiten	CO.25	PO	9	CIO/BPE		P				H	
mit oder ohne Führungsaufgaben	Sicherstellung eines Budgets für Risikomaßnahmenpläne	CO.26	PO	9	CFO/BPE		P				H	
	Aufrechterhaltung und Überwachung des Risikomaßnahmenplans	CO.27	PO	9	CEO		P				H	CISA
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO LB LE PMO
	Spezifikation von Anwendungskontrollen innerhalb des Designs	CO.28	AI	2	LE			P			M	PMO
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	LE PMO
	Planung und Durchführung von IT-Kontinuitätstrainings	CO.30	DS	4	LB	S		P	S		M	
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	LB LE

Tabelle 12: COBIT Rollen und Verantwortungen inkl. COSO-Mapping, Teil 1[143]

[143] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21]

Rolle	Hauptaufgaben und Verantwortlichkeiten (Prozesse)	#	Domäne	Prozess	IKS: Überwachung (Rolle)	COSO-Mapping: Kontroll umgebung	Risiko Beurteilung	Kontroll Aktivitäten	Information Kommunikation	Monitoring	Wichtigkeit	vertikale Verantwortung: Designierte Rolle bearbeitet die Aufgabe gemeinsam mit: (als Aufschlüsse zur Prozessbildung)					
Leitung IT-Betrieb (LB)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO		P		S	S	H	BPO	LE				
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.32	PO	9	CPO/CIO		P				H	LA	LE	LAD			
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LA	LE	LAD			
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO	BPO	LE	PMO		
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LE	PMO				
	Definition von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LE	LAD				
	Überwachung der SLA Performance	CO.36	DS	1	SM	S		P	S	S	M	LE					
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LE	LAD				
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LE	LAD				
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P		S	N	LE	LAD				
	Überwachung der Performance und Kapazität der IT-Ressourcen	CO.40	DS	3	LB			P		S	N						
	Entwicklung von IT-Kontinuitätsplänen	CO.41	DS	4	LB	S		P	S	S	M	LE					
	Überwachung von Sicherheitsereignissen	CO.42	DS	5	CIO			P	S	S	H						
	Definition und Implementierung von Verfahren zur Datenwiederherstellung	CO.43	DS	11	CIO			P			H						
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	BPO	LE				
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LE	LAD				
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LA	LE	LAD	PMO	CRSA	
Leitung IT-Architektur (LA)	Überwachung der technologischen Entwicklung	CO.46	PO	3	CIO	S	P	S			M						
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.32	PO	9	CPO/CIO		P				H	LB	LE	LAD			
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB	LE	LAD			
	Entwicklung eines Rahmenwerkes für die IT-Kontinuität	CO.47	DS	4	CIO			P	S		M	CRSA					
	Implementierung von technischen Maßnahmen und Verfahren zum Informationsschutz in Netzwerken	CO.48	DS	5	CIO			P	S	S	H	LE					
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB	LE	LAD	PMO	CRSA	
Leitung IT-Entwicklung (LE)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO		P		S	S	H	LB	BPO				
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.32	PO	9	CPO/CIO		P				H	LB	LA	LAD			
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB	LA	LAD			
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO	BPO	LB	PMO		
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	BPO	PMO				
	Sicherstellung, dass jede kritische Änderung (Change) den Genehmigungsprozess durchläuft	CO.49	AI	6	LB		S	P		S	H						
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LB	PMO				
	Erstellung und Bewertung von Implementierungsplänen	CO.50	AI	7	CIO			P	S	S	M						
	Erstellung und Bewertung einer Teststrategie und einer Planungsmethode für die Testdurchführung	CO.51	AI	7	CIO			P	S	S	M						
	Definition von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LB	LAD				
	Überwachung der SLA Performance	CO.36	DS	1	SM	S		P	S	S	M	LB					
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LB	LAD				
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LB	LAD				
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P		S	N	LB	LAD				
	Entwicklung von IT-Kontinuitätsplänen	CO.41	DS	4	LB	S		P	S		M	LB					
	Implementierung von technischen Maßnahmen und Verfahren zum Informatosschutz in Netzwerken	CO.48	DS	5	CIO			P	S	S	H	LA					
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	BPO	LB				
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LB	LAD				
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB	LAD	LAD	PMO	CRSA	

Tabelle 13: COBIT Rollen und Verantwortungen inkl. COSO-Mapping, Teil 2[144]

[144] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21]

Rolle	Hauptaufgaben und Verantwortlichkeiten (Prozesse)	#	Domäne	Prozess	IKS: Überwachung (Rolle)	COSO-Mapping: Kontroll umgebung	Risiko beurteilung	Kontroll Aktivitäten	Information Kommunikation	Monitoring	Wichtigkeit	verteilte Verantwortung: Designierte Rolle bearbeitet die Aufgabe gemeinsam mit: (als Aufschlüsse zur Prozessbildung)				
Leitung IT-Administration (LAD)	Identifikation, Kommunikation und Monitoring der IT-Investitionen	CO.52	PO	5	CIO		S	P			M					
	Entwicklung von IT-Richtlinien	CO.53	PO	6	CIO	P			P		M					
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.32	PO	9	CPO/CIO		P				H	LB	LA	LE		
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB	LA	LE		
	Definiton von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LB	LE			
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LB	LE			
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LB	LE			
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P	S	S	N	LB	LE			
	Planung und Entwicklung der Wiederherstellung von IT-Systemen nach Totalausfall	CO.54	DS	4	LB	S		P	S		M	PMO				
	Entwicklung und Aufrechterhaltung eines IT-Kosten Kontrollprozesses	CO.55	DS	6	CIO			P			N					
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LB	LE			
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB	LA	LE	PMO	CRSA
Projektbüro (PMO)	Erstellung eines taktischen IT-Plan	CO.56	PO	1	CIO		P		S	S	H					
	Erstellung und Erhaltung eines IT-Projektüberwachungs, -messungs und -managementsystems	CO.57	PO	10	LB	S	S	P		S	H					
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO	BPO	LB	LE	
	Spezifikation von Anwendungskontrollen innerhalb des Designs	CO.28	AI	2	LE			P			M	BPO				
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	BPO	LE			
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LB	LE			
	Planung und Entwicklung der Wiederherstellung von IT-Systemen nach Totalausfall	CO.54	DS	4	LB	S		P	S		M	LAD				
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB	LA	LE	LAD	CRSA
Compliance, Risk, Security und Audit (CRSA)	Aufrechterhaltung und Überwachung des Risikomaßnahmenplans	CO.27	PO	9	CEO		P				H	BPO				
	Entwicklung eines Rahmenwerkes für die IT-Kontinuität	CO.47	DS	4	CIO	S		P	S		M	LA				
	Erstellung und Unterhaltung eines IT-Sicherheitsplans	CO.58	DS	5	CIO			P	S	S	H					
	Monitoring von Sicherheitsverletzungen	CO.59	DS	5	CIO			P	S	S	H					
	Regelmäßige Durchführung von Verletzbarkeits- und Schwachstellenanalysen	CO.60	DS	5	CIO			P	S	S	H					
	Überwachung von Internen Kontrolltätigkeiten	CO.61	ME	2	CIO					P	M					
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB	LA	LE	LAD	PMO
	Implementierung der Erkenntnisse von externen Audits	CO.62	ME	4	AR	S		P	S		H					
Configuration Management (CM)	Überprüfung von Konfigurationsinformationen (inkl. der Entdeckung von nicht autorisierter Software)	CO.63	DS	9	LB			P			M					
Problem Management (PM)	Identifizierung und Klassifizierung von Problemfällen	CO.64	DS	10	LB			P	S	S	M					
	Durchführung von Ursachenanalysen	CO.65	DS	10	PM			P	S	S	M					
	Überprüfung des Status der Problemfälle	CO.66	DS	10	LB			P	S	S	M					
	Führung von Problemreports	CO.67	DS	10	PM			P	S	S	M					

Tabelle 14: COBIT Rollen und Verantwortungen inkl. COSO-Mapping, Teil 3[145]

[145] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21]

					IKS	COSO-Mapping						Verteilung Verantwortlichkeit
Rolle	Hauptaufgaben und Verantwortlichkeiten (Prozesse)	#	Domäne	Prozess	Überwachung (Rolle)	Kontroll-Umgebung	Risiko-Beurteilung	Kontroll-Aktivitäten	Information-Kommunikation	Monitoring	Wichtigkeit	Designierte Rolle bearbeitet die Aufgabe gemeinsam mit (als Aufschlüsse zur Prozessbildung)
Aufsichtsrat (AR)	Wahrnehmung von Überwachungsaktivitäten des CEO	CO.1	ME	1-4		P	S	P	S	P	H	
Vorstand oder Geschäftsführung (CEO)	Entwicklung von Verträgen, welche das Interesse des Unternehmens schützen	CO.2	AI	5	CIO			P			M	
	Ermöglichung der Aufsichtstätigkeiten durch den Aufsichtsrat	CO.3	ME	4	AR	P	S		S	P	H	
	Überwachung der IT-Performance, Ressourcen und RM im Einklang mit der Unternehmensstrategie	CO.4	ME	4	AR	P	S		S	P	H	
	Periodische Beauftragung von externen Audits zur Beurteilung der Performance und Compliance	CO.5	ME	4	AR	P	S		S	P	H	
	Umsetzung der Beobachtungen und Empfehlungen der externen Audits	CO.6	ME	4	AR	P	S		S	P	H	
	Erstellung eines IT-Governance Reports	CO.7	ME	4	AR	P	S		S	P	H	CIO
Leitung Finanzen (CFO)	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CIO BPE
	Entwicklung eines allgemeinen Monitoring Ansatzes	CO.9	ME	1	CEO				S	P	H	
Business Process Executive (BPE)	Identifizierung der kritischen Abhängigkeiten und Performance	CO.10	PO	1	CIO		P		S	S	H	
Senior Management	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CFO CIO
	Berichterstattung über die IT-Performance	CO.11	ME	1	CIO				S	P	H	
Leitung Informatik (CIO)	Verbindung der Kongruenzziele mit IT Zielen	CO.12	PO	1	BPE		P		S	S	H	
	Erstellung eines strategischen IT-Plans	CO.13	PO	1	CEO		P		S	S	H	
	Pflege des Programmportfolios	CO.8	PO	5	CEO		S	P			M	CFO BPE
	Definition, Erstellung und Aufrechterhaltung eines Qualitätsmanagementsystems	CO.14	PO	8	CIO	P		P	S	P	H	
	Erstellung und Kommunikation eines Qualitätsstandards	CO.15	PO	8	CIO	P		P	S	P	H	
	Erstellung und Management eines Qualitätsplans für kontinuierliche Verbesserung	CO.16	PO	8	CIO	P		P	S	P	H	
	Messung, Überwachung und Überprüfung der Compliance mit Qualitätszielen	CO.17	PO	8	CIO	P		P	S	P	H	
	Unterhaltung und Überwachung eines RisikomaßnahmenplansCO.18		PO	9	CEO		P				H	
	Definition eines Portfolio- und Programmmanagement Rahmenwerks für IT Investitionen	CO.19	PO	10	BPO	S	S	P		S	H	
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	BPO LB LE PMO
	Überwachung der Service Leistungen von externen Partnern	CO.21	DS	2	BPO	P	S	P		S	N	
	Erstellung einen Ansatzes zur Überwachung von IT-Risiken	CO.22	ME	1	CEO				S	P	H	
	IT-Performance, IT-Strategie, Ressourcen und RM in Einklang mit der Geschäftsstrategie bringen	CO.23	ME	4	AR	P	S		S	P	H	
	Erstellung eines IT-Governance Reports	CO.7	ME	4	AR	P	S		S	P	H	CEO
Business Process Owner (BPO)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO		P		S	S	H	LB LE
Fach- und Hilfspersonal	Priorisierung und Planung von Kontrolltätigkeiten	CO.25	PO	9	CIO/BPE		P				H	
mit oder ohne Führungsaufgaben	Sicherstellung eines Budgets für RisikomaßnahmenplanCO.18		PO	9	CFO/BPE		P				H	
	Aufrechterhaltung und Überwachung des RisikomaßnahmenplansCO.18		PO	9	CEO		P				H	CRSA
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO LB LE PMO
	Spezifikation von Anwendungskontrollen innerhalb des Designs	CO.26	AI	2	LE			P			M	PMO
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	LE PMO
	Planung und Durchführung von IT-Kontinuitätstrainings	CO.30	DS	4	LB	S		P	S		M	
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	LB LE
Leitung IT-Betrieb (LB)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO		P		S	S	H	BPO LE
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LA LE LAD
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LA LE LAD
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO BPO LE PMO
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LE PMO
	Definition von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LE LAD
	Überwachung der SLA Performance	CO.36	DS	1	SM	S		P	S	S	M	LE
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LE LAD
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LE LAD
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P		S	N	LE LAD
	Überwachung der Performance und Kapazität der IT-Ressourcen	CO.40	DS	3	LB			P		S	N	
	Entwicklung von IT-KontinuitätsplänenCO.41		DS	4	LB	S		P	S		M	LE
	Überwachung von Sicherheitsereignissen	CO.42	DS	5	CIO			P	S	S	H	
	Definition und Implementierung von Verfahren zur Datenwiederherstellung	CO.43	DS	11	CIO			P			H	
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	BPO LE
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LE LAD
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LA LE LAD PMO CRSA
Leitung IT-Architektur (LA)	Überwachung der technologischen Entwicklung	CO.46	PO	3	CIO		S	P	S		M	
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LE LAD
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LE LAD
	Entwicklung eines Rahmenwerkes für die IT-KontinuitätCO.47		DS	4	CIO			P	S		M	CRSA
	Implementierung von technischen Maßnahmen und Verfahren zum Informationsschutz in Netzwerken	CO.48	DS	5	CIO			P	S	S	H	LE
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB LE LAD PMO CRSA
Leitung IT-Entwicklung (LE)	Analyse des Programm Portfolios und Management des Projekt -und Service Portfolios	CO.24	PO	1	CIO		P		S	S	H	LB BPO
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LA LAD
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LA LAD
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO BPO LB PMO
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	BPO PMO
	Sicherstellung, dass jede kritische Änderung (Change) den Genehmigungsprozess durchläuft	CO.49	AI	6	LB		S	P		S	H	
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LB PMO
	Erstellung und Bewertung von Implementierungsplänen	CO.50	AI	7	CIO			P	S	S	M	
	Erstellung und Bewertung einer Teststrategie und einer Planungsmethode für die Testdurchführung	CO.51	AI	7	CIO			P	S	S	M	
	Definition von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LB LAD
	Überwachung der SLA Performance	CO.36	DS	1	SM	S		P	S	S	M	LB
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LB LAD
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LB LAD
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P		S	N	LB LAD
	Entwicklung von IT-KontinuitätsplänenCO.41		DS	4	LB	S		P	S		M	LB
	Implementierung von technischen Maßnahmen und Verfahren zum Informationsschutz in Netzwerken	CO.48	DS	5	CIO			P	S	S	H	LA
	Beurteilung und Verbesserung der Performance	CO.31	ME	1	CIO				S	P	H	BPO LB
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LB LAD
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB LAD LAD PMO CRSA
Leitung IT-Administration (LAD)	Identifikation, Kommunikation und Monitoring der IT-Investitionen	CO.52	PO	5	CIO		S	P			M	
	Entwicklung von IT-Richtlinien	CO.53	PO	6	CIO	P			P		M	
	Identifikation von Ereignissen, die mit IT-Zielen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LA LE
	Beurteilung und Evaluierung von Risiken, welche mit Ereignissen zusammenhängen	CO.33	PO	9	CPO/CIO		P				H	LB LA LE
	Definition von SLA für kritische IT-Systeme und Applikationen	CO.35	DS	1	SM	S		P	S	S	M	LB LE
	Überwachung der SLA Performance bei externen Partnern (BPO)	CO.37	DS	1	SM	S		P	S	S	M	LB LE
	Identifikation, Bewertung und Reduzierung von lieferantenbezogenen Risiken	CO.38	DS	2	CIO	P	S	P		S	N	LB LE
	Überwachung der Service Delivery der externen Partner	CO.39	DS	2	BPO	P	S	P		S	N	LB LE
	Planung und Entwicklung der Wiederherstellung von IT-Systemen nach Totalausfall	CO.54	DS	4	LB	S		P	S		M	PMO
	Entwicklung und Aufrechterhaltung eines IT-Kosten Kontrollprozesses	CO.55	DS	6	CIO			P			N	
	Monitoring und Steuerung der internen IT-Kontrolltätigkeiten	CO.44	ME	2	CIO/CA					P	M	LB LE
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB LA LE PMO CRSA
Projektbüro (PMO)	Erstellung eines taktischen IT-Plan	CO.56	PO	1	CIO		P		S	S	H	
	Erstellung und Erhaltung eines IT-Projektüberwachungs, -messungs und -managementsystems	CO.57	PO	10	LB	S	S	P		S	H	
	Identifikation, Dokumentation und Analyse von Geschäftsprozessrisiken	CO.20	AI	1	BPO			P			M	CIO BPO LB LE
	Spezifikation von Anwendungskontrollen innerhalb des Designs	CO.26	AI	2	LE			P			M	BPO
	Bewertung der Auswirkung und Priorisierung von Changes	CO.29	AI	6	LB		S	P		S	H	BPO LE
	Verwaltung und Kommunikation von relevanten Änderungen (Changes)	CO.34	AI	6	CIO		S	P		S	H	LB LE
	Planung und Entwicklung der Wiederherstellung von IT-Systemen nach Totalausfall	CO.54	DS	4	LB	S		P	S		M	LAD
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB LA LE LAD CRSA
Compliance, Risk, Security und Audit (CRSA)	Aufrechterhaltung und Überwachung des RisikomaßnahmenplansCO.27		PO	9	CEO		P				H	BPO
	Entwicklung eines Rahmenwerkes für die IT-KontinuitätCO.47		DS	4	CIO	S		P	S		M	LA
	Erstellung und Unterhaltung eines IT-Sicherheitsplans	CO.58	DS	5	CIO			P	S	S	H	
	Monitoring von Sicherheitsverletzungen	CO.59	DS	5	CIO			P	S	S	H	
	Regelmäßige Durchführung von Verletzbarkeits- und Schwachstellenanalysen	CO.60	DS	5	CIO			P	S	S	H	
	Überwachung von Internen Kontrolltätigkeiten	CO.61	ME	2	CIO					P	M	
	Überwachung der IT Compliance	CO.45	ME	3	CIO			P	S	S	H	LB LA LE LAD PMO
	Implementierung der Erkenntnisse von externen Audits	CO.62	ME	4	AR	S		P	S		H	
Configuration Management (CM)	Überprüfung von Konfigurationsinformationen (inkl. der Entdeckung von nicht autorisierter Software)	CO.63	DS	9	LB			P			M	
Problem Management (PM)	Identifizierung und Klassifizierung von ProblemEllen	CO.64	DS	10	LB			P	S	S	M	
	Durchführung von Ursachenanalysen	CO.65	DS	10	PM			P	S	S	M	
	Überprüfung des Status der ProblemEllle	CO.66	DS	10	LB			P	S	S	M	
	Führung von Problemreports	CO.67	DS	10	PM			P	S	S	M	

Tabelle 15: COBIT Rollen und Verantwortungen inkl. COSO-Mapping, Gesamtansicht[146]

[146] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21]

Um der vollständigen Betrachtungen aller Rollen gerecht zu werden, wurde zudem ein Mapping der Rollen von COSO, COBIT 4.1 und ITIL v3 vorgenommen, welches in Tabelle 16 dargestellt ist.

