MASTERARBEIT

Titel der Masterarbeit

Harmonisierung des Risikomanagements für Einsatz und Outsourcing von Informationstechnologie

Theorie und abgeleitetes Integrationsmodell zur Abbildung in ein unternehmensweit einheitliches und effektives Risikomanagement-System für den Einsatz und die Auslagerung von Diensten der Informationstechnologie

Verfasser

Christian Sieberer, BSc

angestrebter akademischer Grad

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2012

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienbuchblatt:	Masterstudium Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. Dr. techn. 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, den 23. Jänner 2012

Unterschrift:

_____

Christian SIEBERER

Danksagung

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

Inhalt

Kapitel 1 : Einführung 1
1.1 Kontext, Motivation und Forschungsfrage 1
1.2 Begriffsdefinitionen 5
1.3 Die Modellbildung und ihr wissenschaftstheoretischer Hintergrund 14
1.4 Related Work 15
Kapitel 2 : Entwicklung eines Vorgehensmodells 19
2.1 Das Vorgehensmodell im Überblick 19
Kapitel 3 : Recherche und Objektorientierte Analyse 21
3.1 Vorgehen 21
3.2 Vorstellung der relevanten Ansätze 27
3.3 Grobstrukturierung 66
Kapitel 4 : Objektorientiertes Design 69
4.1 Vorgehen 69
4.2 Das harmonisierte Integrationsmodell 78
Kapitel 5 : Evaluierung und kritische Betrachtung 105
5.1 Wissenschaftstheoretischer Kontext 105
5.2 Erfüllung spezifischer Anforderungen und Mehrwert der Arbeit 107
Kapitel 6 : Zusammenfassung und Schlussfolgerung 111
6.1 Zusammenfassung 111
6.2 Schlussfolgerungen 112
6.3 Weiterführende Fragestellungen 113
Literaturverzeichnis 115
Abbildungsverzeichnis 121
Tabellenverzeichnis 125
Anhang A: Abstract 127
A.1 English 127
A.2 Deutsch 127
Anhang B: Lebenslauf 129

Kapitel 1: Einführung

Dieses Kapitel beschreibt den Kontext, die grundlegende Motivation und die Fragestellung der Arbeit. Nach einer Definition der wesentlichen Begriffe wird zudem eine Einordnung in den wissenschaftstheoretischen Kontext vorgenommen, sowie die vorliegende Arbeit von anderen Werken aus dem gleichen Themenkreis abgegrenzt.

1.1 Kontext, Motivation und Forschungsfrage

1.1.1 Kontext

Der heutige globalisierte Wirtschaftsbetrieb konfrontiert Unternehmen auf vielfältige Weise mit einem breiten Spektrum an Risiken, dem es durch geeignete Maßnahmen Rechnung zu tragen gilt.

- So stehen Organisationen neuartigen Herausforderungen wie sich rascher als zuvor ändernden Rahmenbedingungen gegenüber, die mit zunehmender Häufigkeit auch die Form globaler Krisen annehmen. Derartige Situationen erfordern rasche Reaktionen und geben – wie die internationale Finanz- und Wirtschaftskrise der letzten Jahre – Stimmen für tiefer greifende Regulierungen des Wirtschaftsbetriebs immer breitere öffentliche Akzeptanz. [1]

  Als Beispiele hierfür sind unter anderem die international gültigen Baseler Eigenkapitalvorschriften im Finanzdienstleistungssektor zu nennen (*Basel II* [2]), die detaillierte Vorschriften zum Risikomanagement enthalten, die mit entsprechenden Modifikationen auch für eine branchenübergreifende Anwendung geeignet sind.

- Zusätzlich steigt durch die Entwicklung globaler Märkte mit hoher Konkurrenz der Kostendruck über alle Unternehmensbereiche hinweg und unterstreicht die Forderung nach Optimierung und Transparenz der Kosten und Leistungen von IT-Systemen, was durch einen klar geregelten und überwachten Betrieb von Informationssystemen erreicht werden kann. [3]

  Zu diesem Zweck steht eine Reihe von komplexen Rahmenwerken wie *ITIL* [4] und *COBIT* [5] zur Verfügung, die die durchgehende Steuerung (Governance) der IT unterstützen.