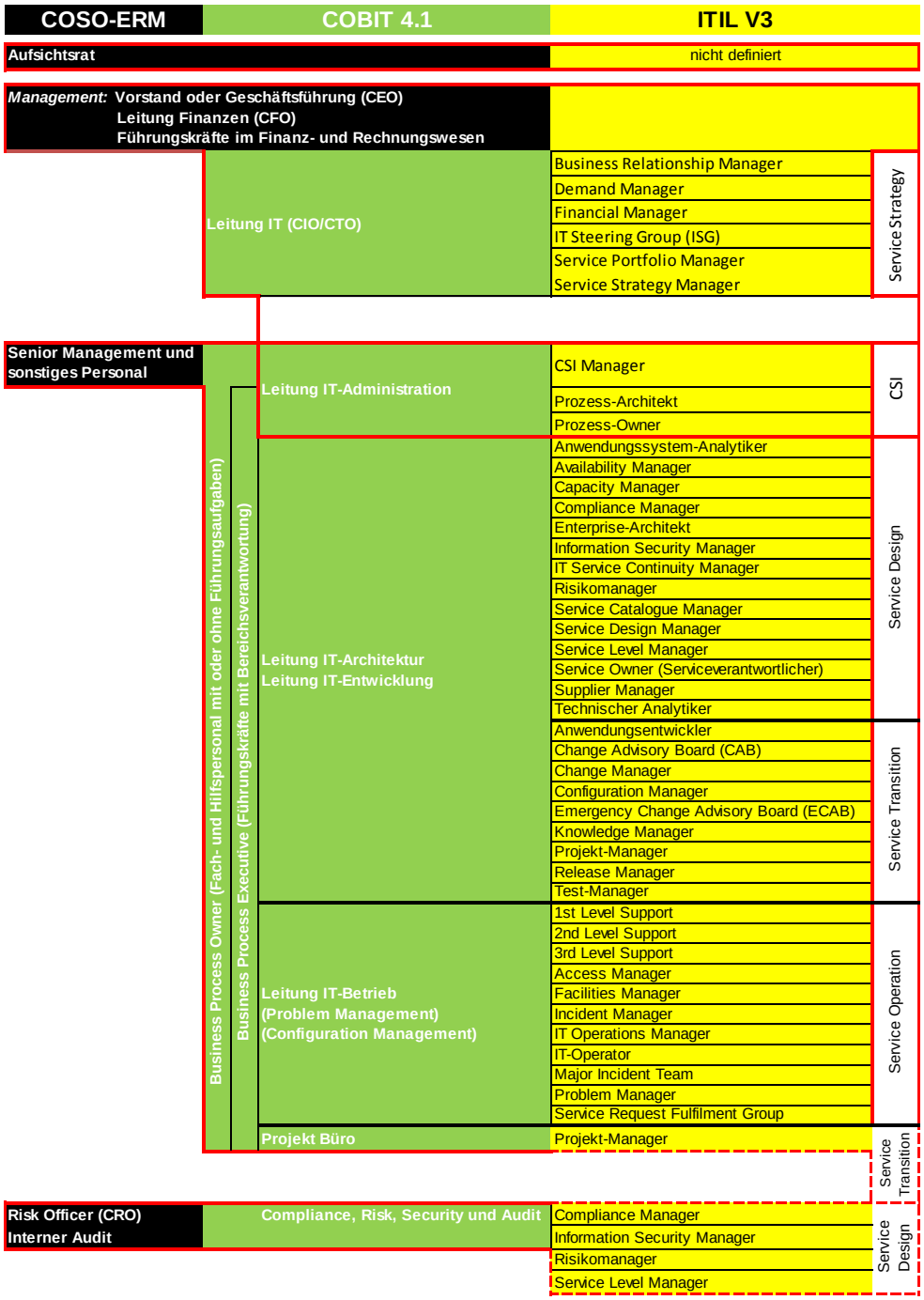

Tabelle 16: Mapping der Rollen in COSO, COBIT und ITIL v3[147]

[147] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21], [87], [74]

Tabelle 16 veranschaulicht in einer Übersicht die Verantwortung der COSO Rollen im Hinblick auf die Planung und Durchführung der ERM-Aufgaben in der IT. Eine detaillierte Beschreibung der ITIL V3 Rollen sowie deren ERM-Aufgaben werden im Rahmen dieser Arbeit nicht mehr weiter ausgeführt.

Tabelle 17 zeigt eine zusammenfassende Darstellung der identifizierten, unternehmensinternen ERM Rollen, welche anhand der bisherigen Analysen und den Inhalten der MaRisk [54] vorgenommen wurde. Diese Zusammenfassung stellt die Basis für die Erstellung des Integrationsmodells auf Ebene der Organisation dar.

	Rolle ist definiert in:				
	COSO	COBIT	MaRisk	ERM	IKS
Aufsichtsrat	■	■			
Vorstand oder Geschäftsführung (CEO)	■	■			
Leitung Finanzen (CFO)	■	■			
Senior Management	■				
Führungskräfte im Finanz- und Rechnungswesen	■				
Risk Officer (CRO)	■		■		
Interne Revision	■		■		
Sonstiges Personal	■				
Leitung Informatik (CIO)		■			
Business Process Owner		■			
Leitung IT-Betrieb (LB)		■			
Leitung IT-Architektur (LA)		■			
Leitung IT-Entwicklung (LE)		■			
Leitung IT-Administration (LAD)		■			
Projektbüro (PMO)		■			
Compliance, Risk, Security und Audit (CRSA)		■	■		
Problem Management (PM)		■			
Configuration Management (CM) [1)]		■			
Problem Management (PM) [1)]		■			
Risikocontrolling			■		
Risk Owner				■	
Kotrollprozess Verantwortliche					■
Kotrollprozess Durchführende					■

[1)] *diese Rollen nehmen nur wenige Aufgabe wahr und werden im Integrationsmodell nicht dargestellt*

Tabelle 17: Zusammenfassende Darstellung der ERM-Rollen[148]

Die Rollen *Kontrollprozess Verantwortliche* (ist für die Durchführung verantwortlich und delegiert unter Umständen die Durchführung) und *Kontrollprozess Durchführende* (führt die Kontrolle selbst durch) finden sich in keinen der betrachteten Rahmenwerke sondern wurden auf Basis der durchgeführten Interviews zusätzlich identifiziert.

Abbildung 34 zeigt das resultierende Integrationsmodell der *Ebene Organisation*. Neben den bisher beschriebenen Rollen wurde zudem der gesetzlichen Anforderung zur Bestellung eines Prüfungsausschusses nachgekommen[149].

[148] Quelle: eigene Darstellung in Anlehnung an [18, S. 173], [4], [21], [54] und den Erfahrungen des Autors

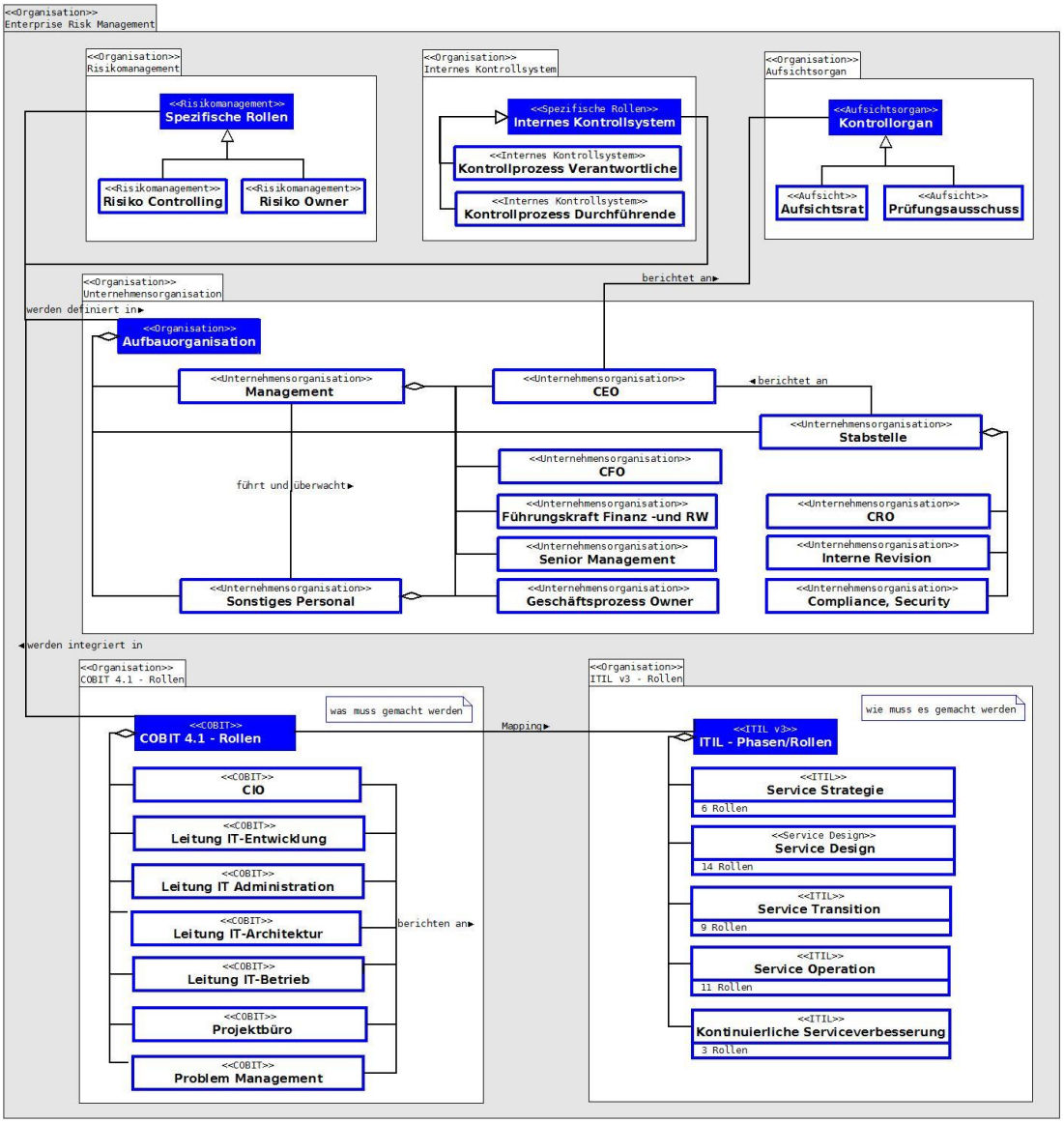

Abbildung 34: Darstellung des Integrationsmodells im Hinblick auf ERM-Rollen[150]

Die im Zuge der Rollendefinition durchgeführten Analysen, welche auch die Betrachtung der Aufgaben je Rolle inkludierten, stellen die Basis für die Identifikation der ERM Prozesse dar.

[149] Siehe zum Beispiel die Anforderungen in der 8. EU-Richtlinie [67, S. L 157/90] oder im URÄG [25, S. 9]

[150] Quelle: eigene Darstellung

5.1.3 Ebene Prozesse

Für die Analyse und Definition, der für das ERM relevanten Prozesse, wurde als Basisstruktur das COSO II Rahmenwerk gewählt. Dieses eignet sich, nach den Einschätzungen des Autors, sehr gut für eine allgemeingültige, lückenlose Darstellung. Die Identifikation der Prozesse erfolgte gemäß folgender Vorgangsweise:

- Identifikation von Prozessen in den einzelnen COSO Komponenten.
- Analyse und Identifikation der, nach den Einschätzungen des Autors, relevanten Prozesse, welche in den ISO Normen 27001 und 27005, der MaRisk sowie COBIT 4.1 erwähnt werden. Zuweisung der identifizierten Prozesse zu den einzelnen COSO Komponenten
- Zusammenfassung der Ergebnisse in Tabellenform. Für die ISO/IEC 27001 Norm wurde zudem angegeben, welcher Phase (Plan-Do-Check-Act) der Prozess zuzuordnen ist.
- Bei den identifizierten COBIT Prozessen wird jeweils die Domäne und Prozessnummer angegeben.
- Vergabe einer eindeutigen Prozess-ID (PID) und Aktivitäten-ID (AID) für das Mapping von Risikomanagement und IKS Aufgaben.
- Durchführung von Vereinfachungen als Basis für die Modellierung der Prozesse indem nur die identifizierten Hauptprozesse (mit PID) herangezogen wurden. Die, den Hauptprozessen nachgelagerten Aktivitäten (mit AID) werden für die Modellierung der Aktivitätendiagramms zur Umsetzung des statischen Integrationsmodells verwendet.

Das Ergebnis der Analyse ist in den Tabellen 20 bis 24 dargestellt. Die Modellierung der ERM-Prozesse, welche in den Abbildungen 35 bis 39 dargestellt ist, wurde anhand der Analyseergebnisse durchgeführt.

5.1.4 Ebene Systeme und Artefakte

Im Zuge der Identifizierung der Prozesse wurde analysiert, welche Systeme für die Umsetzung benötigt werden bzw. welche Artefakte daraus resultieren. Je Prozess wird hierbei zwischen Systemen und Artefakten des Risikomanagements und IKS unterschieden. Die in den Tabellen 20 bis 24 dargestellten Tabellen zeigen zudem die Zuweisung zu den jeweiligen Prozessen. Die Modellierung der Systeme und Artefakte, welche in den Tabellen 18 und 19 dargestellt ist erfolgte anhand der Analyseergebnisse. In der Folge werden diese Risikomanagement- und IKS-Systeme und Artefakte kurz beschrieben.

RISIKOMANAGEMENT	
System	**Artefakt**
Textverarbeitung zur Erstellung von Berichten, Anweisungen, Protokollen, usw.	Berichte, Anweisungen, Protokolle, Richtlinien, Interne Mitteilungen in freier oder gebundener Textform
Grafik-Anwendung zur Skizzierung von Aufbau- und Ablaufdiagrammen	Diagramme zur Beschreibung von Abläufen oder Zuständen
Business Intelligence Anwendung für Risiko Auswertungen, Planungen und Analysen	*Balanced Scorecards*[151] zur Zielfestlegung und Analyse der Plan/Ist Daten
Datenbank: zur Speicherung von ERM relevanten Datensätzen	Datenbank-Einträge der ERM relevanten Datensätze
Tabellenkalkulation für Analysen und Tracking Listen	Plandaten in Form von Budgetplänen sowie Kommunikationspläne zur Planung von periodischen Information an beteiligte Personen oder Organisationen
Risikomanagement-Anwendung: spezialisiertes System für die Dokumentation und Steuerung von Risiken	Risikolandkarten zur Darstellung des Risikoinventars, Risikobereitschaften und Risikotoleranzen

Tabelle 18: Risikomanagement Systeme und Artefakte[152]

INTERNES KONTROLLSYSTEM	
System	**Artefakt**
Textverarbeitung	Prüfprotokolle in freier oder gebundener Textform sowie Testprotokoll zur Überprüfung der Effizienz von Kontrollen
Business Intelligence Anwendung für Auswertungen, Planungen und Analysen von Kontrollen	Auswertungen für Kontrollen Performance Überwachungsergebnis zur Überprüfung der geplanten Ziele
Tabellenkalkulation	Maßnahmenpläne zur Überwachung von geplanten Aktivitäten
Datenbank	Datenbank-Abfrage zur Auswertung für Kontrollen
PDF-Software zur Erzeugung von revisionssicheren Dokumenten	Genehmigungen in Form von elektronischen oder manuellen Unterschriften
IKS Anwendung: spezialisiertes System für die Steuerung und Kontrolle von Risiken	Risikobericht zur Analyse der Umsetzungsqualität der Maßnahmen
HR Anwendung zum Eintrag von Verfehlungen und der Verwaltung von Empfangsbestätigungen Web Anwendung zur Verwaltung und Analyse von internen Umfrageergebnissen	Empfangsbestätigungen bei Aussendung von verbindlichen Vorgaben, Anweisungen oder Richtlinien

Tabelle 19: IKS Systeme und Artefakte[153]

[151] vgl. [98] - „*Die Balanced Scorecard ist ein Verbindungsglied zwischen Strategiefindung und -umsetzung. In ihrem Konzept werden die traditionellen finanziellen Kennzahlen durch eine Kunden-, eine interne Prozess- und eine Lern- und Entwicklungsperspektive ergänzt*“

[152] Quelle: eigene Darstellung

[153] Quelle: eigene Darstellung

COSO-Komponente	ID	Alt	Prozess Kurzbeschreibung	COSO Prozess	ISO/IEC 27001 Phase	ISO/IEC 27005 Prozess	MaRisk Anforderung	COBIT Domäne Prozess	Risikomanagement Artefakt	Risikomanagement System	Internes Kontrollsystem Artefakt	Internes Kontrollsystem System
Internes Umfeld	1		Risikomanagement Philosophie entwickeln	•					Interne allgemeine Richtlinie	Textverarbeitung	Auswertung Personal Umfrageergebnis	Business Intelligence Tabellenkalkulation Web Anwendung
	2		Grenzen des Anwendungsbereiches definieren (Kontext festlegen)		PLAN	•			Interne allgemeine Richtlinie	Textverarbeitung	Auswertung Personal Umfrageergebnis	Business Intelligence Tabellenkalkulation Web Anwendung
		a	Allgemeine ERM-Leitlinie definieren		PLAN				Interne allgemeine Richtlinie	Textverarbeitung	Auswertung Personal Umfrageergebnis	Business Intelligence Tabellenkalkulation Web Anwendung
	3		Allgemeinen Verhaltenskodex entwickeln	•			•		Interne allgemeine Richtlinie	Textverarbeitung	Personal Empfangsbestätigung	Tabellenkalkulation HR Anwendung
		a	Schulung und Bewusstseinsbildung umsetzen		DO				Datenbank-Eintrag Trainingsliste	Datenbank	Datenbank Abfrageergebnis	Datenbank
	4		Aufbau- und Ablauforganisation planen (Organisationsstruktur)	•		•			Organisationsrichtlinie	Textverarbeitung	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		a	Risikomanagement auf Gruppenebene implementieren (CRO)				•		Organisationsrichtlinie	Textverarbeitung	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		b	Risikocontrolling Funktion festlegen				•		Organisationsrichtlinie	Textverarbeitung	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		c	Compliance Funktion festlegen				•		Organisationsrichtlinie	Textverarbeitung	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		d	Risikosteuerungsprozesse implementieren				•		Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		e	Unvereinbare Tätigkeiten trennen				•		Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		f	Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege und -pflichten festlegen				•		Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		g	IT-Berechtigungen, Zeichnungsberechtigungen und sonstige entgeltrunte Kompetenzen regelmäßig und anlassbezogen überprüfen				•		Interne IT Richtlinie	Textverarbeitung	IT-Prüfprotokoll	PDF-Software Textverarbeitung
		h	Schnittstellen zu wesentlichen Auslagerungen (Outsourcing) regelmäßig und anlassbezogen überprüfen				•		Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		i	Organisationsrichtlinien schriftlich fixieren und intern kommunizieren				•		Interne Mitteilung	Textverarbeitung	Personal Empfangsbestätigung	Tabellenkalkulation HR Anwendung
		j	Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten durch die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse sicherstellen				•		Interne IT Richtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		k	Notfallkonzept für zeitkritische Prozesse implementieren				•		Interne IT Richtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		l	Budget für Risikomaßnahmenpläne sicherstellen					PO-9	Budgetplan	Business Intelligence Planungsanwendung	Budget Überwachung	Business Intelligence Planungsanwendung
		m	Aufsichtstätigkeiten durch den Aufsichtsrat ermöglichen					ME-4	Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Protokoll Aufsichtsratssitzung	Textverarbeitung
Zielfestlegung	5		Strategische Ziele festlegen	•		•			Balanced Score Card PLAN (gesamt)	Tabellenkalkulation Business Intelligence	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		a	Strategische Ziele dem Aufsichtsrat zur Kenntnis bringen und mit diesem erörtern			•			Interne Mitteilung	Textverarbeitung	Protokoll Aufsichtsratssitzung	Textverarbeitung
	6		Aus den strategischen Zielen abgeleitete Ziele definieren	•					Balanced Score Card PLAN (je Bereich)	Tabellenkalkulation Business Intelligence	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		a	Zukünftigen Kapitalbedarf planen			•			Balanced Score Card PLAN (Finanzperspektive)	Tabellenkalkulation Business Intelligence	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		b	Strategischen IT-Plan erstellen					PO-1	Balanced Score Card PLAN (IT)	Tabellenkalkulation Business Intelligence	Performance Überwachung	PDF-Software Tabellenkalkulation Business Intelligence
		c	IT-Programm-, Management-, Projekt- und Serviceportfolio analysieren					PO-1	Analyseprotokoll	Textverarbeitung Tabellenkalkulation	IT-Prüfprotokoll	PDF-Software Textverarbeitung
		d	Taktischen IT-Plan erstellen					PO-1	Interne IT Richtlinie	Textverarbeitung Tabellenkalkulation	Budget Genehmigung	Business Intelligence Planungsanwendung
		e	Portfolio- und Programmmanagement Rahmenwerk für IT-Investitionen definieren					PO-10	Interne IT Richtlinie	Textverarbeitung Tabellenkalkulation	Budget Genehmigung	Business Intelligence Planungsanwendung
		f	IT-Sicherheitsplan erstellen (und aufrechterhalten)					DS-5	Interne IT Richtlinie	Textverarbeitung Tabellenkalkulation	Budget Genehmigung	Business Intelligence Planungsanwendung
		g	Technische Maßnahmen und Verfahren zum Informationsschutz in Netzwerken implementieren					DS-5	Interne IT Richtlinie	Textverarbeitung	IT-Prüfprotokoll	PDF-Software Textverarbeitung
		h	Verfahren zur Datenwiederherstellung definieren und implementieren					DS-11	Interne IT Richtlinie	Textverarbeitung	IT-Prüfprotokoll	PDF-Software Textverarbeitung
	7		Risikobereitschaft festlegen	•					Risikolandkarte (PLAN)	Tabellenkalkulation	Prüfprotokoll	PDF-Software Textverarbeitung
		a	Kriterien für die Risikoakzeptanz festlegen			•			Risikolandkarte (PLAN)	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
	8		Risikotoleranzen festlegen	•					Risikolandkarte (PLAN)	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung

Tabelle 20: Prozessanalyse - COSO Komponente *Internes Umfeld* und *Zielfestlegung*[154]

[154] Quelle: eigene Darstellung in Anlehnung an [4], [18], [12], [14], [54]

COSO-Komponente	ID		Prozess Kurzbeschreibung	COSO Prozess	ISO/IEC 27001 Phase	ISO/IEC 27005 Prozess	MaRisk Anforderung	COBIT Domäne Prozess	Risikomanagement Artefakt	Risikomanagement System	Internes Kontrollsystem Artefakt	Internes Kontrollsystem System
Ereignisidentifikation	9		Risiken (Ereignisse) identifizieren	•	PLAN	•	•		Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		a	Vermögenswerte identifizieren			•			Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		b	Bedrohungen und daraus resultierende Konsequenzen identifizieren			•			Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		c	Schwachstellen und daraus resultierende Konsequenzen identifizieren			•	•		Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		d	Risiken, ausgelagerter Aktivitäten identifizieren (Outsourcing)						Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		e	Bedeutende Schadensfälle unverzüglich hinsichtlich ihrer Ursachen analysieren				•		Prüfprotokoll	Datenbank	Prüfprotokoll	Textverarbeitung IKS Anwendung
		f	Kritische IT-Abhängigkeiten und Performance identifizieren					PO-1	Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		g	Ereignisse, die mit IT-Zielen zusammenhängen identifizieren					PO-5	Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
	10		Ereignisse und Ziele verknüpfen	•					Risikoinventurliste	Business Intelligence Planungsanwendung	Budget Genehmigung	Business Intelligence Planungsanwendung
		a	Kerngeschäftsziele mit IT Zielen verlinken					PO-1	Risikoinventurliste	Business Intelligence Planungsanwendung	Budget Genehmigung	Business Intelligence Planungsanwendung
	11		Methoden zur Ereignisidentifikation festlegen	•			•		Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	Tabellenkalkulation
		a	Angemessenheit der Methoden und Verfahren zumindest jährlich durch die fachlich zuständigen Mitarbeiter überprüfen				•		Interne allgemeine Verfahrensrichtlinie	Texterarbeitung IKS Anwendung	Testprotokoll	Texterarbeitung IKS Anwendung
	12		Ereignisvarianten entwickeln	•					Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		a	Ereignisse kategorisieren	•					Risikoinventurliste	Datenbank	Budget Genehmigung	Datenbank
		b	Überblick über Wesentlichkeit regelmäßig und anlassbezogen verschaffen				•		Prüfprotokoll	Texterarbeitung IKS Anwendung	Testprotokoll	Texterarbeitung IKS Anwendung
	13		Beziehung zwischen den die Zielerreichung beeinflussenden Ereignissen analysieren	•					Analyseprotokoll	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
Risikobewertung	14		Inhärente und verbleibende Risiken analysieren und beurteilen/bewerten	•	PLAN	•	•	PO-5	Bewertungsprotokoll	Datenbank Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		a	Vorgehensweise zur Risikoeinschätzung festlegen		PLAN				Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
		b	Kriterien für die Risikoabschätzung festlegen			•	•		Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
		c	Kriterien für die Risikoauswirkung festlegen			•	•		Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
	15		Risikobeurteilungen auf Gesamtorganisations-Niveau darstellen	•					Bewertungsprotokoll	Datenbank Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		a	Auswirkungen in verschiedenen Unternehmensbereichen analysieren und darstellen	•		•			Bewertungsprotokoll	Datenbank Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		b	IT-Performance beurteilen und verbessern					ME-1	Bewertungsprotokoll	Datenbank Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
Risikosteuerung	16		Risikosteuerungsmaßnahmen festlegen	•		•			Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
		a	Optionen für die Risikobehandlung bewerten		PLAN				Bewertungsprotokoll	RM-Anwendung Texterarbeitung	Prüfprotokoll	Texterarbeitung IKS Anwendung
		b	Maßnahmen und Maßnahmenziele auswählen		PLAN				Bewertungsprotokoll	RM-Anwendung Texterarbeitung	Prüfprotokoll	Texterarbeitung IKS Anwendung
		c	Zustimmung zu den Restrisiken vom Management einholen		PLAN				Interne allgemeine Verfahrensrichtlinie	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		d	ISMS durch das Management genehmigen		PLAN				Interne allgemeine Verfahrensrichtlinie	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		e	Erklärung zur Anwendbarkeit erstellen		PLAN				Anwendbarkeitsbericht	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
		f	Risikobehandlungsplan formulieren		DO		•	PO-5	Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
		g	Risiken reduzieren, akzeptieren, vermeiden, übertragen	•		•	•		Prüfprotokoll	Texterarbeitung IKS Anwendung	Testprotokoll	Texterarbeitung IKS Anwendung
		h	Internen Prozess zur Sicherstellung der Risikotragfähigkeit einrichten				•		Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
		i	Erstellung einen Ansatzes zur Überwachung von IT-Risiken					ME-1	Interne allgemeine Verfahrensrichtlinie	Texterarbeitung	Prüfprotokoll	PDF-Software Texterarbeitung
	17		Auswirkungen der Risikosteuerungsmaßnahmen auf das verbleibende Risiko darstellen	•					Bericht verbleibende Risiken	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
	18		Kosten/Nutzen der Risikosteuerungsmaßnahmen evaluieren	•					Analyseprotokoll	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung
	19		Portfolio- Sicht auf verbleibende Risiken darstellen	•					Bericht Risikoportfolio	Texterarbeitung Tabellenkalkulation	Prüfprotokoll	Texterarbeitung IKS Anwendung

Tabelle 21: Prozessanalyse - COSO Komponente *Ereignisidentifikation, Risikobewertung* und *Risikosteuerung*[155]

[155] Quelle: eigene Darstellung in Anlehnung an in Anlehnung an [4], [18], [12], [14], [54]

COSO-Komponente	PID	ADD	Prozess Kurzbeschreibung	COSO Prozess	ISO/IEC 27001 Phase	ISO/IEC 27005 Prozess	MaRisk Anforderung	COBIT Domäne Prozess	Risikomanagement Artefakt	Risikomanagement System	Internes Kontrollsystem Artefakt	Internes Kontrollsystem System
Kontrollaktivitäten	20		Kontrollaktivitäten zur Sicherstellung der Umsetzung der Maßnahmen festlegen	•				PO-5	Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		a	Risikobehandlungsplan definieren		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung IKS Anwendung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		b	Maßnahmen und Ziele auswählen		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung IKS Anwendung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		c	Maß der Wirksamkeit der Kontrollen definieren		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		d	Verfahren für die Verwaltung von Betrieb und Ressourcen definieren		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		e	Verfahren für die sofortige Erkennung von Sicherheitsereignissen definieren		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		f	Verfahren für die Reaktion auf Sicherheitsvorfälle definieren		DO		•		Interne allgemeine Verfahrensrichtlinie	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		g	Existierende Kontrollen identifizieren			•			Analyseprotokoll	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung IKS Anwendung
		h	Budget für Risikomaßnahmenpläne festlegen					PO-5	Budgetplan	Business Intelligence Planungsanwendung	Budget Genehmigung	Business Intelligence Planungsanwendung
		i	IT-Projektüberwachungs, -messungs- und -managementsystem festlegen					PO-10	Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
	21		Kontrollen durchführen		DO	•			Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		a	Verfahren zur Überwachung und Überprüfung ausführen		CHECK				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		b	Wirksamkeit der Kontrollen (ISMS) regelmäßig überprüfen		CHECK				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		c	Wirksamkeit von Maßnahmen messen		CHECK				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		d	Risikoeinschätzungen, Restrisiken und des akzeptables Risikoniveaus regelmäßig überprüfen		CHECK				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		e	Sicherheitspläne aktualisieren		CHECK				Analyseprotokoll	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		f	Einflüsse auf die Wirksamkeit der Kontrollen erkennen		CHECK				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		g	Regelmäßig sowie anlassbezogen angemessene Stresstests durchführen				•		Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		h	Risiken die Vermögenslage (inklusive Kapitalausstattung), die Ertragslage oder die Liquiditätslage wesentlich beeinträchtigen können prüfen				•		Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		i	Sicherheitsverletzungen monitoren					DS-5	Prüfprotokoll	Textverarbeitung IKS Anwendung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		j	Verletzbarkeits- und Schwachstellenanalysen regelmäßig durchführen					DS-5	Analyseprotokoll	Textverarbeitung Tabellenkalkulation	Testprotokoll	Textverarbeitung IKS Anwendung
		k	(IT) Compliance überwachen					ME-3	Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		l	IT-Performance, Ressourcen und RM im Einklang mit der Unternehmensstrategie überwachen					ME-4	Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
Information & Kommunikation	22		Informationsflüsse darstellen	•					Aktivitätendiagramm	UML-Anwendung	Prüfprotokoll	Textverarbeitung
	23		Gezielte und direkte Kommunikation planen und durchführen	•					Aktivitätendiagramm	UML-Anwendung	Prüfprotokoll Interne Revision	Textverarbeitung
		a	Maßnahmen und Verbesserungen an alle Beteiligten kommunizieren		ACT				Interne Mitteilung	Tabellenkalkulation	Prüfprotokoll Interne Revision	Textverarbeitung
		b	Erfahrungen und Aktionen an betroffene Stellen kommunizieren		ACT	•			Interne Mitteilung	Textverarbeitung	Prüfprotokoll Interne Revision	Textverarbeitung
		c	Inhalte sowie Änderungen der Strategien innerhalb des Instituts in geeigneter Weise kommunizieren				•		Interne Mitteilung	Textverarbeitung	Prüfprotokoll Interne Revision	Textverarbeitung

Tabelle 22: Prozessanalyse - COSO Komponente *Kontrollaktivitäten* und *Information & Kommunikation*[156]

[156] Quelle: eigene Darstellung in Anlehnung an in Anlehnung an [4], [18], [12], [14], [54]

COSO-Komponente	PID	AID	Prozess Kurzbeschreibung	COSO Prozess	ISO/IEC 27001 Phase	ISO/IEC 27005 Prozess	MaRisk Anbindung	COBIT Domäne Prozess	Risikomanagement Artefakt	Risikomanagement System	Internes Kontrollsystem Artefakt	Internes Kontrollsystem System
Überwachung	24		Laufende Überwachungstätigkeiten definieren	•					Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
	25		ERM-Betrieb und Ressourcen analysieren und verwalten		DO				Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		a	Identifizierte Verbesserungen umsetzen		ACT				Maßnahmenprotokoll	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung IKS Anwendung
		b	Geeignete Korrektur- und Vorbeugungsmaßnahmen durchführen		ACT				Maßnahmenprotokoll	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung IKS Anwendung
		c	Sicherheitserfahrungen mit einbeziehen		ACT				Maßnahmenprotokoll	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung IKS Anwendung
		d	Beabsichtigte Zielerreichung sicherstellen		ACT				Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		e	Ansatz zur Überwachung von IT-Risiken erstellen					ME-1	Interne IT Richtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
		f	Sicherheitsereignisse überwachen					DS-5	Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		g	Auswirkung und Priorisierung von Changes bewerten					AI-6	Analyseprotokoll	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung IKS Anwendung
		h	Durchlaufen jeder kritische Änderung (Change) durch den Genehmigungsprozess sicherstellen					AI-6	Prüfprotokoll	Textverarbeitung IKS Anwendung	Testprotokoll	Textverarbeitung IKS Anwendung
		i	Gesondete Beurteilungen durchführen	•					Anweisung der Geschäftsführung	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	26		Interne Audits risikoorientiert und prozessunabhängig durchführen	•	CHECK		•		Prüfprotokoll Interne Revision	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		a	Tätigkeit der Internen Revision auf einem umfassenden und jährlich fortzuschreibenden Prüfungsplan ausrichten						Interner Auditplan	Textverarbeitung Tabellenkalkulation	Prüfprotokoll	Textverarbeitung
		b	Schriftliche Berichte über Interne Audits verfassen				•		Prüfprotokoll Interne Revision	Textverarbeitung	Prüfprotokoll	Textverarbeitung
		c	Bei schwerwiegenden Feststellungen gegen Geschäftsleiter der Geschäftsleitung unverzüglich Bericht erstatten				•		Ad-hoc Auditbericht	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		d	Bei schwerwiegenden Feststellungen gegen Geschäftsleiter unverzüglich den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstitutionen informieren (GL kommt die Geschäftsleitung ihrer Berichtspflicht nicht nach oder beschließt sie keine sachgerechten Maßnahmen, so hat die Interne Revision den Vorsitzenden des Aufsichtsorgans zu unterrichten)				•		Ad-hoc Auditbericht	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		f	Bei nicht erbrachter Mängelbeseitigung die Geschäftsleitung spätestens im Rahmen des nächsten Gesamtberichts schriftlich über die noch nicht beseitigten Mängel unterrichten				•		Prüfprotokoll Interne Revision	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		g	Aufsichtsorgan mindestens einmal jährlich über die von der Internen Revision festgestellten schwerwiegenden sowie über die noch nicht behobenen wesentlichen Mängel in inhaltlich prägnanter Form unterrichten				•		Mängelprotokoll	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
		e	Fristgerechte Beseitigung der bei der Prüfung festgestellten Mängel in geeigneter Form durch die IT überwachen (Gegebenenfalls hierzu eine Nachschauprüfung ansetzen)					ME-4	Maßnahmenprotokoll	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	27		Externen Audits zur Beurteilung der Performance und Compliance periodisch beauftragen					ME-4	Externer Auditbericht	Textverarbeitung	Maßnahmenplan	Textverarbeitung
	28		Einheitliche Berichte (intern und extern) definieren	•					Interne allgemeine Verfahrensrichtlinie	Textverarbeitung	Prüfprotokoll	PDF-Software Textverarbeitung
	29		Mängelberichte erstellen	•					Mängelprotokoll	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	30		Aufsichtsorgan über die Risikosituation in angemessener Weise schriftlich informieren				•		Risikobericht	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	31		Geschäftsleitung in angemessenen Abständen über die Risikosituation berichten				•		Risikobericht	Textverarbeitung RM-Anwendung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	32		Die Geschäftsleitung mindestens jährlich über bedeutende Schadensfälle und wesentliche operationelle Risiken unterrichten				•		Risikobericht	Textverarbeitung RM-Anwendung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	33		(IT) Governance Report erstellen					ME-4	Governance Bericht	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung
	34		Über die IT-Performance Bericht erstatten					ME-1	IT Performance Bericht	Textverarbeitung	Prüfprotokoll	Textverarbeitung IKS Anwendung

Tabelle 23: Prozessanalyse - COSO Komponente *Überwachung*[157]

[157] Quelle: eigene Darstellung in Anlehnung an in Anlehnung an [4], [18], [12], [14], [54]

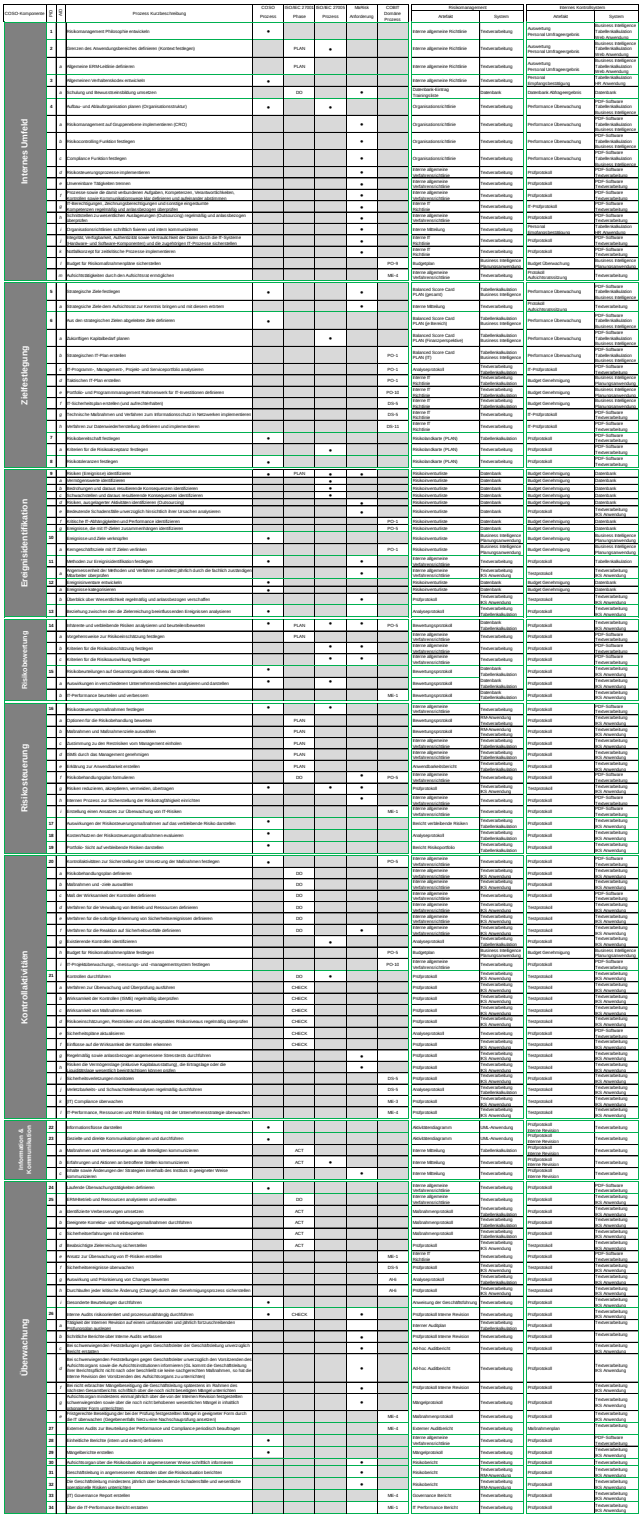

Tabelle 24: Gesamtansicht der identifizierten ERM Prozesse[158]

[158] Quelle: eigne Darstellung in Anlehnung an in Anlehnung an [4], [18], [12], [14], [54]

Die Abbildungen 35 bis 39 veranschaulichen die Modellierung der statischen Betrachtungsweisen der ERM Prozesse auf Basis der COSO Komponenten inklusive der Aspekte der ISO Normen 27001 und 27005, der MaRisk sowie der COBIT Prozesse. Die Risikomanagementprozesse sind in blauer und die IKS Prozesse in roter Farbumrahmung dargestellt. Die Verlinkung zwischen den dargestellten Klassen liefert einen Hinweis für das Mapping von Risikomanagement- und IKS Aufgaben.

COSO Komponenten *Internes Umfeld* und *Zielfestlegung*

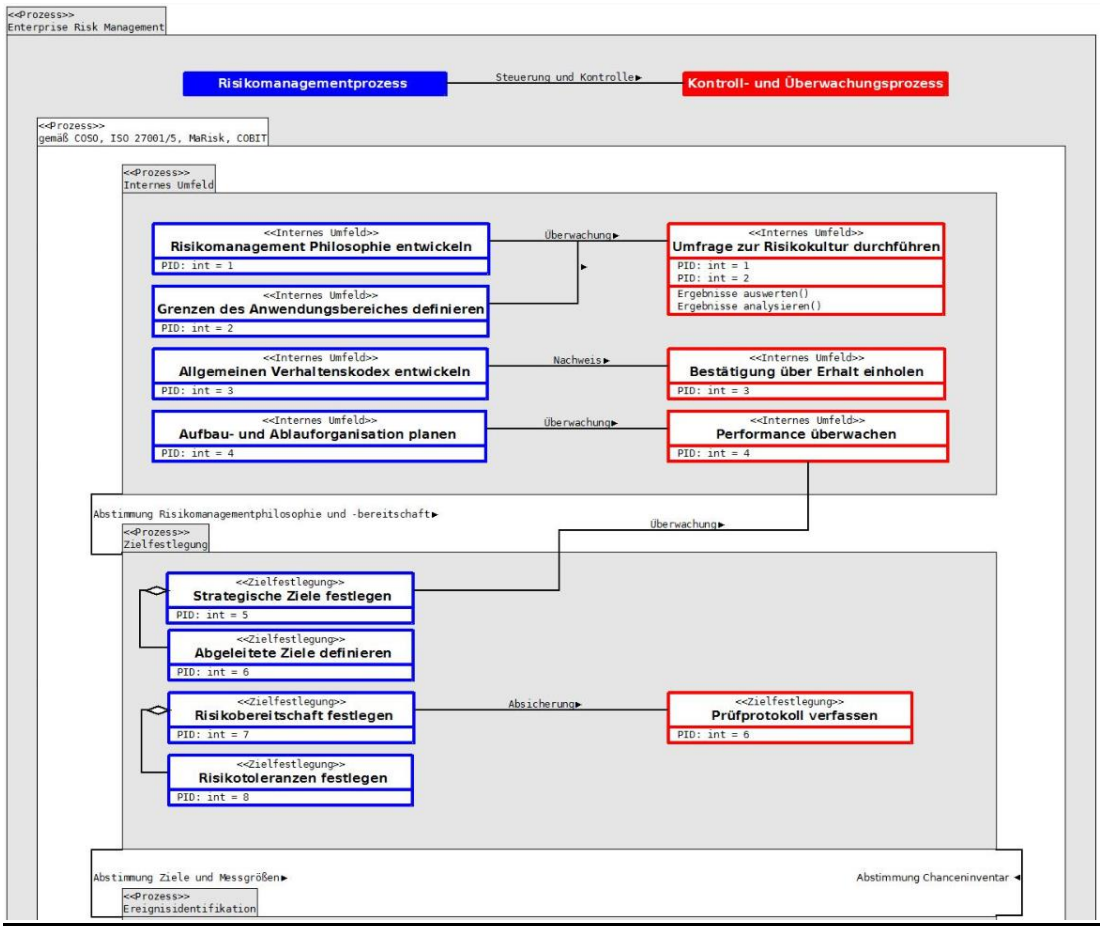

Abbildung 35: Statisches Integrationsmodell der Prozesssicht (Ausschnitt)[159]

Die in den Klassen enthaltene Prozess-ID (PID) verweist auf den Eintrag in den Tabellen 20 bis 24. Zudem ist der Übergang zwischen den einzelnen UML-Paketen dargestellt, welcher einen Aufschluss über die vertikale Integration liefert. Im gegenständlichen Fall in Abbildung 35 muss die Risikomanagement Philosophie und die einhergehende Risikobereitschaft übereinstimmen. Außerdem werden Ziele und Messgrößen für die Ereignisidentifikation festgelegt. Nach der

[159] Quelle: eigene Darstellung in Anlehnung an [4], [18], [12], [14], [54]

Ereignisidentifikation erfolgt eine Abstimmung bzw. Aktualisierung des Chanceninventars.