- Betrugs- und Bilanzskandale werfen die Frage nach effektiver *Corporate Governance* auf, wobei aufgrund deren integraler Wichtigkeit im Unternehmensbetrieb zunehmend der Einsatz von Informationssystemen in den Blickpunkt rückt. [6], [7]

  Auch hieraus entstehen Regulierungen wie der aus den USA stammende (und auch für international tätige Unternehmen gültige) *Sarbanes-Oxley Act (SOX*

[8]*)*, der 2002 infolge der aufsehenerregenden Bilanzskandale rund um den Energieversorger *Enron* und das Telekommunikationsunternehmen *WorldCom* verabschiedet wurde und unter anderem Anforderungen an die Kontrolle der Finanzberichterstattung stellt [7]. Rahmenwerke wie *COSO ERM* [9] bieten umfangreiche Hilfestellung bei der Planung, Einführung und Verwaltung von internen Kontrollsystemen, die zu diesem Zweck eingesetzt werden.

- Auch die Komplexität und der hohe Vernetzungsgrad der eingesetzten Informationstechnologie an sich bergen neuartige Gefahren und eröffnen mannigfaltige Angriffsmöglichkeiten, die zu umfangreichen Bedrohungen der Informationssicherheit führen können.

  Die große Häufigkeit solcher Vorfälle ist längst nicht mehr nur in IT-Kreisen bekannt, sondern erregt bei besonders spektakulären Fällen oft auch die Aufmerksamkeit der breiten Öffentlichkeit, wie die mediale Berichterstattung im Jahr 2011 zeigt. [10] Für betroffene Institutionen ergeben sich neben den Schäden durch Brüche der Informationssicherheit weitere Nachteile, wie Einbußen durch Vertrauensverluste und Rufschädigung. [11]

  Eine umfassende Absicherung lässt sich unter anderem mit Standards zum Management von Informationssicherheit erreichen, wie sie von der ISO/IEC mit der Reihe 2700x bereitgestellt werden.

- Schließlich unterstreichen unvorhergesehene Ereignisse wie Naturkatastrophen den Bedarf für umfassende Notfallplanungen, zeigen aber auch die Grenzen der Möglichkeiten auf, Risiken zuverlässig abzuschätzen. Gerade in Katastrophensituationen stellt eine zuverlässige Informationsversorgung jedoch eine kritische Leistung von unschätzbarem Wert dar, die es erlaubt, weitere Schäden an Leib, Leben und Ausrüstung zu minimieren. [12]

  Zu diesem Zweck stellen Standards und Rahmenwerke zum Risiko- und Notfallmanagement im IT-Bereich ein verbreitetes Hilfsmittel dar. [13]

1.1.2 Motivation

Angesichts derartiger Herausforderungen entstand seit Beginn der neunziger Jahre eine Vielzahl an Ansätzen zur Steuerung und Kontrolle von Risiken, die auf den sicheren und wirtschaftlichen Einsatz von Informationssystemen ebenso abzielen wie auf den sicheren allgemeinen Unternehmensbetrieb und von öffentlichen wie von privaten Institutionen entwickelt wurden. Unter anderem durch die mannigfachen Hintergründe dieser Ansätze – seien sie bedingt durch die Betrachtung unterschiedlicher Branchen, die Herkunft aus unterschiedlichen Ländern oder die Fokussierung auf unterschiedliche Bereiche des Unternehmens- und IT-Betriebs – weisen diese Ansätze zumeist eine starke Heterogenität auf, und erscheinen trotz vielfacher inhaltlicher Überlappungen aufgrund struktureller wie inhaltlicher Unterschiede kaum zueinander kompatibel.

Kapitel 2 stellt eine Auswahl derartiger Ansätze zur Steuerung und Kontrolle von Risiken vor, zeigt bestehende Divergenzen auf und führt eine erste Klassifikation der Ansätze ein.

Da es sich bei jenen Ansätzen, die als Grundlage für die vorliegende Arbeit betrachtet werden, durchgängig um Rahmenwerke, Standards und Regulierungen handelt, die im praktischen Einsatz eine hohe Verbreitung erfahren haben, ist davon auszugehen, dass diese trotz der vielfältigen Unterschiede im Unternehmens- und IT-Betrieb Wert generieren, der deren Verwendung sinnvoll erscheinen lässt.