COSO Komponenten *Ereignisidentifikation* und *Risikobewertung*

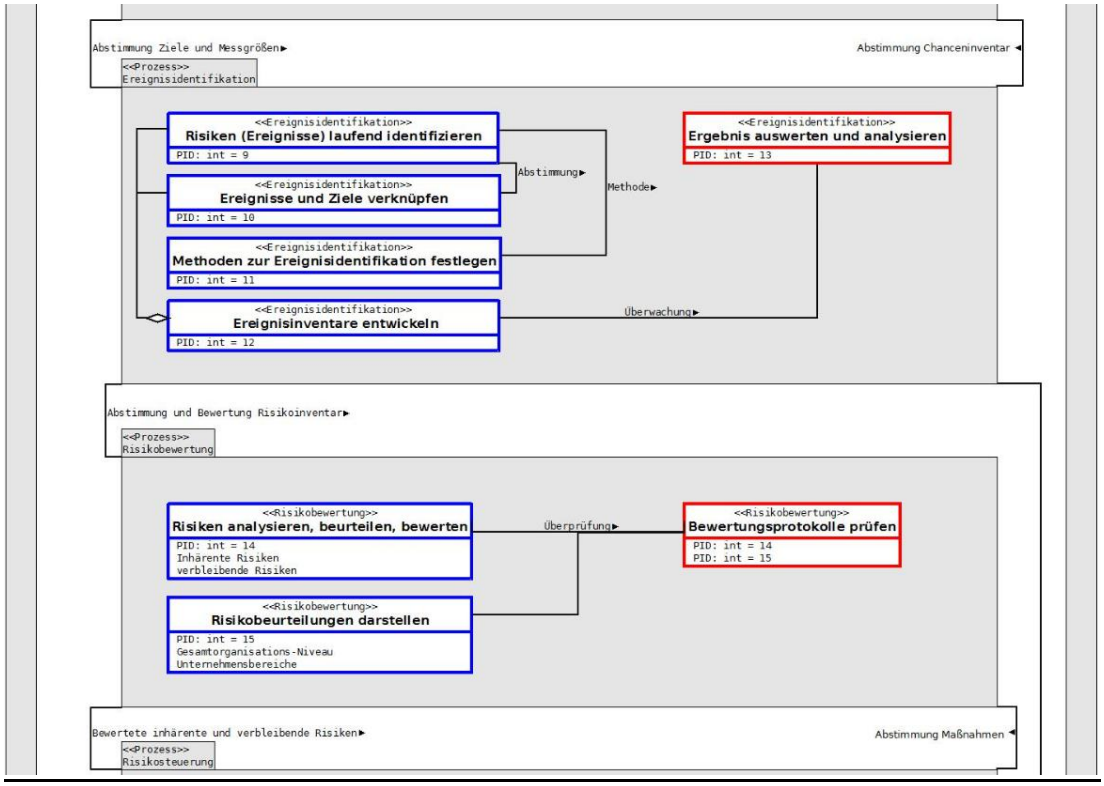

Abbildung 36: Statisches Integrationsmodell der Prozesssicht (Ausschnitt)[160]

Ereignisse sind, gemäß COSO II, mit Risiken gleichzusetzen. Das Ergebnis der Komponente Ereignisidentifikation ist ein Inventar an Risiken. Im Paket Risikobewertung werden die identifizierten Risiken mit verschiedenen Methoden beurteilt. Damit werden konkrete Ansatzpunkte in Form von Zahlen für die, im nächsten Schritt folgende, Risikosteuerung definiert.

[160] Quelle: eigene Darstellung in Anlehnung an [4], [18], [12], [14], [54]

COSO Komponenten *Risikosteuerung, Kontrollaktivitäten* und *Information & Kommunikation*

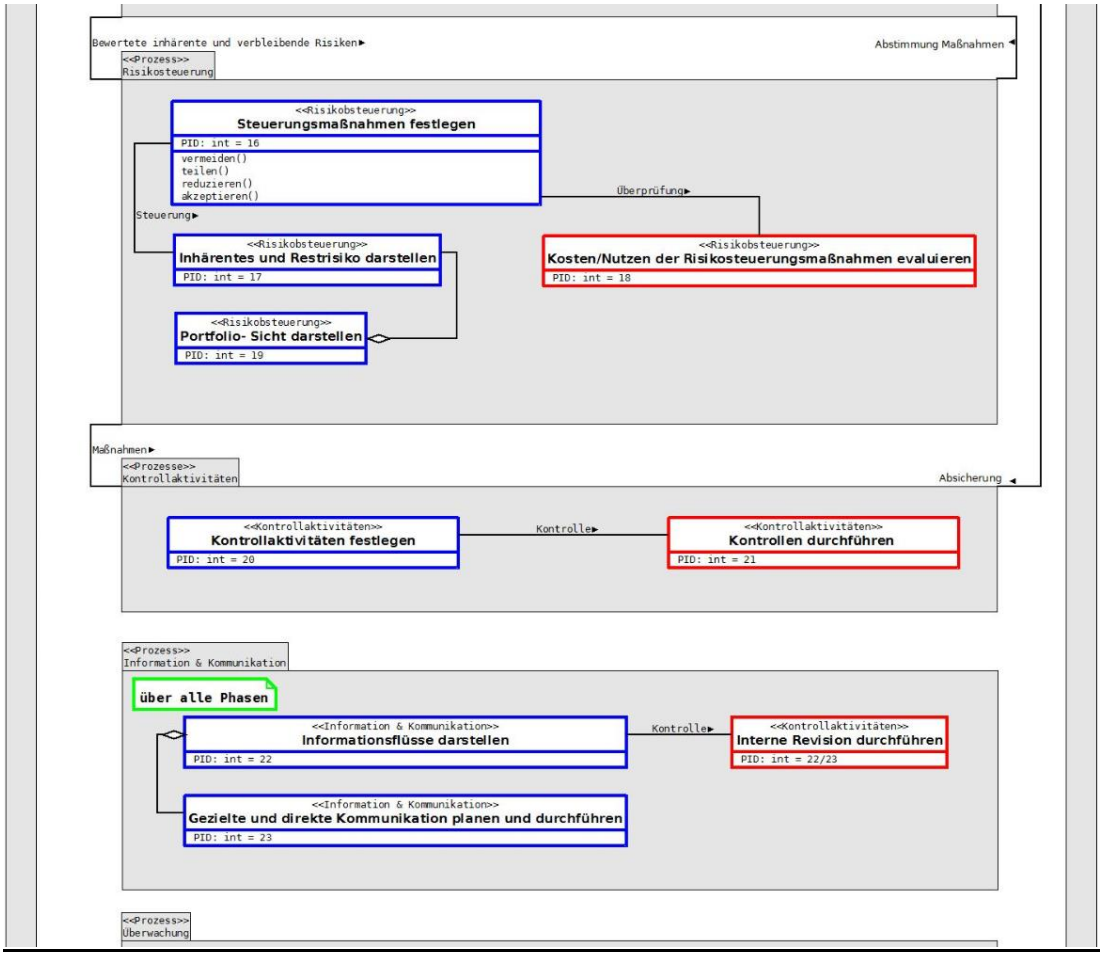

Abbildung 37: Statisches Integrationsmodell der Prozesssicht (Ausschnitt)[161]

Durch die Festlegung der Risikosteuerungsmaßnahmen werden Kontrollaktivitäten ausgelöst, welche eine Steuerung für die identifizierten Ereignisse vornehmen.

Die Komponente *Information und Kommunikation*, welche mit allen anderen Paketen verbunden ist, weist darauf hin, dass das unternehmensweite Risikomanagement durch eine gezielte interne und externe Informationspolitik unterstützt wird. Die Interne Revision überwacht hierbei die Informationsflüsse im Sinne der richtigen Informationen zum richtigen Zeitpunkt am richtigen Ort.

[161] Quelle: eigene Darstellung in Anlehnung an [4], [18], [12], [14], [54]

COSO Komponenten *Überwachung*

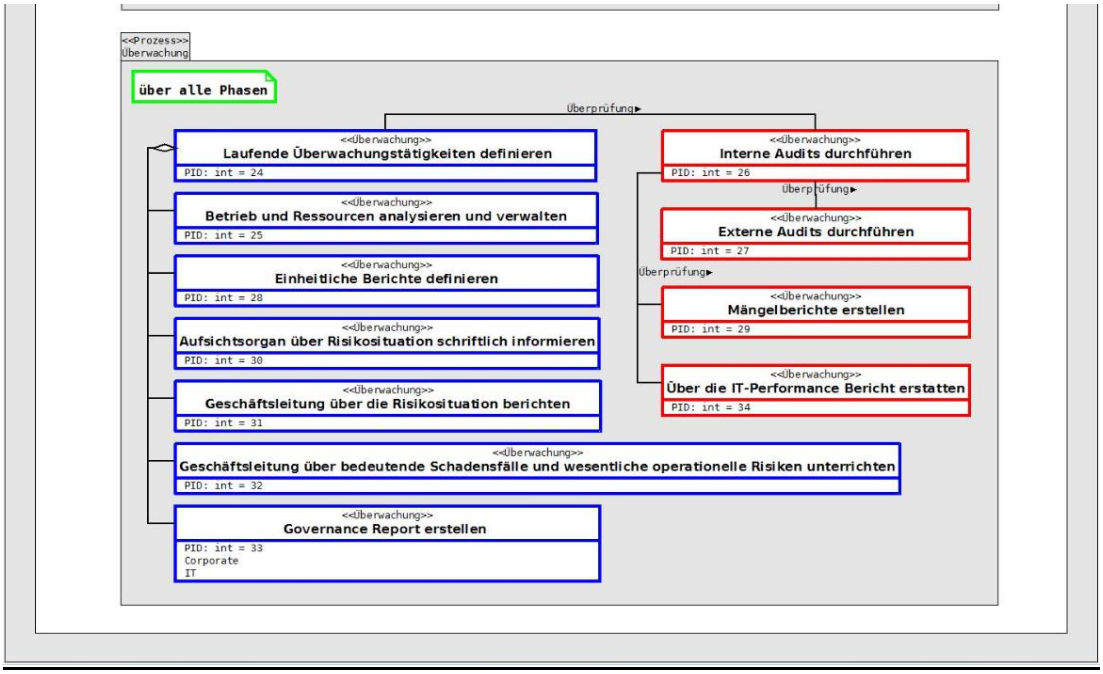

Abbildung 38: Statisches Integrationsmodell der Prozesssicht (Ausschnitt)[162]

Die Komponente *Information und Kommunikation* ist, wie erwähnt, mit allen anderen Paketen verbunden und zeigt verschiedene Aktivitäten zur Definition von Überwachungs- und Berichtstätigkeiten sowie konkrete Ansatzpunkte zur Durchführung von Überprüfungen.

Abbildung 39 zeigt das gesamte ERM Prozessmodell. Es wurden insgesamt 27 Klassen im Bereich Risikomanagement sowie 14 im Bereich IKS modelliert. Das bedeutet eine wesentliche Vereinfachung gegenüber der Prozess Analyse in Tabelle 24 mit insgesamt 131 identifizierten Prozessen. Die vereinfachte Darstellung wurde gewählt, um die Übersichtlichkeit über das gesamte Integrationsmodell zu bewahren. Da jede Organisation den Ausprägungsgrad des unternehmensweiten Risikomanagements selbst bestimmt[163] stellt diese vereinfachte Sichtweise einen allgemein gültigen, generellen Rahmen für die ERM Prozesse dar, welcher bei Bedarf durch die Inhalte der Analysen in Tabelle 24 beliebig erweitert werden kann.

[162] Quelle: eigene Darstellung in Anlehnung an [4], [18], [12], [14], [54]
[163] vgl. die Ausführungen zu den Organisationsrichtlinien in [54, S. 14]

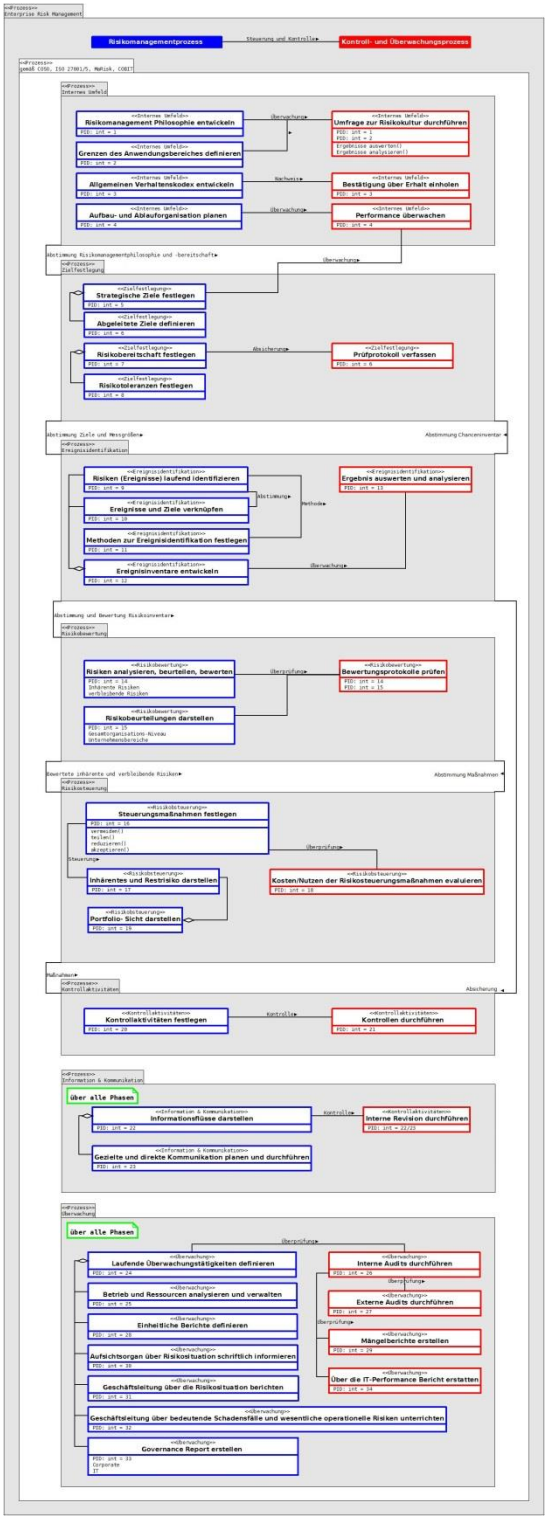

Abbildung 39: Gesamtsicht der modellierten ERM Prozesse[164]

[164] Quelle: eigene Darstellung

Abbildung 40 zeigt die für die Umsetzung von Risikomanagement und IKS maßgeblichen Systeme.

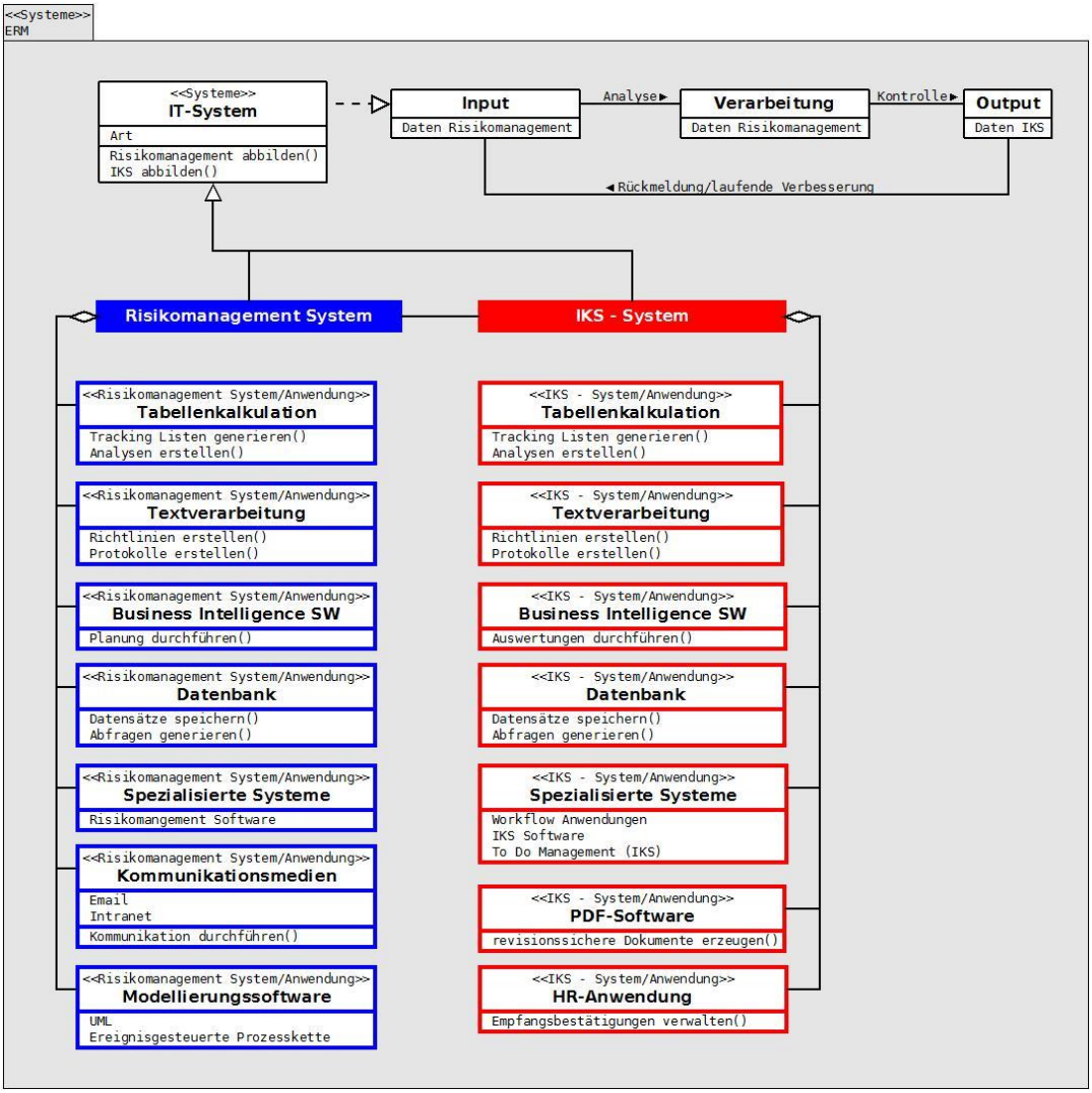

Abbildung 40: Gesamtsicht der modellierten ERM Systeme[165]

Die Auswahl der Systeme wurde nach den Einschätzungen und Erfahrungen des Autors vorgenommen und erhebt keinen Anspruch auf Vollständigkeit. Für die Bildung des Integrationsmodells und der Vorgangsweise zur Umsetzung ist in diesem Kontext lediglich wichtig, dass Systeme, welche die Risikomanagement und IKS Prozesse ausführen, identifiziert und bewertet werden.

[165] Quelle: eigene Darstellung

Abbildung 41 veranschaulicht unterschiedliche Artefakte, welche die Ergebnisse der, durch die identifizieren Systeme ausgeführten, Prozesse darstellen während Abbildung 42 wird das gesamte, statische Integrationsmodell dargestellt.

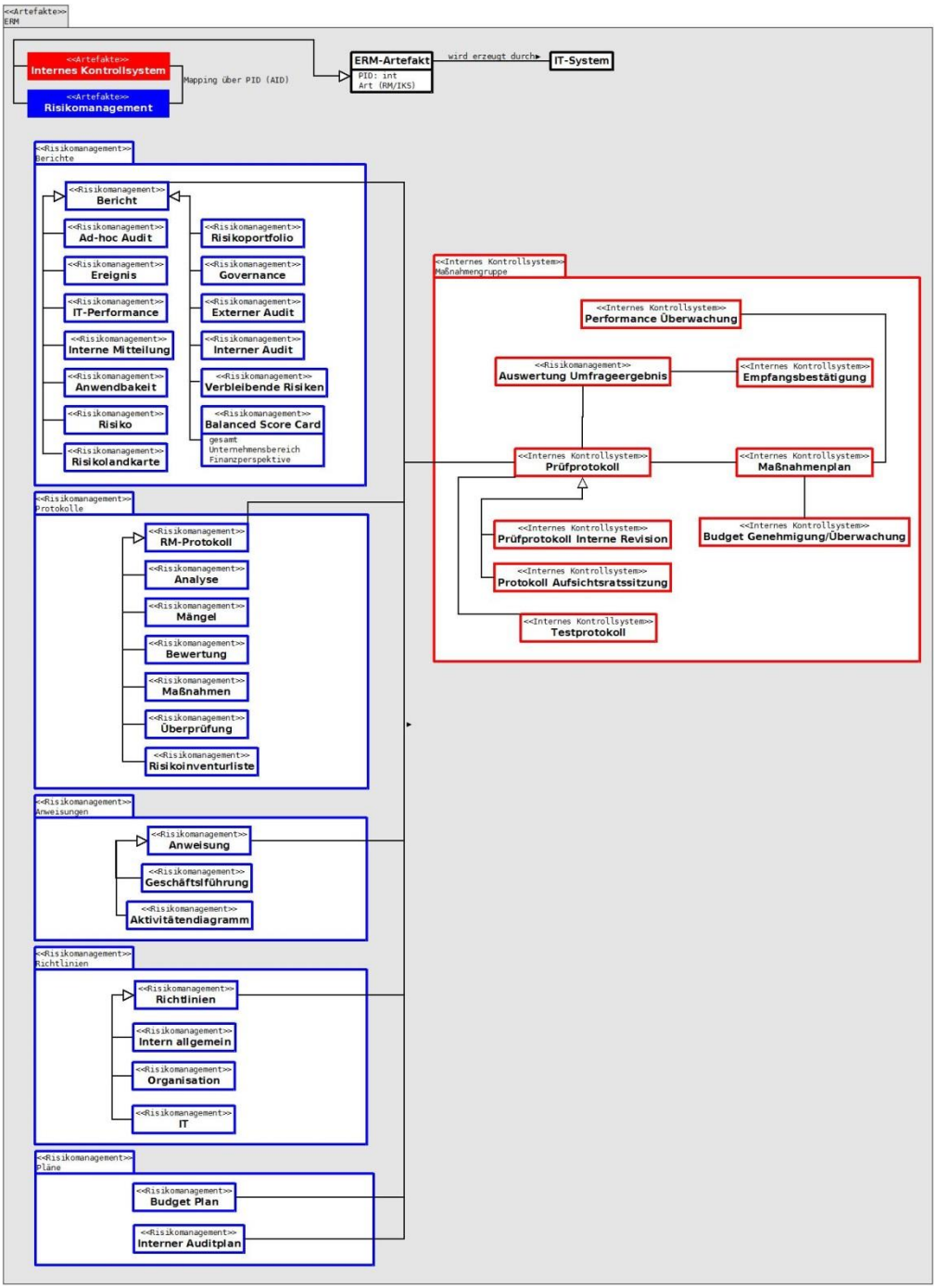

Abbildung 41: Gesamtansicht der modellierten ERM Artefakte[166]

[166] Quelle: eigene Darstellung

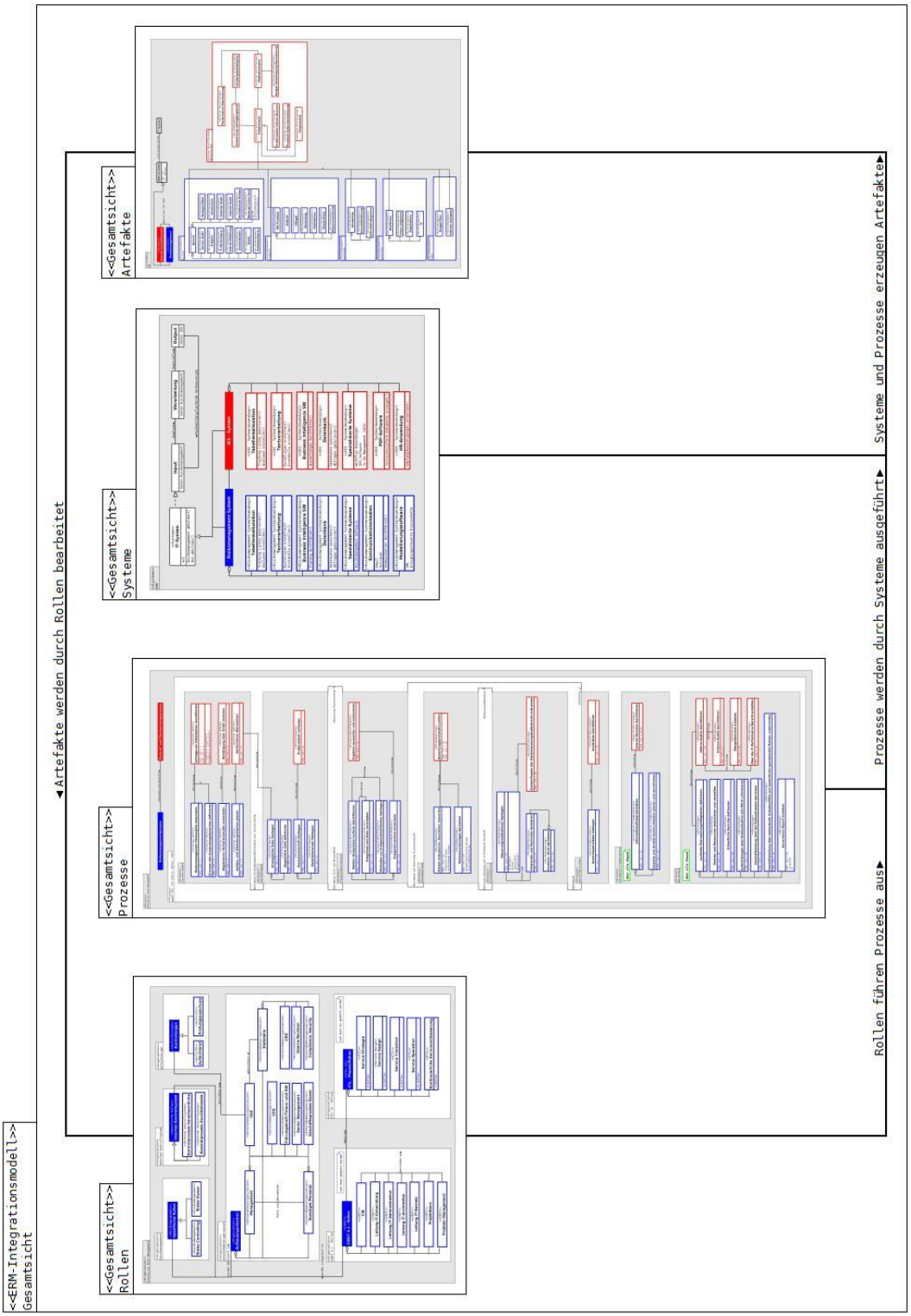

Abbildung 42: Gesamtansicht des statischen Integrationsmodells[167]

[167] Quelle: eigene Darstellung

5.2 Vorgehensmodell zur Umsetzung der Integration

Nach der Modellierung der statischen Aspekte des Integrationsmodells im vorigen Abschnitt wird in der Folge das Vorgehensmodell zur operationellen Umsetzung der Integration in Form von UML-Aktivitätendiagrammen dargestellt. Das Ziel der Modellierung ist, den nach COSO vorgegebenen Idealzustand in der operationellen Umsetzung zu erreichen. Wie bereits mehrfach im Rahmen der vorliegenden Arbeit erwähnt, verfügen die in Abschnitt vier dargestellten Vorgaben über keine ausreichenden Informationen über konkrete Handlungsanweisungen in diesem Kontext. Die Modellierung erfolgte daher nach den Erfahrungen und Einschätzungen des Autors.

Die Inhalte der modellierten Elemente orientieren sich an den Ausführungen in Abschnitt 5.1.3, welcher die Prozesssicht des statischen Integrationsmodells darstellt. Neben den, in den Mapping Tabellen enthaltenen Prozess-IDs (PID) werden hierfür auch die dargestellten Aktivitäten, welche jeweils mit Aktivitäten-IDs (AID) versehen sind, berücksichtigt. Aufgrund der großen Anzahl an nebenläufigen Aktivitäten und fehlenden Handlungsanweisungen in diesem Zusammenhang entsprechen die Diagramme nicht exakt der UML Syntax. Die dargestellten Abläufe werden lediglich auf Basis der Hauptaufgaben (PIDs, grün unterlegte Elemente) modelliert. Die Unteraufgaben (AID, weiß unterlegte Elemente) werden hierbei den Hauptaufgabe zugeordnet, jedoch nicht in eine stringente Reihenfolge gebracht.

5.2.1 Struktur des Prozessmodells

Abbildung 43 veranschaulicht das Prozessmodell zur Umsetzung der Integration anhand der in COSO II enthaltenen Komponenten in vereinfachter Form im Überblick. Jede Komponente sieht hierbei einen Validierungsschritt vor, mit welchem die in der jeweiligen Komponente gesetzten Maßnahmen überwacht werden. Nach der Komponente *Überwachungsaktivitäten durchführen* befindet sich eine Verzweigung, welche zu allen anderen Komponenten des Diagramms führt. Diese zeigt, dass der Prozess den unternehmensweiten Risikomanagements nie endet sondern laufend verbessert wird[168].

Die modellierten Detailansichten des Prozessmodells werden in den Abbildungen 44 bis 51 dargestellt[169]. Die Gesamtansicht des Modells ist in Abbildung 52 zu sehen. Die für das Risikomanagement relevanten Aktivitäten sind in den blau umrandeten Paketen zu finden, während sämtliche IKS-Pakete in roter Umrandung dargestellt sind. Grün unterlegte Elemente stellen die Hauptaktivitäten dar und können in eine

[168] Siehe dazu die Bemerkungen in [21, S. 17] welche das *Enterprise Risk Management* als Prozess im Sinne eines kontinuierlichen und wiederholten Zusammenspiels von Aktivitäten, die in einer Organisation stattfinden, beschreibt

[169] Da es sich bei diesen Abbildungen nur um Teilsegmente handelt fehlt die Startphase. Diese ist in der Gesamtansicht dargestellt. Die Reihenfolge einiger Modellelemente kann frei gewählt werden. Aus diesem Grund fehlen einzelne Teile des Kontrollflusses. In dieser Hinsicht wurde die formale UML Methode eines *Aktivitätendiagramms* nicht eingehalten

Reihenfolge gebracht werden. Die Aktivitäten in weißer Farbe sind den Hauptaktivitäten zugeordnet und können in beliebiger Reihenfolge abgearbeitet werden.

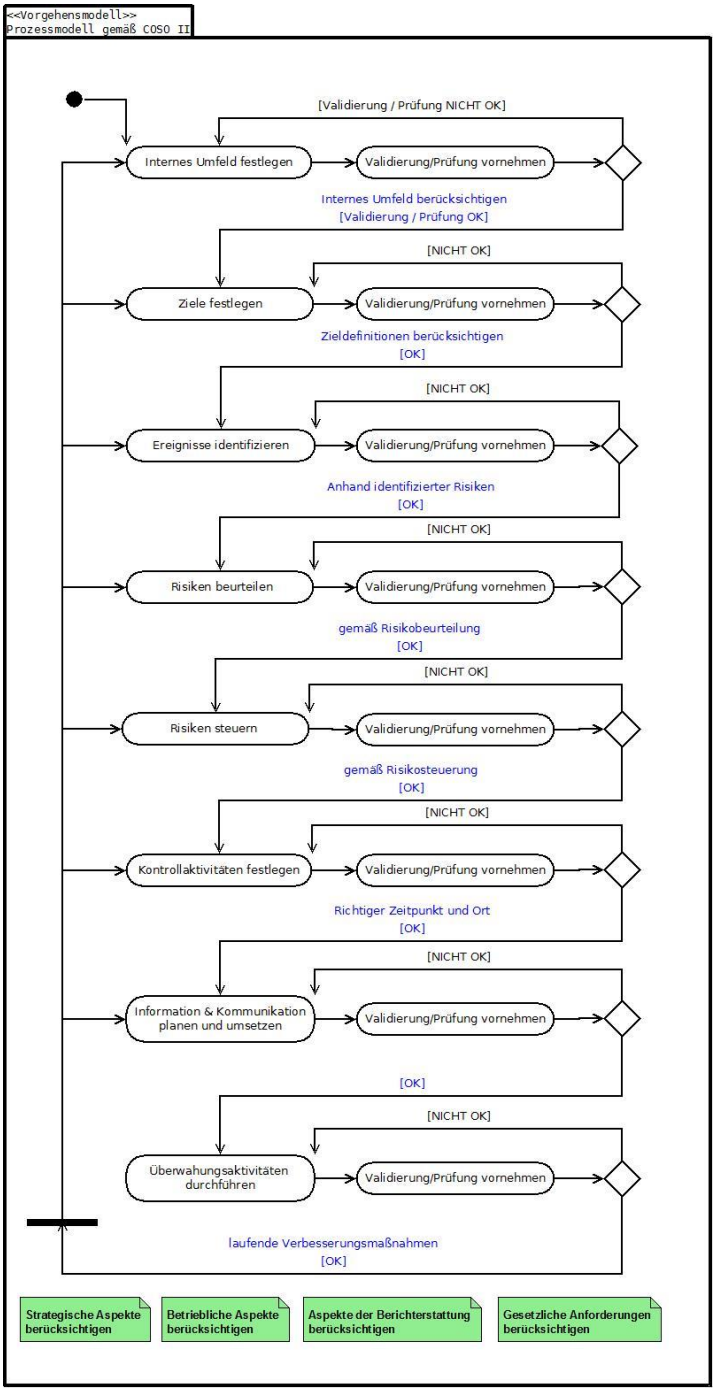

Abbildung 43: Prozessmodell zur Umsetzung der Integration, vereinfachte Form[170]

[170] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

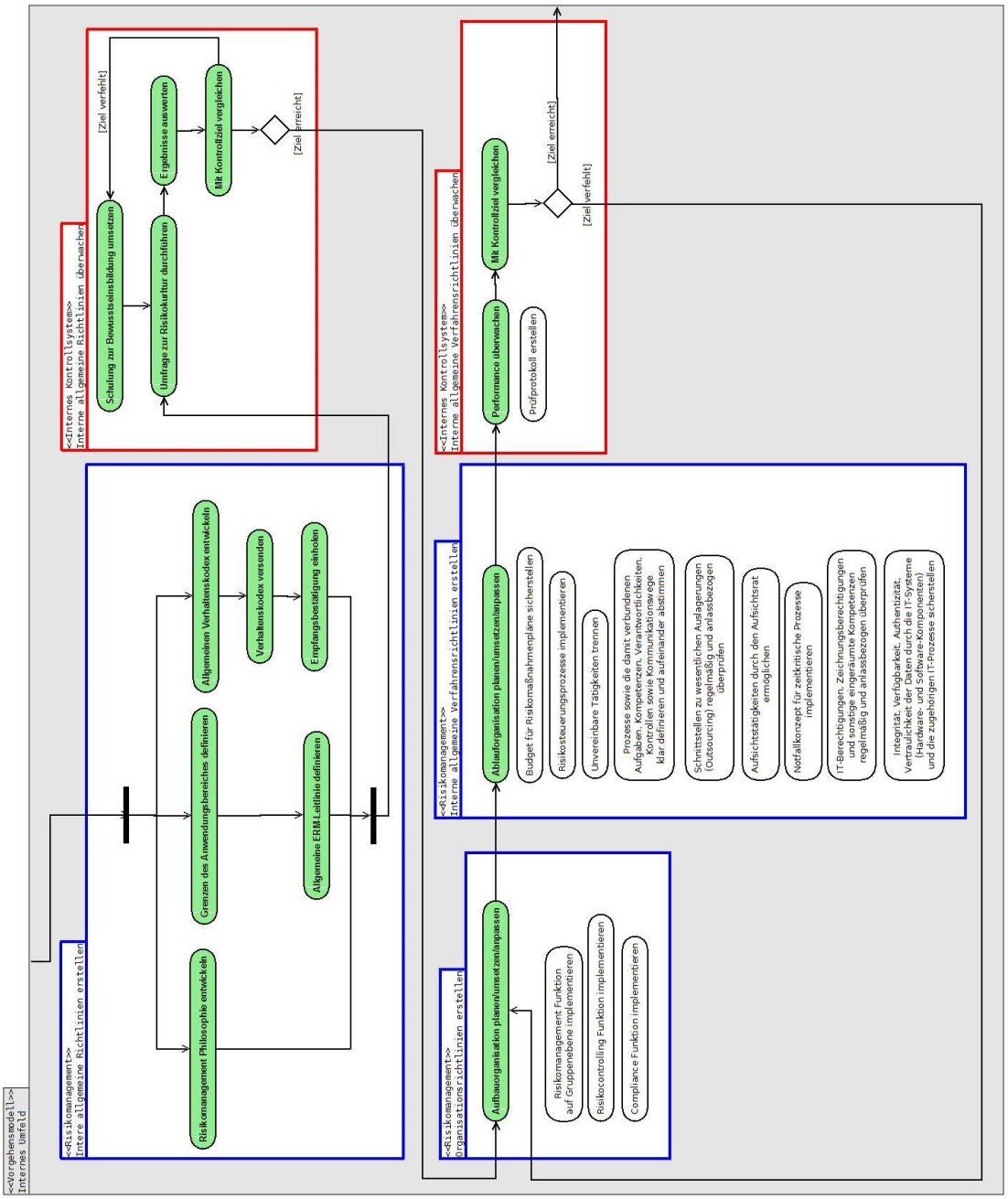

Abbildung 44: Prozessmodell der COSO Komponente *Internes Umfeld*[171]

Im Rahmen der Festlegung des *Internen Umfelds* werden interne allgemeine sowie Organisationsrichtlinien erstellt, kommuniziert und validiert. In der Folge wird durch die Definition und Validierung von Verfahrensrichtlinien die Umsetzung der vorab erstellten Richtlinien beschrieben.

[171] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

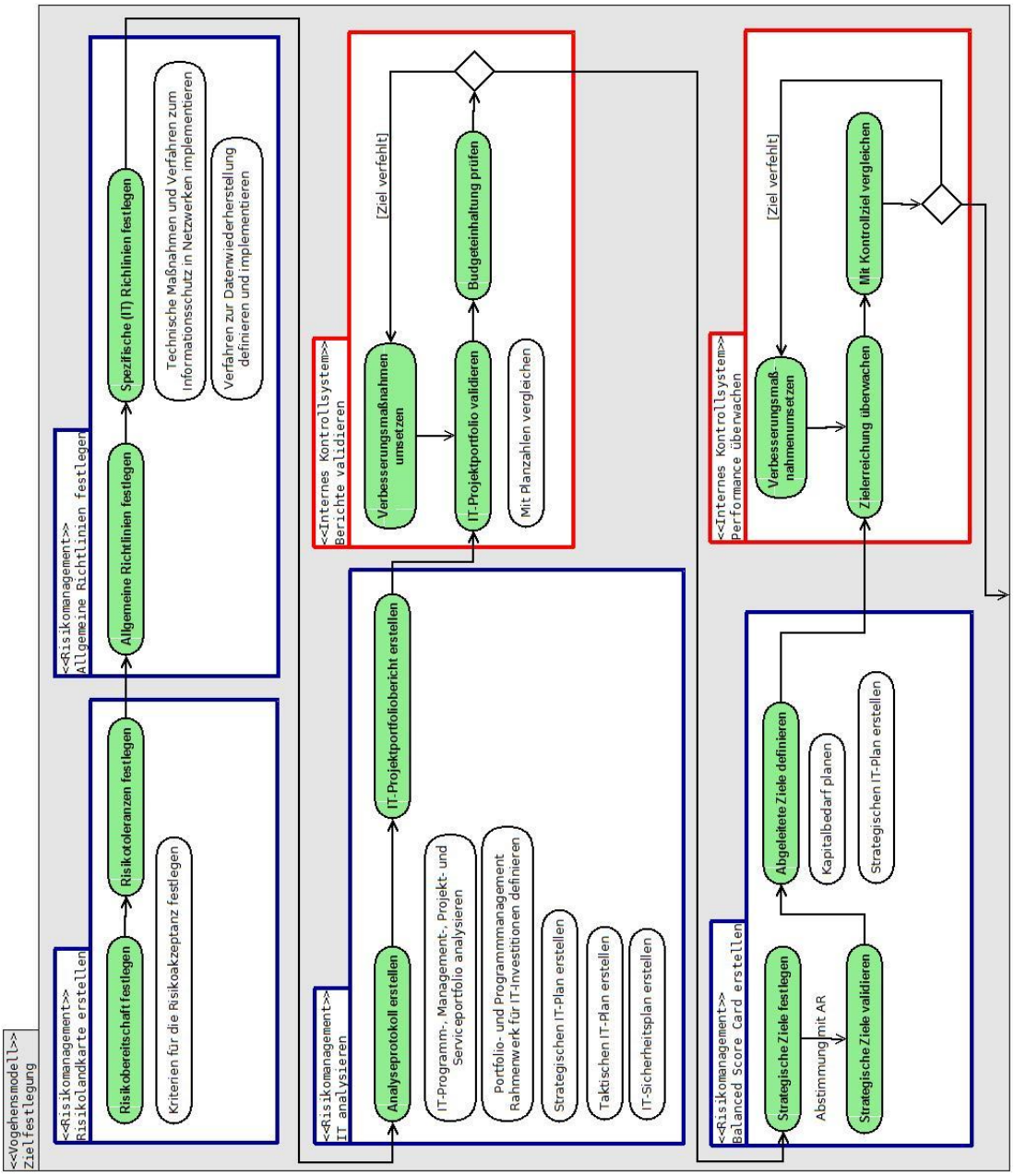

Abbildung 45: Prozessmodell der COSO Komponente *Zielfestlegung*[172]

Im Bereich der Zielfestlegung werden im ersten Schritt Risikolandkarten erstellt, mit welchen die Gebiete der akzeptierten Risiken dargestellt werden. Nach der Definition von allgemeinen und IT spezifischen Richtlinien werden Analyseprotokolle und ein daraus resultierendes IT-Projektportfolio erstellt, welches validiert und mit dem Budget abgeglichen wird. Diese Vorarbeiten sind die Basis für die Festlegung von strategischen Zielen.