Gleichzeitig ist in der Praxis allerdings oft festzustellen, dass viele Institutionen zwar über grundlegende Mechanismen zur Behandlung von Risiken verfügen, die den verschiedenen Rahmenwerken, Standards und Regulierungen entnommen sind. Werden diese Maßnahmen, wie oft zu beobachten ist, jedoch nicht einheitlich verwaltet und gesteuert, so wird eine durchgängige strategische Ausrichtung stark erschwert, woraus aus Sicht des Autors eine Reihe an Gefahren entstehen kann:

- Durch die fehlende integrierte Betrachtung kann der Überblick über die tatsächliche Angemessenheit und Sinnhaftigkeit der getroffenen Maßnahmen und deren Werterbringung verloren gehen.
- Aufgrund der stark dezentralen Steuerung und Verwaltung können ineffiziente Prozesse mit unklaren Verantwortlichkeiten entstehen, die global betrachtet sowohl Effizienz als auch Effektivität des Risikomanagements im gesamten Unternehmen beeinträchtigen und nur schwer an geänderte Rahmenbedingungen angepasst werden können.
- Diese Unklarheiten verstärken sich entlang der Schnittstellen zwischen inter-organisationalen Geschäftsprozessen, etwa bei ausgelagerten Diensten bei Dienstleister und auslagerndem Unternehmen, oder bei eng verbundenen Supply Chains bei Zulieferer und Abnehmer.
- Mitarbeiter empfinden die so entstehende Bürokratie in ihrer Tätigkeit oft als Behinderung, was Motivation und Produktivität beeinträchtigen kann.
- Eventuelle Verbesserungspotenziale in den Geschäftsprozessen des Unternehmens bleiben unentdeckt.
- Die Informationslage über Risiken und zugehörige Trends kann unzureichend sein, da eventuell gesammelte Daten oft nicht ausreichend integriert werden.
- Rechtzeitige Reaktionen auf eintretende Risiken werden daher erschwert.
- In Notfällen ist keine ausreichende zentrale Koordination vorhanden.
- Risikomanagement wird damit insgesamt zum Selbstzweck und leistet keinen messbaren Beitrag zur Erreichung der Unternehmensziele.

1.1.3 Forschungsfrage

Somit ist nicht lediglich die Verwendung von Maßnahmen aus einzelnen Ansätzen zielführend, sondern es besteht die Notwendigkeit einer klar definierten, über das gesamte Unternehmen hinweg einheitlich strukturierten Vorgehensweise, die von der Geschäftsebene getrieben ist und Auslagerungen bzw. interorganisationale Geschäftsprozesse berücksichtigt. Diese hat sämtliche relevanten Rahmenwerke, Standards und Regelungen zu identifizieren, zu integrieren und aufeinander abzustimmen, und somit ein effektives und wirtschaftliches Risikomanagement zu schaffen.

Es ist davon auszugehen, dass eine derartige Harmonisierung der unterschiedlichen Ansätze eine Reihe entscheidender Vorteile bringen kann, die die Werterbringung durch IT-Risikomanagement nach Meinung des Autors deutlich verbessern:

- Über eine durchgängige Erhebung der Assets im Unternehmen lässt sich deren Schutzbedarf feststellen und gezielt Maßnahmen treffen, um diesem Schutzbedarf zu entsprechen.

- Die Prozesse des Risikomanagements können unternehmensweit einheitlich strukturiert werden, was Effizienz und Effektivität erhöht.

- Durch eine Überarbeitung der Geschäftsprozesse können Tätigkeiten besser strukturiert werden, um für die Mitarbeiter angenehmere Arbeitsflüsse zu erzeugen, während gleichzeitig global gesehen Effizienz und Effektivität gesteigert werden können.

- Eine rechtzeitige Reaktion auf eintretende Risiken kann durch deren zentrale Überwachung und der laufenden Aggregation entsprechender Daten im Zusammenspiel mit klar definierten Abläufen und Verantwortlichkeiten sichergestellt werden, bei Auslagerungen oder enger Zusammenarbeit über Supply Chains auch über Organisationsgrenzen hinweg.

- Risikomanagement kann laufend auf die Unternehmensstrategie und sich ändernde Anforderungen angepasst werden und leistet einen aktiven Beitrag zur Erreichung der Unternehmensziele.