[172] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

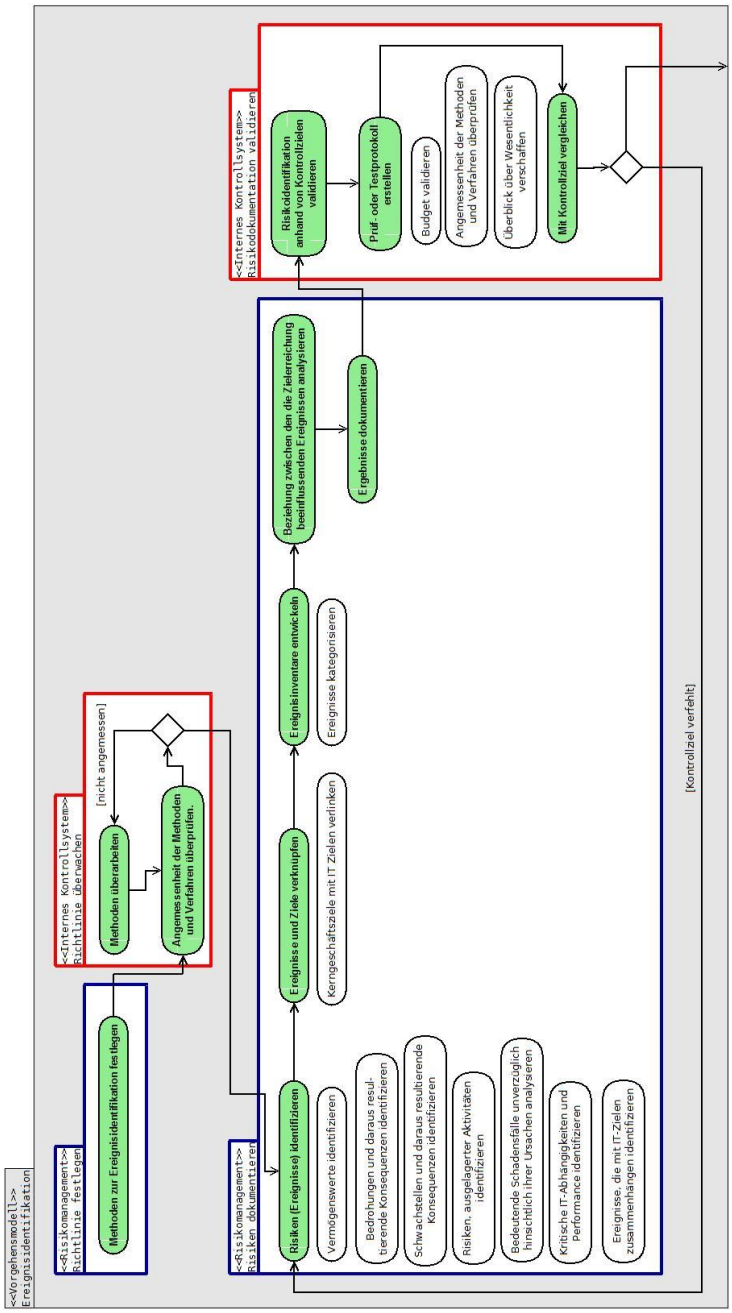

Abbildung 46: Prozessmodell der COSO Komponenten *Ereignisidentifikation*[173]

Im Rahmen dieses Paketes werden zuerst die Methoden für die Identifikation von Risiken festgelegt und auf Angemessenheit überprüft. Danach wird die eigentliche Identifikation der Risiken vorgenommen, mit den Zielen verknüpft und sogenannte Ereignisinventare entwickelt. Nach der Analyse von den die Zielerreichung beeinflussenden Ereignissen werden die Ergebnisse dieser Phase dokumentiert und durch die Erstellung von Prüf- und Testprotokollen überwacht.

[173] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

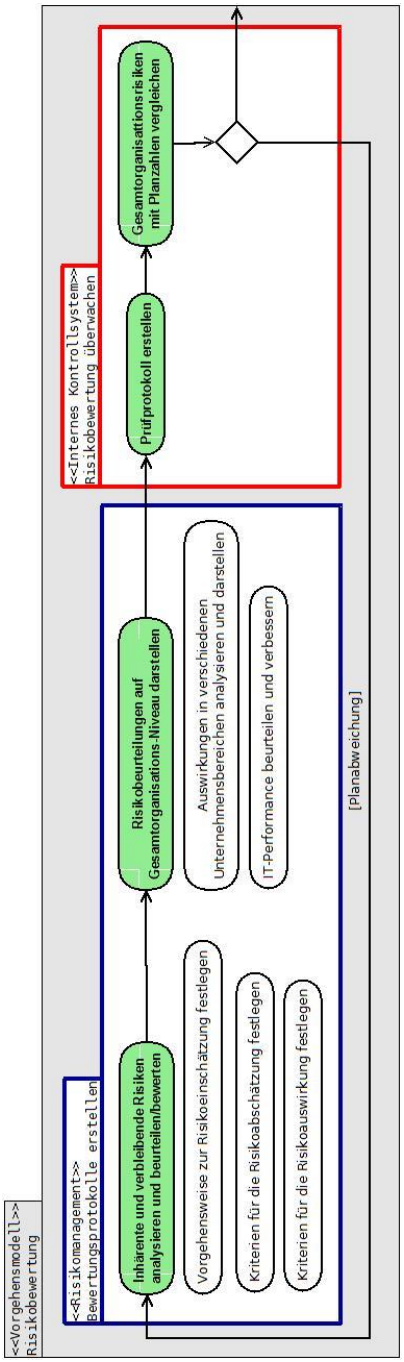

Abbildung 47: Prozessmodell der COSO Komponente Risikobewertung[174]

Die in der vorangegangenen Phase identifizierten Risiken werden im Rahmen dieser Komponente vorerst analysiert und bewertet. Im Anschluss werden die Risikobeurteilungen auf Gesamtorganisationsniveau dargestellt, mit Prüfprotokollen validiert bzw. überwacht sowie mit den Unternehmensplanzahlen verglichen.

[174] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

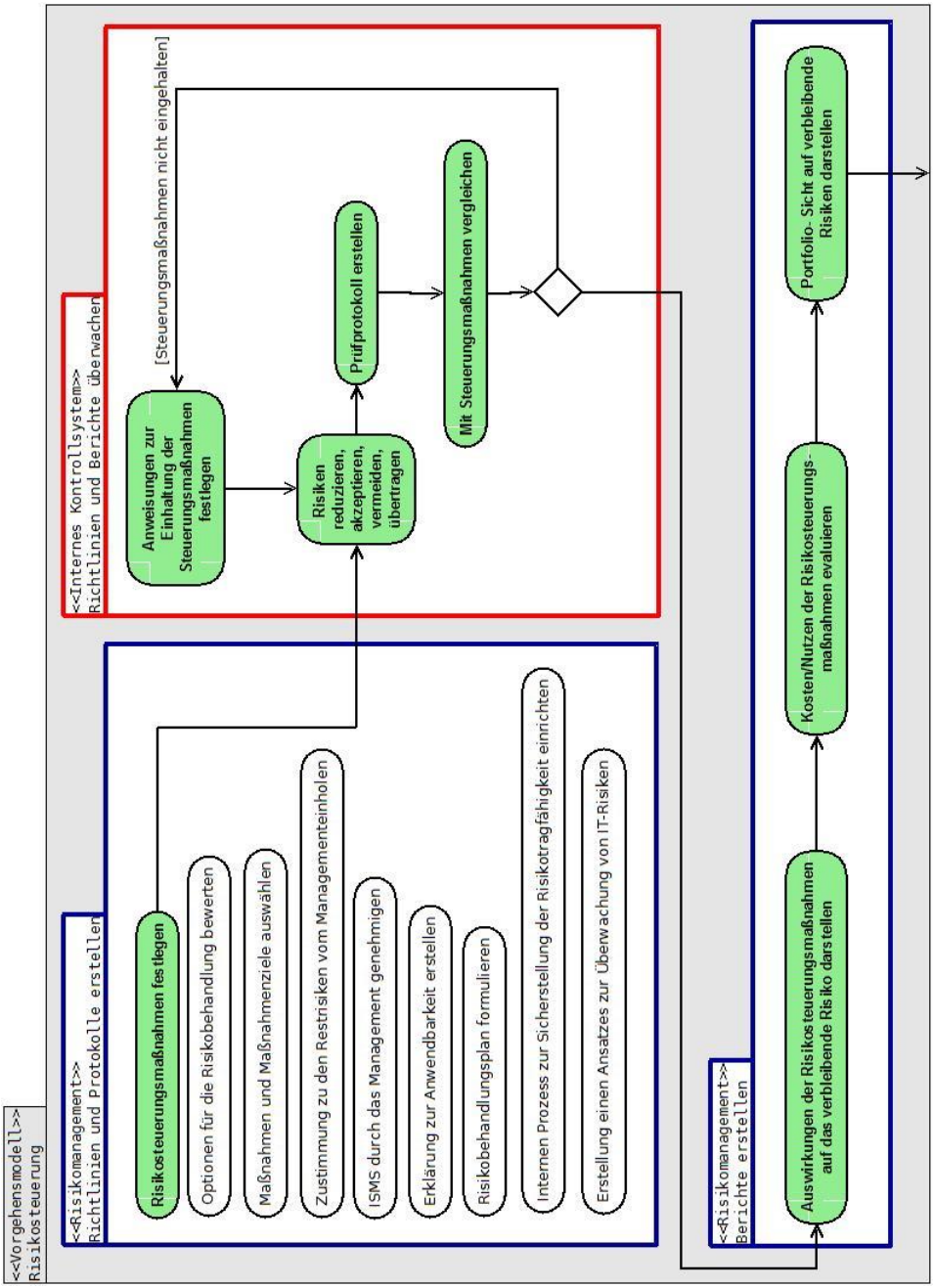

Abbildung 48: Prozessmodell der COSO Komponente *Risikosteuerung*[175]

Die Risikosteuerungsmaßnahmen werden zuerst durch die Erstellung von Richtlinien und Protokollen festgelegt und danach umgesetzt und auf Einhaltung überwacht. In der Folge werden Berichte erstellt, welche die Auswirkung der Maßnahmen auf das verbleibende Risiko, die Kosten/Nutzensicht der Steuerungsmaßnahmen sowie ein Risikoportfolio der verbleibenden Risiken umfassen.

[175] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

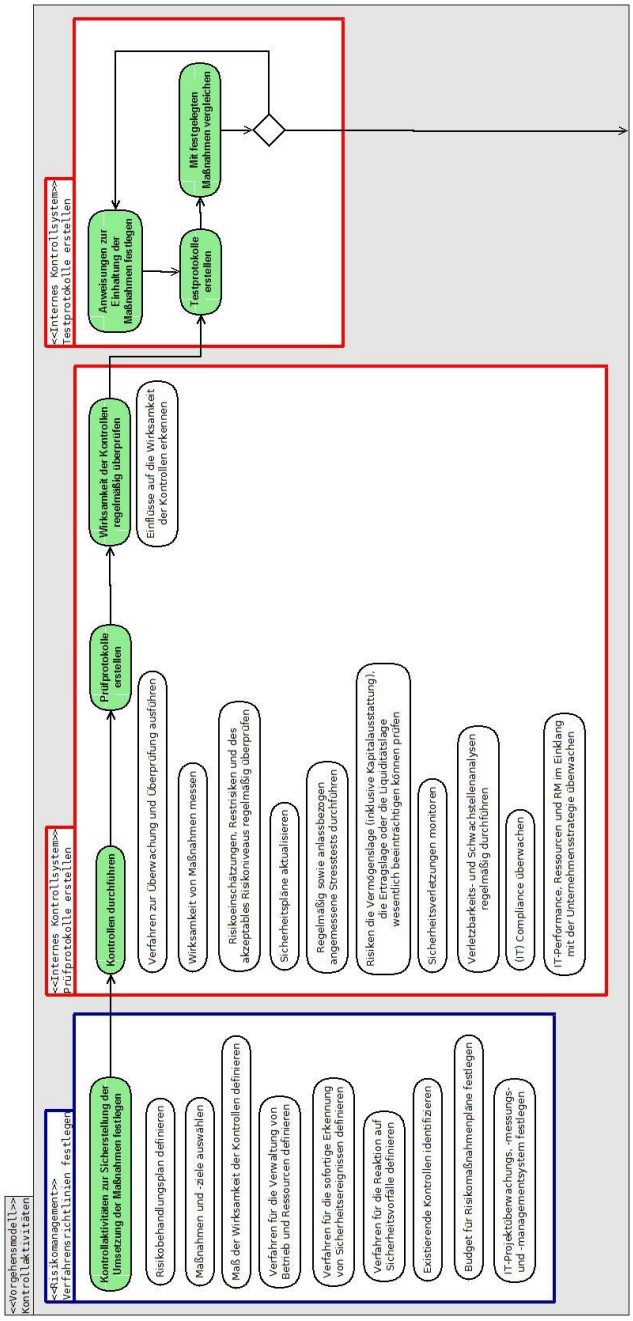

Abbildung 49: Prozessmodell der COSO Komponente *Kontrollaktivitäten*[176]

Diese Phase des Integrationsmodells umfasst die laufenden Kontrollaktivitäten, die zuerst methodisch festgelegt und anschließend durchgeführt werden. Die Dokumentation der Ergebnisse erfolgt in Prüfprotokollen, welche die Basis für die Überwachung der Wirksamkeit der Kontrollen darstellen. Mit anschließend folgenden Testprotokollen wird überprüft, ob die vorab definierten Kontrollmaßnahmen eingehalten wurden.

[176] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

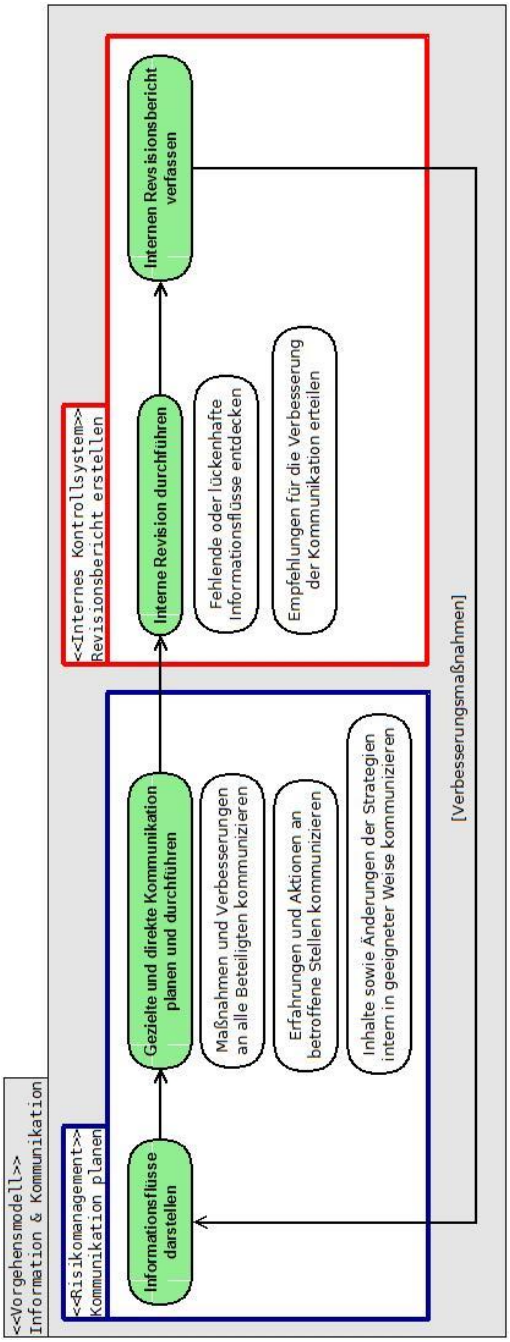

Abbildung 50: Prozessmodell der COSO Komponente *Information & Kommunikation*[177]

Der Risikomanagement Teil dieser Komponente bezieht sich auf die Planung der Informationsflüsse und deren Durchführung. Die Interne Revision prüft im Rahmen ihrer Überwachungstätigkeiten ob die Informationen an richtiger Stelle zum richtigen Zeitpunkt vorhanden sind.

[177] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

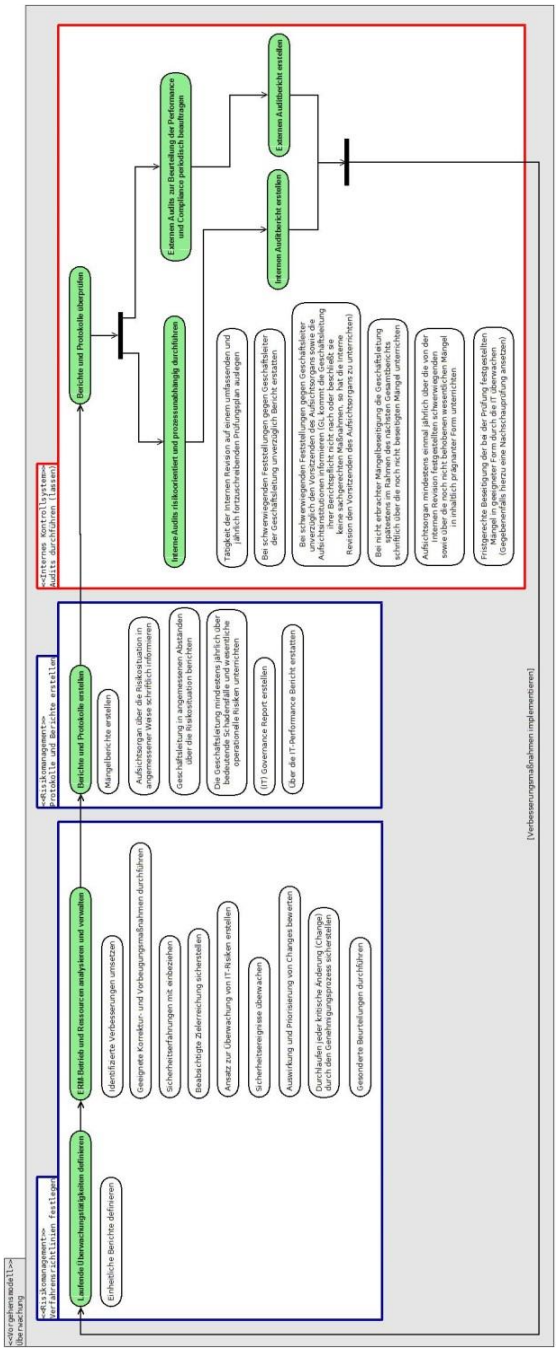

Abbildung 51: Prozessmodell der COSO Komponente *Überwachung*[178]

In der abschließenden Phase *Überwachung* werden zunächst die laufenden Überwachungstätigkeiten zur Verwaltung und Analyse des ERM Betriebes und Ressourcen festgelegt. Im Anschluss werden damit einhergehende Berichte und Protokolle erstellt, welche durch interne und externe Audits validiert und geprüft werden.

[178] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

Abbildung 52: Prozessmodell – *Gesamtansicht* mit allen Komponenten[179]

[179] Quelle: eigene Darstellung in Anlehnung an [21], [4], [16]

In der Gesamtsicht des Prozessmodells wird der gesamte Ablauf zur Umsetzung des Integrationsmodells mit allen Verbindungen zwischen den einzelnen Komponenten dargestellt. Die Startphase weist darauf hin, dass das unternehmensweite Risikomanagement neu eingeführt oder überarbeitet wird. Im Falle einer Überarbeitung sind demnach auch alle dargestellten Phasen zu durchlaufen. In der letzten Phase Überwachung schließt sich der Kreis hin zur Startphase, indem die Ergebnisse der internen und externen Audits zur Überarbeitung oder Verbesserung des unternehmensweiten Risikomanagements herangezogen werden.