Die vorliegende Arbeit geht der Frage nach, inwieweit eine derartige Harmonisierung möglich ist und fokussiert dabei auf den Einsatz und die Auslagerung von Diensten der Informationstechnologie (IT-Risikomanagement). Um die genannten Vorteile zu erreichen, ist aus betriebswirtschaftlicher Sicht dabei wesentliches Augenmerk auf die Integration eines derartigen IT-Risikomanagementsystems mit den bestehenden Ansätzen des betrieblichen Risikomanagements zu legen (Enterprise Risk Management, ERM). Im Sinne der Nachverfolgbarkeit sowie möglicher Zertifizierungen ist zudem zu gewährleisten, dass im Rahmen der Modellbildung die einfließenden Ansätze klar benannt werden und durchgängig identifizierbar bleiben.

Kapitel 4 widmet sich eingehend der Beantwortung der vorliegenden Forschungsfrage und stellt die Ergebnisse der beispielhaften Modellierung eines idealtypischen IT-Risikomanagement-Ansatzes vor.

1.2 Begriffsdefinitionen

Als Grundlage für das weitere Verständnis der Arbeit ist es notwendig, zunächst jene elementaren Begriffe aus dem Themenkreis des Risikomanagements zu erläutern, die überblicksweise in Abbildung 1.1 dargestellt werden. Wo nötig, werden im Rahmen der Modellbildung in Kapitel 4 detailliertere Definitionen vorgenommen.

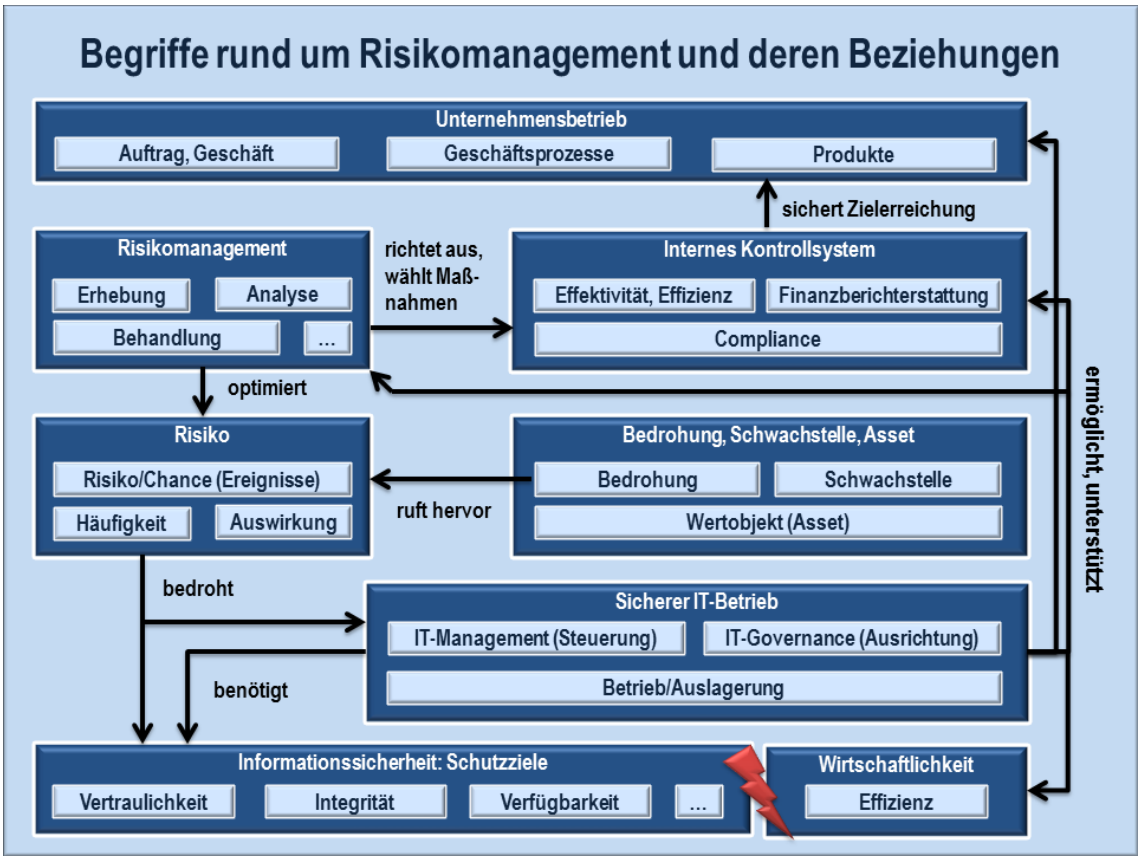

Abbildung 1.1: Begriffe rund um Risikomanagement und deren Beziehungen[1]

1.2.1 Unternehmen, Geschäft und Prozesse

Unternehmen bezeichnet im Rahmen dieser Arbeit generell jegliche Form von Institution, die einen klar definierten Auftrag erfüllt. Dieser Begriff schließt somit sowohl private als auch öffentliche Organisationen mit ein, wie Finanzdienstleister oder Regierungsbehörden, und gilt auch unabhängig von einer möglichen oder nicht vorhandenen Gewinnorientierung.

[1] Quelle: eigene Darstellung

All jene grundlegenden fachlichen Tätigkeiten, die der Erfüllung des Auftrags der jeweiligen Institution dienen, werden unter dem Begriff *Geschäft* zusammengefasst. Dabei kann es sich um die Bereitstellung von Finanzdienstleistungen ebenso handeln wie um die Wahrnehmung von Regierungsaufgaben oder das Leisten von Entwicklungshilfe.

Unter *Geschäftsprozessen* sind wiederum alle strukturierten Abläufe zu verstehen, die eine Institution zur Herstellung eines *Produkts* ausführt. Bei Produkten kann es sich um materielle wie immaterielle Objekte von Wert (eingeschlossen Dienstleistungen) handeln, die die Institution zur Erfüllung ihres Auftrags bereitstellt. In Abhängigkeit davon, wie stark ein Geschäftsprozess an der Wertschöpfungskette im Unternehmen beteiligt ist, wird häufig zwischen *Kern-* und *unterstützenden Prozessen* (*Support-Prozessen*) unterschieden, wobei letztere beispielsweise auch die Prozesse rund um die Erbringung von Diensten der Informationstechnologie (*IT-Prozesse*) beinhalten. Zudem existieren *Management-Prozesse*, welche die Führungs- und Steuerungsaufgaben des Unternehmens bündeln.

1.2.2 Risikomanagement und Informationssicherheit

Der folgende Abschnitt definiert einführend die Begriffsfelder Risikomanagement und Informationssicherheit und führt die beiden Konzepte anschließend zusammen.

Risikomanagement

Trotz vieler unterschiedlicher Begriffsdefinitionen existiert eine Reihe an grundlegenden Eigenschaften rund um die Termini *Risiko* und *Risikomanagement*, die von praktisch allen thematisch relevanten Quellen beschrieben werden. [9], [14], [15], [16], [17]

Dazu ist zunächst das *Risiko* selbst zu zählen, welches ein *Ereignis* darstellt, das mit einer bestimmten *Häufigkeit* oder *Wahrscheinlichkeit* eintritt und dabei *Auswirkungen* hervorruft, die positiv oder negativ sein können, und deren Höhe zumindest grob quantifizierbar ist.[2]

Risiken werden durch *Bedrohungen* hervorgerufen, die die *Assets*[3] einer Organisation angreifen. Dies ist möglich, da Assets – wie technische Anlagen, Prozesse, Informationen oder Mitarbeiter eines Unternehmens – *Schwachstellen* aufweisen, die verschiedenster Natur sein können und von den Bedrohungen ausgenutzt werden.

Tabelle 1.1 führt einige Beispiele für Schwachstellen, Bedrohungen und Risiken an.

[2] Bei positiven Auswirkungen sprechen einige Quellen anstelle von Risiken auch von *Chancen*

[3] Unter Assets sind alle Objekte zu verstehen, die für das Unternehmen Wert besitzen. Die wörtliche deutsche Übersetzung des Begriffs Asset lautet „Anlagevermögen"; da dieser Begriff jedoch nicht den Kern des englischen Ausdrucks trifft, wird auf eine Übersetzung im Rahmen der vorliegenden Arbeit verzichtet.

Risiko	Bedrohung	Schwachstelle
Interner Betrug	Vorsätzlich nicht gemeldete Transaktionen (z.B. Abbuchungen)	Fehlende Überprüfung von Transaktionen auf Konten
Externer Angriff, Betrug	Hackerangriffe, Bedrohung durch Schadsoftware	Fehlende technische Absicherung von IT-Systemen
Beschäftigung, Arbeitsplatzsicherheit	Verstöße gegen Gesundheits- und Sicherheitsbestimmungen	Ungesicherter Einsatz von Produktionsmaschinen
Kunden, Produkte, Geschäft	Marktmanipulationen	Fehlende Prüfung auf Insidergeschäfte
Sachschäden	Naturkatastrophen (z.B. Erdbeben, Stürme, Hochwasser)	Unzureichende Konstruktion von Gebäuden
Unterbrechungen, Ausfälle	Ausfall von IT-Systemen	Mängel bei der redundanten Auslegung von IT-Systemen
Abwicklung, Vertrieb, Prozessmanagement	Unzureichende Erbringung von Dienstleistungen bei Outsourcing	Fehlende Leistungsspezifikation bei Auslagerungen