6 Evaluierung

Das Ziel bei der in Abschnitt fünf dargestellten Modellbildung ist die vereinfachte Darstellung einer komplexen Struktur (siehe Abschnitt 1.3), welche sich bei der Betrachtung der umfangreichen Vorgaben zur Umsetzung der Integration von Risikomanagement- und Internem Kontrollsystem ergibt. Die Ergebnisse der in diesem Abschnitt dargestellten Evaluierung zeigen, inwieweit dieses Ziel erreicht werden konnte.

Zur Erlangung der Evaluierungsergebnisse wurde folgende Vorgangsweise gewählt:

- Ausarbeitung eines Fragenkatalogs, welcher die Struktur und Inhalte der erstellen Modelle enthält.
- Auswahl von, nach den Einschätzungen des Autors, geeigneten Personen zur Durchführung der Evaluierung.
- Darlegung der Herangehensweise zur Modellbildung vor den Interviews.
- Durchführung von Interviews anhand des Fragenkatalogs.
- Auswertung, Analyse und Interpretation der Ergebnisse.

Mit der Befragung wird festgestellt, welche in den Modellen enthaltenen ERM-Rollen, Prozesse, Systeme und Artefakte in den Unternehmen oder Organisationen vorhandenen sind. In den folgenden Abschnitten wird die erwähnte Vorgangsweise durch die Darstellung des Fragenkatalogs und die Auswertung sowie Interpretation der gesammelten Antworten präzisiert.

6.1 Fragenkatalog zur Evaluierung der erstellten Modelle

Der Fragenkatalog umfasst insgesamt 112 Fragen, durch welche festgestellt wird, ob die jeweilige Organisation die wesentlichen Elemente des statischen Integrationsmodells implementiert hat. Die befragten Personen bewerten jede Frage mit einer Wertigkeit zwischen 0 und 2 wie folgt:

- Wertigkeit 0: in der eigenen Organisation nicht vorhanden; eine Implementierung ist nicht vorgesehen, da der Nutzen nicht erkannt wird.
- Wertigkeit 1: in der eigenen Organisation nicht vorhanden; eine Implementierung ist jedoch in absehbarer Zeit vorgesehen.
- Wertigkeit 2: in der eigenen Organisation vorhanden und fester Bestandteil des ERM.

Durch diese Sichtweise kann bewertet werden, inwieweit die Modellelemente in der Praxis Berücksichtigung finden. Tabelle 25 zeigt als Beispiel einen Ausschnitt des Fragenkatalogs, welcher die Rollen und Funktionen des Integrationsmodells enthält.

Modell Ebene	Risikomanagement	IKS	#	Frage	Bewertung	Summen
Organisation				**Welche der folgenden Rollen/Funktionen sind in Ihrer Organisation vorhanden?**		
			1	Aufsichtsrat		
			2	Chief Executive Officer		
			3	Chief Financial Officer		
			4	Chief Risk Officer		
			5	Führungskräfte im Finanz- und Rechnungswesen		
			6	Geschäftsprozess Owner		
			7	Chief Infomation Officer		
			8	Interne Revision		
			9	Compliance Beauftragte		
			10	Sicherheitsbeauftragte		
			11	Prüfungsausschuss		
			12	Risiko Controlling		
			13	Risiko Owner		
			14	Kontrollprozess Verantwortliche		
			15	Kontrollprozess Durchführende		
			16	Leitung IT-Entwicklung (COBIT)		
			17	Leitung IT-Administration (COBIT)		
			18	Leitung IT-Architektur (COBIT)		
			19	Leitung IT-Betrieb (COBIT)		
			20	Projektbüro (COBIT)		
			21	Problem Management (COBIT)		
			22	IT-Service Strategie (IITIL)		
			23	IT-Service Design (ITIL)		
			24	IT-Service Transition (ITIL)		
			25	IT-Service Operation (ITIL)		
			26	IT Kontinuierliche Serviceverbesserung (ITIL)		
			27	Sonstige, nicht erwähnte, ERM-Rollen/Funktionen (Wertung: 0=vorhanden, 2=nicht vorhanden)	0	
					Summe Organisation	**0**

Tabelle 25: Ausschnitt des Fragenkatalogs zur Evaluierung der Modellebne *Organisation*[180]

Der Rest des Fragenkatalogs umfasst weitere Fragen zu den in den Organisationen implementierten ERM Prozessen, den vorhandenen und für das unternehmensweite Risikomanagement genutzten Systeme sowie die im Zuge der Aktivitäten erzeugten Artefakte.

[180] Quelle: eigene Darstellung

6.2 Auswertung der Ergebnisse

Es wurden insgesamt fünf Interviews mit folgenden Unternehmen oder Organisationen durchgeführt (die Gesprächspartner/Innen wurden aus Gründen der Vertraulichkeit nicht genannt):

Inter-view	Unternehmen	Position - Gesprächspartner/In	Datum des Interviews
1	Multinationaler Industriekonzern	Head of Risk & Opportunity Management, ICS	2013-05-03
2	Österreichische Bundesbehörde	Projektleitung zentrales Risikomanagement	2013-05-08
3	Internationale Unternehmensberatung	Associate Partner	2013-05-08
4	Multinationaler Industriekonzern	Head of Information Security & Standards Chief Information Security Officer (CISO)	2013-05-10
5	Österreichisches Bundesunternehmen	Corporate Compliance & Risk Management	2013-05-16

Tabelle 26: Darstellung der Unternehmen/Personen für die Interviews

Die in Tabelle 26 angeführten Personen verfügen jeweils über langjährige Erfahrungen im Bereich Risikomanagement sowie Interne Kontrollsysteme und bewerten das Modell aus der Sicht von börsennotierten Aktiengesellschaften, Behörden sowie der Unternehmensberatung.

Die Dauer der Interviews betrug jeweils eine Stunde. Alle Interviews mit jeweils 112 Fragen konnten im geplanten Zeitlimit durchgeführt werden. Dies lässt darauf schließen, dass die Elemente des Integrationsmodells in der Praxis bekannt sind und durch die befragten Personen, ohne zusätzlichen Erklärungsbedarf rasch identifiziert werden konnten. Die Ergebnisse der Befragung werden in der Folge dargestellt.

Tabelle 27 veranschaulicht die aggregierten Werte der Befragung, aufgeteilt nach den einzelnen Unternehmen und den Modellebenen *Organisation*, *Prozesse*, *Systeme* und *Artefakte*. Die Darstellung umfasst die Summe an Punkten je Modellebene sowie jeweils den *Grad der Übereinstimmung*, welcher sich durch die Verhältniszahl zur maximal erzielbaren Punktezahl ergibt. Der Grad der Zielerreichung beträgt zwischen 62,5 und 91,1 Prozent. Auffallend ist, dass drei Unternehmen mit einer Zielerreichung von 62,5 bis 72,3 Prozent eine relativ hohe Abweichung aufweisen, während die beiden anderen Organisationen mit 87,5 bzw. 91,1 Prozent eine sehr hohe Deckung zum Integrationsmodell zeigen.

Modell Ebene		Unternehmen / Organisation				
		Interview 1 am 3.5.2013	**Interview 2 am 8.5.2013**	**Interview 3 am 8.5.2013**	**Interview 4 am 10.5.2013**	**Interview 5 am 16.5.2013**
Organisation	Punkte (max. 54)	36	39	29	50	46
	Grad der Übereinstimmung	66,7%	72,2%	53,7%	92,6%	85,2%
Prozesse	Punkte (max. 80)	60	55	53	74	68
	Grad der Übereinstimmung	75,0%	68,8%	66,3%	92,5%	85,0%
Systeme	Punkte (max. 24)	18	16	13	19	22
	Grad der Übereinstimmung	75,0%	66,7%	54,2%	79,2%	91,7%
Artefakte	Punkte (max. 66)	48	50	45	61	60
	Grad der Übereinstimmung	72,7%	75,8%	68,2%	92,4%	90,9%
Summe	**Punkte (max. 224)**	**162**	**160**	**140**	**204**	**196**
	Grad der Übereinstimmung	**72,3%**	**71,4%**	**62,5%**	**91,1%**	**87,5%**
Rang (Übereinstimmung, gesamt)		**3**	**4**	**5**	**1**	**2**

Tabelle 27: Ergebnisse der Befragungen zur Modellevaluierung[181]

[181] Quelle: eigene Darstellung

6.3 Analyse und Interpretation der Ergebnisse

Nach der Durchführung und Dokumentation der Interviews werden in der Folge die Ergebnisse interpretiert. Bei der Fragenauswahl wurde darauf Wert gelegt, dass die Auswertungen der Befragungen miteinander verglichen werden können. Aus diesem Grund wurde auf offene Fragen gänzlich verzichtet.

Tabelle 28 zeigt das Gesamtergebnis aller fünf Interviews nach Modellebenen im Sinne des Grades der Übereinstimmung mit dem Integrationsmodell.

Modell Ebene		**Interview 1 bis 5**	**Rang**	**max. Punkte**	**Anzahl Fragen**
Organisation	Punkte	200	**3**	270	135
	Grad der Übereinstimmung	**74,1%**			
Prozesse	Punkte	310	**2**	400	200
	Grad der Übereinstimmung	**77,5%**			
Systeme	Punkte	88	**4**	120	60
	Grad der Übereinstimmung	**73,3%**			
Artefakte	Punkte	264	**1**	330	165
	Grad der Übereinstimmung	**80,0%**			
Summe	**Punkte**	**862**		**1120**	**560**
	Grad der Übereinstimmung	**77,0%**			

Tabelle 28: Gesamtergebnis der fünf Interviews nach Modellebenen nach Grad der Übereinstimmung[182]

Die Anzahl an Fragen ergibt sich durch das Produkt von 112 Fragen mal fünf Interviews. Die maximale Punktezahl wird erreicht, wenn jede Frage mit zwei Punkten bewertet wird.

Der gesamte Grad der Übereinstimmung beträgt 77 Prozent, wobei die Modellebene *Artefakte* den höchsten Wert aufweist. Die relativ große Abweichung bei der Ebene *Systeme* ergibt sich durch die geringe Anzahl an Fragen und den hohen Detaillierungsgrad des Integrationsmodells, welcher bei den befragten Unternehmen in dieser Ausprägung zum Teil nicht gegeben ist. Zudem zeigte sich im Zuge der Befragungen, dass spezialisierte Systeme für Risikomanagement und IKS nur bedingt eingesetzt werden und durchwegs auf die Kontrolle von Empfangsbestätigungen des Personals für den Erhalt von wichtigen internen Informationen des Managements, wie zum Beispiel den allgemeinen Verhaltenskodex, verzichtet wird.

Die erzielten Punkte je Modellebene und in Summe liegen jeweils deutlich über dem Mittelwert, welcher sich durch eine Bewertung von einem Punkt je Frage ergibt. Diese Sichtweise lässt auf eine allgemeingültige Darstellung des Integrationsmodells schließen. Die jeweils relativ geringen Grade der

[182] Quelle: eigene Darstellung

Übereinstimmungen in jeder Modellebene zeigen, dass die befragten Unternehmen den Detaillierungsgrad des Integrationsmodells in der Praxis nicht umsetzen können oder wollen.

Tabelle 29 veranschaulicht eine weitere Sichtweise auf das Gesamtergebnis, welche durch die Anzahl der jeweiligen Wertungen von null bis zwei dargestellt wird.

Modell Ebene		**Anzahl Wertungen**				**Rang**
		0	**1**	**2**	**1 plus 2**	
Organisation	Punkte	20	30	85	115	**2**
	Prozentueller Anteil	**14,8%**	**22,2%**	**63,0%**	**85,2%**	
Prozesse	Punkte	29	32	139	171	**1**
	Prozentueller Anteil	**14,5%**	**16,0%**	**69,5%**	**85,5%**	
Systeme	Punkte	13	6	41	47	**4**
	Prozentueller Anteil	**21,7%**	**10,0%**	**68,3%**	**78,3%**	
Artefakte	Punkte	25	16	124	140	**3**
	Prozentueller Anteil	**15,2%**	**9,7%**	**75,2%**	**84,8%**	
Summe	**Punkte**	**87**	**84**	**389**	**473**	
	Prozentueller Anteil	**15,5%**	**15,0%**	**69,5%**	**84,5%**	
Rang (gemäß Verhältiniszahl, gesamt)		**2**	**3**	**1**		

Tabelle 29: Gesamtergebnis der fünf Interviews nach Modellebenen nach Anzahl der Wertungen[183]

Für die Erstellung der Tabelle wurden alle Bewertungen von null bis zwei separat gezählt und in Verhältnis zur gesamten Anzahl an Fragen gebracht. Fragen, die mit eins oder zwei bewertet wurden zeigen auf, dass die jeweiligen Modellelemente einen Mehrwert für die befragen Personen darstellen (siehe Bewertungsmethode in Abschnitt 6.1). Demnach werden diese für die Berechnung des Übereinstimmungsgrades herangezogen.

Der prozentuelle Anteil von 84,5 Prozent ergibt eine sehr hohe Deckung mit dem Integrationsmodell. Diese Sichtweise zeigt, dass für die befragten Unternehmen die Elemente des Integrationsmodells zum größten Teil einen Mehrwert aufweisen. Die durchgängige Umsetzung wird allerdings durchwegs als problematisch angesehen, da der damit verbundene Aufwand generell als zu hoch bewertet wird.

Die Durchführung der Interviews ist als Falsifikationsversuch gemäß dem kritischen Rationalismus zu sehen (siehe Abschnitt 1.3). Der Versuch der Widerlegung erfolgte durch die langjährige Erfahrung und das theoretische Wissen der befragten Personen. Durch die teilweise sehr hohe Deckung der Ergebnisse mit dem Integrationsmodell ist der Falsifikationsversuch misslungen. Demnach hat sich die Theorie des entwickelten Modells vorerst bewährt (siehe Abschnitt 2.1).

[183] Quelle: eigene Darstellung

7 Zusammenfassung, Fazit und Ausblick

Im letzten Abschnitt wird in Form einer Zusammenfassung auf die wichtigsten Erkenntnisse der vorliegenden Arbeit eingegangen. Zudem werden, neben einem Fazit, Anregungen von Themen, die in dieser Arbeit zwar erwähnt aber nicht weiter behandelt wurden und zu weiteren Forschungsfragen führen können, in Form eines Ausblicks beschrieben.

7.1 Zusammenfassung

In der vorliegenden Arbeit wurde anhand von geltenden Axiomen ein umfassendes und allgemeingültiges Integrationsmodell für die Zusammenführung von Risikomanagement- und Internem Kontrollsystem entwickelt. Überdies wurde die Erstellung eines Vorgehensmodells zur Umsetzung der Integration vorgenommen. Der für Organisationen erzielbare Mehrwert bei der Anwendung des Modells sowie dessen Handhabbarkeit wurde durch Interviews mit erfahrenen Wissensträgern, welche im Abschnitt sechs dargestellt sind, evaluiert.

Nach der Einleitung und Beschreibung der Vorgangsweise sowie Methodik wurden in den Abschnitten drei und vier die für das Risikomanagement und IKS relevanten strukturellen Aspekte in Form von gesetzlichen Vorgaben, Rahmenwerken, Normen und Richtlinien beschrieben, welche die Basisinformationen für die Modellbildung darstellten.

Bei der Umsetzung der Modellbildung, welche in Abschnitt fünf dargestellt ist, wurden die, nach den Einschätzungen des Autors, folgenden relevanten Gesichtspunkte berücksichtigt:

- Darstellung der Organisationshierarchie in Unternehmen mit Berücksichtigung der Rollen und Verantwortlichkeiten.
- Analyse und Modellierung der für das Risikomanagement und IKS identifizierten Prozesse.
- Berücksichtigung und Integration von Systemen, welche Prozesse ausführen.
- Betrachtung der Artefakte, welche das Ergebnis der durch die Systeme ausgeführten Prozesse darstellen.

Zur Entwicklung des Modells wurden die Syntax bzw. Methoden der Unified Modeling Language (UML) angewandt. Die theoretische Basis des Integrationsmodells bildete die Methode des semantischen Objektmodells (siehe Abschnitt 2.3).

7.2 Fazit

Für die Implementierung und Aufrechterhaltung eines *Risikomanagement-* und *Internen Kontrollsystems* in Unternehmen oder Organisationen existiert eine große Anzahl an Vorgaben in Form von Gesetzgebungen, Empfehlungen, Rahmenwerken, Normen oder Richtlinien. Im Zuge der Analyse dieser Vorgaben wurde jedoch deutlich, dass detaillierte Handlungsanweisungen für die konkrete Umsetzung und Integration oder Harmonisierung der beiden Bereiche kaum vorhanden sind.

Die in der vorliegenden Arbeit entwickelten Modelle zeigen, dass eine Integration möglich ist und durch ein allgemein gültiges Vorgehensmodell zur Umsetzung der Integration konkrete Handlungsanweisungen dargestellt werden können. Die Modellerstellung erfolgte durch Induktion.

Im Zuge der Evaluierung der Modelle, welche durch Interviews erfolgte, stellte sich heraus, dass der generelle Kontext der dargestellten Vorgangsweisen schlüssig ist. Gleichzeitig zeigten sich jedoch auf einigen Detailebenen inhaltliche Auffassungsunterschiede in Form von, nach den Ansichten der Interviewpartner/Innen, fehlenden oder unnötigen Elementen.

Die Widerlegbarkeit der erstellten Modelle weist darauf hin, dass eine gänzlich lückenlose Steuerung von Risiken nicht möglich ist. Dennoch bieten die erstellten Modelle einen Mehrwert indem Risiken und Kontrollen in einer logischen Form miteinander verbunden werden und so eine bewusst risikoorientierte Steuerung von Unternehmen ermöglicht wird.

7.3 Ausblick

Die Durchführung der Modellbildung im Rahmen der vorliegenden Arbeit erfolgte nach eingehender Literatur Recherche und Auswahl von relevanten Gesetzes- und Rahmenwerken sowie Normen und Richtlinien. Diese Auswahl erhebt keinen Anspruch auf Vollständigkeit und kann im Sinne von weiterführenden Forschungstätigkeiten zum Beispiel um folgende Faktoren erweitert werden:

- Die vorliegende Arbeit verweist unter anderem auf Basel II als eine der Primärquellen zur Gestaltung des Risikomanagements und IKS. Zum Zeitpunkt der Erstellung der vorliegenden Arbeit befindet sich Basel III [9] in der Einführungsphase und wurde daher für die Modellbildung nicht berücksichtigt.[184] Es wäre interessant, zu untersuchen inwieweit Basel III neue Erkenntnisse für das ERM mit sich bringt.
- Ein weiterer wichtiger Aspekt das Zusammenwirken von Qualitäts- und Risikomanagement, welches in dieser Arbeit nicht hinlänglich behandelt wurde. Hier kämen dann auch weitere Normen, wie zum Beispiel die ISO-9001 [78] zur Anwendung.

[184] Siehe dazu die Ausführungen in [9, S. 12] , Kapitel C – „Übergangsbestimmungen“

- Bei der Entwicklung des Integrationsmodells wurde mehrfach auf wesentliche Geschäftsprozesse verwiesen, welche jedoch nicht näher analysiert wurden. Eine weitere Arbeit könnte sich damit beschäftigen, wie Wesentlichkeiten festgestellt und kategorisiert werden bzw. das Modell in dieser Hinsicht weiterentwickeln.
- Das Regelwerk 49000 des österreichischen Normungsinstituts (ONR 49000) [80], welches im Jahr 2004 veröffentlicht wurde und einen Management Systemansatz vorstellt [5, S. 56], wurde bei der Modellbildung in der vorliegenden Arbeit nicht berücksichtigt. Für eine Evaluierung des Modells wäre es jedoch auch interessant, diesen Ansatz darzustellen.
- Der ISO-Standard 3100 *Guidelines on Principles and Implementation of Risk Management* [15] wurde zwar erwähnt und dargestellt jedoch nicht bei der Modellbildung berücksichtigt. Der Grund dafür ist, dass durch die *breite Ausgestaltung* der Norm [5, S. 62] keine weiteren Ausschlüsse für das Integrationsmodell gefunden werden konnten.
- Die Inhalte und Konzepte der ITIL V3 wurden im Rahmen dieser Arbeit dargestellt. Bei den Analysen zur Modellbildung wurden die in ITIL definierten Rollen betrachtet (siehe Abschnitt 5.1.2) während die, in diesem Regel- und Definitionswerk enthaltenen Prozesse, nicht berücksichtigt wurden. Nach den Einschätzungen des Autors ist durch die Einbeziehung der umfangreichen und sehr detaillierten Sichtweise der ITIL die Übersichtlichkeit und Verständlichkeit des Integrationsmodells nicht mehr gewährleistet.
- Die in COBIT 5 dargestellten und in Abschnitt 4.2.2 beschriebenen Ansätze für das ERM wurden in der vorliegenden Arbeit nicht berücksichtigt, da der Detaillierungsgrad für das Mapping mit, dem Integrationsmodell zugrunde liegenden, COSO Rahmenwerk noch nicht gegeben ist. Es wäre jedoch interessant, die Inhalte von COBIT 5 nochmals zu analysieren, um festzustellen inwieweit die, für die IT geltenden Grundsätze, für ein ERM der gesamten Organisation angewandt werden können.