Tabelle 1.1: Beispiele für Schwachstellen, Bedrohungen und Risiken[4]

Die Gesamtheit an koordinierten Aktivitäten, die dazu dienen, eine Organisation in Bezug auf derartige Risiken zu leiten, zu steuern und zu kontrollieren, wird – unter anderem durch die *internationale Organisation für Normung* (*ISO*) – als *Risikomanagement* bezeichnet. [15, S. 2] Dazu zählen zumindest:

- die Erhebung von Risiken, Bedrohungen, Assets und Schwachstellen
- die Analyse und Bewertung von Risiken
- die Behandlung von Risiken und deren Überwachung

Zur Risikobehandlung stehen verschiedene Möglichkeiten zur Verfügung, wie die *Vermeidung*, die *Übernahme* bzw. *Akzeptanz*, die *Umlagerung* (bspw. über Versicherungen) oder die *aktive Minderung* von Risiken. [18], [15], [9]

Informationssicherheit

Der Begriff der *Informationssicherheit* wird in unterschiedlichen Publikationen übereinstimmend als eine Reihe von Eigenschaften definiert, die Information in bestimmtem Maße einzuhalten hat, um als sicher zu gelten.[5] Dazu sind nach der internationalen Norm ISO/IEC 27002 [19, S. 1] zumindest die *Vertraulichkeit*

[4] Quelle: eigene Darstellung in Anlehnung an die Klassifikation von Verlustereignissen nach Basel II [2, S. 255f.]

[5] Dieses notwendige Maß an Informationssicherheit wird im Rahmen von Praxisprojekten üblicherweise individuell im Kontext einer Schutzbedarfsfeststellung über sogenannte „Schutzbedarfsklassen“ festgelegt, die den schutzbedürftigen Assets zugewiesen werden.

(*Confidentiality*), *Integrität* (*Integrity*) und *Verfügbarkeit* (*Availability*) zu zählen[6]. In englischer Sprache wird die Kombination dieser Eigenschaften oft nach ihren Anfangsbuchstaben als *CIA-Modell* bezeichnet. Je nach Anwendungsfall können zudem weitere mögliche Kriterien für Informationssicherheit gelten, wie *Authentizität* (*Authenticity*), *Verbindlichkeit* (*Accountability*), *Nichtabstreitbarkeit* (*Non-Repudiation*) oder *Verlässlichkeit* (*Reliability*). [19, S. 1]

Die ISO/IEC 27002 definiert diese Eigenschaften jedoch nicht genauer, weshalb die folgenden Definitionen aus dem Glossar des BSI [20] sowie den Begriffsdefinitionen von COBIT [21, S. 14] stammen, die sinngemäß übereinstimmende und teilweise sich wechselseitig ergänzende Definitionen liefern:

- **Vertraulichkeit (Confidentiality)** wird nach BSI durch den Schutz von Informationen vor unbefugter Preisgabe erreicht.

- **Integrität (Integrity)** bezeichnet nach COBIT und BSI die Korrektheit und Vollständigkeit von Informationen in Bezug auf die enthaltenen Daten und Metadaten (bspw. Autor und zugehörige Zeitstempel) sowie deren Gültigkeit in Übereinstimmung mit den Erwartungen und Werten des Unternehmens.

- **Verfügbarkeit (Availability)** ist nach BSI dann gegeben, wenn Informationen den Benutzern stets wie gewünscht zur Verfügung stehen, wofür nach COBIT insbesondere auch die Ressourcen zu schützen sind, die die Information bereitstellen.

- Die **Authentizität (Authenticity)** von Informationen liegt nach BSI dann vor, wenn sichergestellt ist, dass sie tatsächlich von der angegebenen Quelle erstellt wurden, wobei neben Personen auch Anwendungen oder IT-Komponenten als Quellen dienen können.

- **Nichtabstreitbarkeit (Non-repudiation)** ist nach BSI dann gewährleistet, wenn der Versand und/oder der Empfang von Informationen nicht in Abrede gestellt werden kann.

- Über den Begriff der **Verbindlichkeit (Accountability)** werden nach BSI die Eigenschaften der Authentizität und Nichtabstreitbarkeit zusammengefasst.

- **Verlässlichkeit (Reliability)** fordert laut COBIT ein Maß an Angemessenheit für Informationen, die vom Management verwendet werden, um eine Organisation zu leiten.

Ein Punkt von zentraler Wichtigkeit stellt hierbei die Tatsache dar, dass Informationen in sämtlichen Phasen ihrer Verwendung zu schützen sind, also bei jeglicher Verarbeitung, Übertragung oder Speicherung, und zwar unabhängig vom verwendeten Medium. Daraus kann abgeleitet werden, dass Informationssicherheit nicht mit technischer IT-Sicherheit gleichzusetzen ist, sondern letztere lediglich eine notwendige Voraussetzung für erstere darstellt: Information ist in den Köpfen von Mitarbeitern

[6] Übereinstimmende Definitionen finden sich beispielsweise auch im Glossar zur Internet-Sicherheit des BSI [20] sowie im Dokument zur MaRisk [27, S. AT7.2.2]

einer Organisation ebenso vorhanden wie auf Papierdokumenten, Wechseldatenträgern oder Rechnersystemen.

Informationssicherheit erfordert somit die Absicherung technischer Schwachstellen von EDV-Systemen genauso wie organisatorische Maßnahmen, zu denen beispielsweise Mitarbeiterschulungen oder das Aufsetzen von Leitlinien zur Informationssicherheit (sogenannter *Information Security Policies*) gehören. Diesem Umstand tragen die meisten in dieser Arbeit betrachteten Ansätze durch eine umfangreiche Ausrichtung auf organisatorische Aspekte Rechnung, die die technischen und technisch-organisatorischen Maßnahmen ergänzen.[7]

Informationssicherheit und Risikomanagement – Effektivität vs. Effizienz

Ziel des informationssicherheitsbezogenen Risikomanagements ist die *effektive* und *effiziente* Steuerung und Kontrolle von Organisationen in Bezug auf relevante Ereignisse, um mithilfe geeigneter Maßnahmen das optimale Maß an Informationssicherheit zu erreichen.

Effektivität bedeutet in diesem Zusammenhang, dass das eingesetzte Managementsystem die vorgegebenen Ziele erreicht, also hohe Sicherheitsniveaus für sämtliche schutzbedürftigen Assets gewährleistet. Dies steht oft im direkten Widerspruch zur *Effizienz*, die eine möglichst geringe Störung von Arbeitsflüssen und einen möglichst niedrigen finanziellen Aufwand für die getroffenen Maßnahmen fordert.

Damit gehört es zu den zentralen Aufgaben eines IT-Risikomanagementsystems, durch eine ausdifferenzierte Betrachtung der Kosten- und Nutzenfaktoren auf transparente und nachverfolgbare Art und Weise angemessene Maßnahmen zur Risikobehandlung auszuwählen, deren technische Umsetzbarkeit gegeben und deren ökonomische Sinnhaftigkeit im Unternehmen argumentierbar ist (vgl. bspw. [17, S. 29]).

1.2.3 Internes Kontrollsystem (IKS)

Nach dem Glossar von COSO ERM, das oft als Standard-Referenzmodell für den Entwurf von *Internen Kontrollsystemen* (*IKS*) genannt wird, ist unter einem ebensolchen ein Prozess zu verstehen, der die Erreichung von Zielen in Bezug auf effektiven und effizienten Unternehmensbetrieb, die Zuverlässigkeit der Finanzberichterstattung sowie die Compliance mit relevanten Gesetzen und Regelungen sicherstellt. Für die Ausführung dieses Prozesses ist neben dem restlichen Personal insbesondere der Vorstand bzw. Aufsichtsrat[8] und das Management eines Unternehmens verantwortlich. [9, S. 122] Die Prozesse zur Steuerung und Kontrolle von Risiken werden im Rahmen eines derartigen IKS ausgeführt und überwacht.

[7] Siehe dazu auch den bekannten „McCumber Cube“, der diesen Zusammenhang in einem einfachen Modell anschaulich darstellt [74]

[8] Der Begriff „board“ bzw. „board of directors“ bezeichnet im englischsprachigen Raum eine Leitungsebene, die die Aufgaben von Vorstand und Aufsichtsrat eines Unternehmens vereint und wird im Kontext dieser Arbeit daher entsprechend übersetzt

1.2.4 IT Governance, IT Management und Auslagerungen

Im Folgenden findet zunächst eine Abgrenzung und Erklärung der Begriffe *IT Governance* und *IT Management* statt, worauf der Umfang und die Bedeutung der Auslagerung von Diensten der Informationstechnologie erläutert werden.