Die in diesem Schlusskapitel genannten Inhalte stellen erweiterte und über den Rahmen dieser Arbeit hinausgehende Sichtweisen dar, welche in künftigen, ähnlichen Arbeiten berücksichtigt werden können.

Literaturverzeichnis

[1] F. Wagner, Gabler Versicherungslexikon, Wiesbaden: Springer, 2011.

[2] S. Hunziker, Y. Dietiker, H. Grab und L. Gwerder, IKS-Leitfaden: Internes Kontrollsystem für Gemeinden, Bern: Haupt, 2012.

[3] O. Bungratz, Handbuch Interne Kontrollsysteme (IKS), Steuerung und Überwachung von Unternehmen, 3., neu bearbeitete Auflage, Berlin: Erich Schmidt Verlag, 2012.

[4] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework - Executive Summary, Framework,* Jersey, NJ, USA, 2004.

[5] R. Denk, Corporate Risk Management: Unternehmensweites Risikomanagement als Führungsaufgabe, Wien: Linde Verlag, 2008.

[6] T. Wolke, Risikomanagement, München: Oldenbourg Wissenschaftsverlag, 2008.

[7] A. Klein, Risikomanagement und Risiko-Controlling, Freiburg: Haufe-Lexware, 2011.

[8] B. Hentsche und T. Böhm, IKS-Starthilfe: Leitfaden internes Kontrollsystem zur Personal- und Abrechnungspraxis, Frechen: Datakontext-Fachverlag, 2006.

[9] Basler Ausschuss für Bankenaufsicht, *Basel III: Internationale Rahmenvereinbarung über Messung, Standards und Überwachung in Bezug auf das Liquiditätsrisiko,* Basel: Bank für Internationalen Zahlungsausgleich, 2010.

[10] Republik Österreich, GmbH-Gesetz in der Fassung vom 31.10.2012 (RGBl. Nr. 58/1906), Wien, 2012.

[11] Republik Österreich Aktiengesetz, Fassung vom 31.10.2012 (BGBl. Nr. 98/1965), Wien, 2012.

[12] International Organization for Standardization (ISO)/International Electrotechnical (IEC), ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements, Genf, 2005.

[13] International Organization for Standardization (ISO)/International Electrotechnical (IEC), *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management,* 2005, Genf.

[14] International Organization for Standardization (ISO)/International Electrotechnical (IEC), *ISO/IEC 27005:2008 - Information technology - Security techniques - Infomation security risk management,* Genf, 2008.

[15] International Organization for Standardization (ISO)/International Electrotechnical (IEC), *ISO/IEC 31000:2009 - Risk management - Principles and guidelines,* Genf, 2009.

[16] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control - Integrated Framework - Application Techniques,* Jersey, NJ, USA, 2004.

[17] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,* Rolling Meadows, IL, USA, 2012.

[18] IT Governance Institute (ITGI), *COBIT 4.1 - Framework, Control Objectives, Management Guidelines, Maturity Models,* Rolling Meadows, IL, USA, 2007.

[19] H. Stachowiak, Allgemeine Modelltheorie, Wien, New York: Springer, 1973.

[20] K. R. Popper, Logik der Forschung - zur Erkenntnistheorie der modernen Naturwissenschaft, Wien: Springer Verlag, 1935.

[21] Institut für Interne Revision Österreich, *COSO Enterprise Risk Management - Integrated Framework, Deutsche Fassung,* Wien, 2009.

[22] K. R. Popper, Alles Leben ist Problemlösen : über Erkenntnis, Geschichte und Politik, München, Zürich: Piper, 1996.

[23] D. Hume, A Treatise of Human Nature: Being an Attempt to introduce the experimental Method of Reasoning into Moral Subjects, 1739-40.

[24] *Congress of the United States of America, Sarbanes-Oxley Act,* Washington, D.C, USA, 2002.

[25] *Republik Österreich Unternehmensrechts-Änderungsgesetz 2008, 70. Bundesgesetz,* Wien, 2008.

[26] O. K. Ferstl und E. J. Sinz, „Der Ansatz des Semantischen Objektmodells (SOM) zur Modellierung von Geschäftsprozessen," *WIRTSCHAFTSINFORMATIK 37,* pp. 209 - 220, 1995.

[27] W. Lück, Zentrale Tätigkeitsbereiche der Internen Revision: Aktuelle und zukünftige Schwerpunkte erfolgreicher Revisionsarbeit, Berlin: Erich Schmidt Verlag, 2006.

[28] H. E. Büschgen und C. J. Börner, Bankbetriebslehre, Stuttgart: Lucius & Lucius, 2003.

[29] Österreichische Nationalbank, Günther Thonabauer, Barbara Nösslinger,, „Leitfaden "Management des operationellen Risikos"," Österreichische Nationalbank (OeNB), Österreichische Finanzmarktaufsicht (FMA), Wien, 2005.

[30] C. Stummer, M. Günther und A. M. Köck, Grundzüge des Innovations- und Technologiemanagements, Wien: Facultas, 2008.

[31] The Committee of Sponsoring Organization of the Treadway Commission (COSO), *Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk - Zusammenfassung,* Jersey, NJ, USA, 2004.

[32] P. Albrecht, „Auf dem Weg zu einem holistischen Risikomanagement ?," Mannheimer Manuskripte zu Risikotheorie, Portfolio Management und Versicherungswirtschaft, Mannheim, 1998.

[33] Institut der Wirtschaftsprüfer in Deutschland e.V., *IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261),* 2012.

[34] A. Benz und N. Dose, Governance - Regieren in komplexen Regelsystemen: Eine Einführung, Wiesbaden: Springer, 2010.

[35] W. Lück, Anforderungen an die Interne Revision: Grundsätze, Methoden, Perspektiven, Berlin: Deutsches Institut für Interne Revision, Erich Schmidt Verlag, 2009.

[36] C.-C. Freidank und V. H. Peemöller, Corporate Governance und Interne Revision: Handbuch für die Neuausrichtung des Internal Auditings, Hamburg/Nürnberg: Erich Schmidt Verlag, 2007.

[37] Österreichischer Arbeitskreis für Corporate Governance, „Österreichischer Corporate Governance Kodex, Fassung Jänner 2012," Büro des Beauftragten für Kapitalmarktentwicklung und Corporate Governance, Wien, 2012.

[38] Gartner Research John P. Roberts, „The Elusive Business Value of IT, ID Number: AV-17-2862," Gartner, Inc., Stamford, 2002.

[39] IT Governance Institute (ITGI), „IT Governance für Geschäftsführer und Vorstände, zweite Ausgabe," Rolling Meadows, 2003.

[40] „IT Governance Institute (ITGI)," [Online]. Available: http://www.itgi.org/. [Zugriff am 5 2 2013].

[41] International Organization for Standardization, *ISO/IEC 38500:2008 Corporate governance of information,* Genf, 2008.

[42] H. Schlegel, Steuerung der IT im Klinikmanagement: Methoden und Verfahren, Wiesbaden: Vieweg und Teubner, Springer, 2010.

[43] Institut der Wirtschaftsprüfer in Deutschland e.V., *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980),* 2011.

[44] Bundesministerium der Justiz, Bundesrepublik Deutschland, *Deutscher Corporate Governance Kodex,* Berlin, 2010.

[45] FMA Österreichische Finanzmarktaufsicht, *Grundsätze ordnungsmäßiger Compliance,* Wien, 2007.

[46] G. Wecker, Compliance in Der Unternehmerpraxis: Grundlagen, Organisation Und Umsetzung, Wiesbaden: Gabler, 2009.

[47] P. Windolf, „Korruption, Betrug und 'Corporate Governance' in USA - Anmerkungen zu Enron, Aufsatz," *Leviathan Volume 31, Number 2,* pp. 185-218, 2002.

[48] K. E. Zekany, L. W. Braun und Z. T. Warder, „Behind Closed Doors at WorldCom," *Accounting Education,* S. 101, February 2001.

[49] A. Melis, „Corporate Governance Failures: to what extent is Parmalat a particularly Italian Case?," Blackwell Publishing Ltd, USA, 2005.

[50] Basler Ausschuss für Bankenaufsicht, *Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen,* Basel, 2006.

[51] Basel Committee on Banking Supervision, *The New Basel Capital Accord,* Basel, 2001.

[52] Basler Ausschuss für Bankenaufsicht, *Management operationeller Risiken – Praxisempfehlungen für Banken und Bankenaufsicht,* Basel: Bank für internationalen Zahlungsausgleich, 2003.

[53] Bundesrepublik Deutschland, *Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das zuletzt durch Artikel 3a des Gesetzes vom 20. Dezember 2012 (BGBl. I S. 2777) geändert worden ist,* Berlin, 2011.

[54] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), *Rundschreiben 10/2012 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk,* Bonn/Frankfurt am Main , 2012.

[55] R. Hannemann und A. Schneider, Mindestanforderungen an das Risikomanagement (MaRisk), 3. Auflage, Stuttgart: Schäffer-Poeschel Verlag, 2011.

[56] Official Journal of theEuropean Union, *DIRECTIVE 2009/138/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II),* Brüssel, 2009.

[57] „Website of the IFRS Foundation and the IASB," [Online]. Available: http://www.ifrs.org/Pages/default.aspx. [Zugriff am 8 11 2012].

[58] Kommission der europäischen Gemeinschaften, *Vorschlag für eine Richtlinie des europäischen Parlaments und Rates betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit - SOLVABILITÄT II,* Brüssel, 2007.

[59] M. G. Oxley, *The Sarbanes-Oxley Act of 2002—Restoring Investor Confidence,* Current Issues in Auditing, American Accounting Association, Volume One, Pages C1–C2, 2007.

[60] J. K. Pankaj, K. Jang-Chul und R. Zabihollah, *The effect of the Sarbanes-Oxley Act of 2002 on market liquidity, Working paper,* University of Memphis, 2003.

[61] J. C. Coates IV, „AssociationThe Goals and Promise of the Sarbanes-Oxley Act," *The Journal of Economic Perspectives, Vol. 21, No. 1,* pp. 91-116, 2007.

[62] *Bundesrepublik Deutschland, Bundesgesetzblatt Teil I Nr. 24, Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG),* Bonn.

[63] T. A. Martin und T. Bär, Grundzüge des Risikomanagements nach KonTraG, München: Oldenbourg Wissenschafsverlag, 2002.

[64] U. Götze, K. Henselmann und B. (. Mikus, Risikomanagement, Heidelberg: Physika, 2001.

[65] Deutscher Bundestag - Drucksache 13/9712, *Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG),* Bonn, 1998.

[66] Amtsblatt der Europäischen Gemeinschaften, *Vertrag über die Arbeitsweise der europäischen Union (Konsilidiert Fassung),* Brüssel, 2012.

[67] *Amtsblatt der Europäischen Union, RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES,* Brüssel, 2006.

[68] Republik Österreich, *Regierungsvorlage: IRÄG, 734 der Beilagen XX. GP,* Wien, 1997.

[69] American Institute of Certified Public Accountants (AICPA), *Auditing Standards Board, Statements on Auditing Standards (SAS) 70Reports on the processing of transactions by service organizations,* New York, 1992.

[70] PricewaterhouseCoopers Aktiengesellschaft, Wirtschaftsprüfungsgesellschaft, Frankfurt am Main, „SAS 70 Report: Auswirkungen und Trends," [Online]. Available: http://www.pwc.de/de/automobilindustrie/sas-70-report-auswirkungen-und-trends.jhtml. [Zugriff am 26 2 2013].

[71] G. Steck, *Die Regulierung der U.S. Wirtschaftsprüfung nach Enron,* Trier University: REGEM Analysis No.12, 2004.

[72] Bundesrepublik Deutschland, *Solvabilitätsverordnung vom 14. Dezember 2006 (BGBl. I S. 2926), welche durch den Artikel 1 der Verordnung vom 5. Oktober 2010 (BGBl. I S. 1330) geändert wurde (SolvV),* Berlin, 2010.

[73] Office of Government Commerce (OGC), The Official Introduction to the ITIL Service Lifecycle (ITIL V3), London: The Stationery Office (TSO), 2007.

[74] IT Governance Institute (ITGI), *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit,* Rolling Meadows, IL USA, 2008.

[75] Deutsches Institut für Interne Revision e.V., *Interne Überwachung der Finanzberichterstattung - Leitfaden für kleinere Aktiengesellschaften, Band I: Zusammenfassung,* Frankfurt/Main, 2006.

[76] M. Fröhlich und K. Glasner, IT-Governance: Leitfaden Für Eine Praxisgerechte Implementierung, Wiesbaden: Gabler, 2007.

[77] International Organization for Standardization, *ISO/IEC 15504: Information technology - Process assessment (Teile 1 - 10),* Genf, 2003 - 2011.

[78] International Organization for Standardization (ISO), *ISO 9001:2008 Quality management systems - Requirements,* Genf, 2008.

[79] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Standard 100-1, Version 1.5,* Bonn, 2008.

[80] B. Brühwiler, Risikomanagement als Führungsaufgabe: ISO 31000 mit ONR 49000 wirksam umsetzen, 3. Auflage, Haupt, 2011.

[81] A guide to the Project Management Body of Knowledge (PMBOK Guide), Fourth Edition, Pennsylvania: Project Management Institute, Inc., 2008.

[82] „GRC Overview," Microsoft Corporation, [Online]. Available: http://technet.microsoft.com/en-us/library/cc531020.aspx. [Zugriff am 30 1 2013].

[83] Software Engineering Institute (SEI), „CMMI Institute - the home of Capability Maturity Model Integration," [Online]. Available: http://cmmiinstitute.com/. [Zugriff am 4 2 2013].

[84] „Solvency II Kompakt," [Online]. Available: http://www.solvency-ii-kompakt.de/. [Zugriff am 8 11 2012].

[85] R. Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance,* New York: New York University School of Law, 2004.

[86] Republik Österreich, *Regierungsvorlage: URÄG, 467 der Beilagen XXIII. GP - Regierungsvorlage - Materialien,* Wien, 2008.

[87] ISACA, itSMF, ITIL-COBIT-Mapping: Gemeinsamkeiten und Unterschiede von ITIL V3 und COBIT 4.1, Düsseldorf, 2011.

[88] Office of Government Commerce (OGC), *Service Strategy (ITIL V3),* London: The Stationery Office (TSO), 2007.

[89] Office of Government Commerce (OGC), *Service Design (ITIL V3),* London: The Stationery Office (TSO), 2007.

[90] Office of Government Commerce (OGC), *Service Operation (ITIL V3),* London: The Stationery Office (TSO), 2007.

[91] Office of Government Commerce (OGC), *Service Transition (ITIL V3),* London: The Stationery Office (TSO), 2007.

[92] Office of Government Commerce (OGC), *Continual Service Improvement (ITIL V3),* London : The Stationery Office (TSO), 2007.

[93] „Duden online," [Online]. Available: http://www.duden.de/rechtschreibung/Risiko. [Zugriff am 31 1 2013].

[94] „Webseite des Österreichischen Arbeitskreises für Corporate Governance," [Online]. Available: http://www.corporate-governance.at/. [Zugriff am 5 2 2013].

[95] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), „BaFin-Umsetzung Solvency II," [Online]. Available: http://www.bafin.de/DE/Aufsicht/VersichererPensionsfonds/UmsetzungSolvencyII/umsetzungsolvency2_node.html. [Zugriff am 9 4 2013].

[96] ZEIT ONLINE - Wirtschaft, „Bilanz-Skandal: Urteil im Worldcom-Prozess," [Online]. Available: http://www.zeit.de/2005/11/worldcom_urteil. [Zugriff am 18 2 2013].

[97] ISACA, „COBIT Assessment Programme update," 12 8 2011. [Online]. Available: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=160. [Zugriff am 10 4 2013].

[98] Gabler Wirtschaftslexikon, „Stichwort: Balanced Scorecard, online im Internet," [Online]. Available: http://wirtschaftslexikon.gabler.de/Archiv/1856/balanced-scorecard-v7.html. [Zugriff am 15 4 2013].

[99] Gabler Wirtschaftslexikon, „Stichwort: Zahlungsfähigkeit, online im Internet," [Online]. Available: http://wirtschaftslexikon.gabler.de/Archiv/13519/zahlungsfaehigkeit-v5.html. [Zugriff am 12 2 2013].

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A: Abstract

A.1 English

Through upscale market demands in the form of increased competition situations, higher expectations of the shareholders and complex business models, it is becoming increasingly difficult for companies to achieve and safeguard plan goals. Consciously taking risks and avoiding errors in this context are important factors for the achievement of objectives. Therefore, a structured risk management is an indispensable instrument to achieve growth and business objectives. With the extended approach of Enterprise Risk Management (ERM), the integrated corporate control is performed.

The Internal Control System (ICS) as a part of the ERM is recognized to manage risk through controls. Internal controls are reactions to an identified and assessed risk. Effective corporate governance can only be perceived through the integration of ICS and ERM. In the literature and in many companies, risk management and ICS are considered as isolated systems. The effects are separated units in the organizational structure, isolated business processes and artefacts and different systems for the implementation of risk management and ICS.

To achieve the integration of the two systems, a generally applicable model for integration of risk management and ICS is created with the present work. Another essential aspect of the work is the creation of a process model to implement the integration. The methodological basis for the modelling is the Semantic Object Model (SOM). The models themselves are created with the Unified Modelling Language (UML) as a semantic class diagram.

A.2 Deutsch

Durch gehobene Marktansprüche in Form von verstärkten Konkurrenzsituationen, höheren Erwartungen der Shareholder sowie komplexer werdenden Geschäftsmodellen wird es für Unternehmen immer schwieriger, Planziele zu erreichen bzw. abzusichern. Das bewusste Eingehen von Risiken und die Vermeidung von Fehlern sind in diesem Zusammenhang wichtige Faktoren für die Zielerreichung. Ein strukturiertes Risikomanagement ist daher ein unverzichtbares Instrument, um Wachstums- und Geschäftsziele zu erreichen. Mit dem erweiterten Ansatz des Enterprise Risk Managements (ERM) wird die ganzheitliche Unternehmenssteuerung wahrgenommen.

Das Interne Kontrollsystem (IKS) als ein Teil des ERM dient dazu, erkannte Risiken durch Kontrollen zu steuern. Interne Kontrollen sind Reaktionen auf ein identifiziertes und bewertetes Risiko. Nur durch die Integration von ERM und IKS kann eine effektive Unternehmenssteuerung wahrgenommen werden. In der Literatur und in vielen Unternehmen werden das Risikomanagement und IKS jedoch meistens als isolierte Systeme betrachtet. Die Auswirkungen sind getrennte Einheiten in der Aufbauorganisation, isolierte Geschäftsprozesse und Artefakte sowie unterschiedliche Systeme zur Umsetzung von Risikomanagement und IKS.

Zur Erreichung der Integration der beiden Systeme wird mit der vorliegenden Arbeit ein allgemeingültiges Integrationsmodell für Risikomanagement und IKS erstellt. Ein weiterer wesentlicher Aspekt der Ausarbeitung ist die Erstellung eines Vorgehensmodells zur Umsetzung der Integration. Die methodische Basis für die Modellierung und Gestaltung der Geschäftsprozesse sowie Anwendungssysteme bildet das Semantische Objektmodell (SOM). Die Modelle selbst werden mit der Unified Modeling Language (UML) als semantisches Klassendiagramm erstellt.

Anhang B: Lebenslauf

Kurt Berthold, BSc

Grundäckergasse 31
A-1100 Wien
Email: kurt.berthold@aon.at
Geboren am 15.März 1959 in Wien

AUSBILDUNG

Oktober 2007 – November 2011	**Bachelorstudium** Wirtschaftsinformatik Universität Wien, Universitätsring 1, A-1010 Wien
Oktober 2011 – Juni 2013	**Masterstudium** Wirtschaftsinformatik Universität Wien, Universitätsring 1, A-1010 Wien

BERUFSERFAHRUNG

2006 Dato	**Selbständiger Unternehmensberater** IKS / Risikomanagement bzw. Interim Geschäftsführung **DIRECTURE GmbH** - Consulting / Personalberatung, Direktvertrieb (kurzfristiges Anstellungsverhältnis)
2000 2006	**Xerox Austria GmbH** Direktor Xerox Services, Mitglied der Geschäftsleitung, Channels Manager
1997 1999	**Actebis Computerhandelsges.m.b.H** Geschäftsführer
1994 1997	**Sharp Electronics Ges.m.b.H.** Sales/Marketingmanager, Mitglied der Geschäftsleitung, Prokurist
1992 1994	**Lotus Development GmbH** Corporate Account Manager
1991 1992	**W. Stolz Ges.m.b.H.** Key Account Manager
1982 1991	**Philips Data Systems Ges.m.b.H.** Account Manager Banken/Behörden
1974 1982	**Kapsch AG** Sachbearbeiter Abteilung Auftragsverrechnung