IT Governance

Der englische Begriff *Governance* lässt sich unter anderem mit dem Wort *Steuerung* treffend ins Deutsche übersetzen. Auf eine genaue Diskussion der verschiedenen Begriffsdefinition, die in der Literatur zum Teil stark divergieren, wird im Kontext der vorliegenden Arbeit verzichtet und stattdessen die Definition des Good-Practice-Frameworks COBIT 4.1, das aufgrund der weiten Verbreitung als de-facto-Standard zur IT Governance gilt, leicht modifiziert übernommen: [5, S. 8]

Demnach besteht *IT Governance* aus Führungsaufgaben, Organisationsstrukturen und Prozessen, die sicherstellen, dass die betriebliche Informationstechnologie die Unternehmensziele unterstützt. IT Governance liegt im Verantwortungsbereich des Vorstands bzw. Aufsichtsrats sowie der Management-Ebene des Unternehmens.

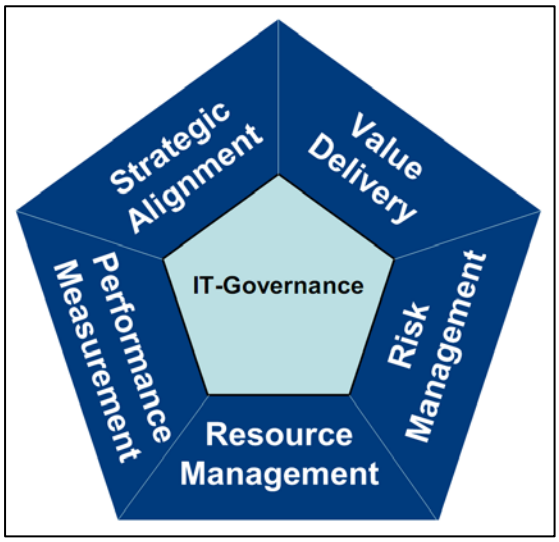

Abbildung 1.2: Kernbereiche der IT Governance[9]

Nach COBIT lässt sich IT Governance in fünf Teilbereiche gliedern (siehe Abbildung 1.2): [5, S. 6]

- Die **Strategische Ausrichtung** stellt die Orientierung der IT-Planung an den Zielen der Geschäftsebene sicher (*IT-Business-Alignment*)
- Die **Werterbringung** sichert die Erfüllung des strategischen Wertbeitrags der IT bei durchgängiger Kostenoptimierung.

[9] Quelle: [21, S. 7]

- Das **Ressourcenmanagement** ist für die Anschaffung und Verwaltung kritischer IT-Ressourcen verantwortlich. Dazu zählen Anwendungen ebenso wie Information, Infrastruktur und Mitarbeiter des Unternehmens.

- Im Rahmen der **Performance-Messung** findet eine umfassende Messung und Überwachung aller Aspekte des IT-Lebenszyklus statt – als Beispiele hierfür sind unter anderem die Umsetzung von Strategien, der Fortschritt von Projekten, die Verwendung von Ressourcen oder der Ablauf von Geschäfts- und IT-Prozessen zu nennen.

- Zudem wird **Risikomanagement** als eigener Teilbereich angeführt, der somit als Schnittstelle zum Thema dieser Arbeit dienen kann: Aus pragmatischen Gründen wird IT Governance im Folgenden als Hilfsmittel eingeordnet, um Maßnahmen zur Steuerung und Kontrolle von Risiken auf effektive und effiziente Art umzusetzen.

IT Management

Der aktuell vorliegende Entwurf zum IT-Governance-Framework *COBIT 5* enthält erstmals eine Definition des Begriffs *IT Management*, der klar von *IT Governance* abgegrenzt wird: [22, S. 34]

IT Management ist demnach die Gesamtheit jener Mittel, bestehend aus Ressourcen, Personen, Prozessen, Verfahren und dergleichen, die einer Organisation zur Verfügung stehen, um den IT-Lebenszyklus zur Erreichung ihrer Ziele planen, organisieren, steuern und kontrollieren zu können.

Damit stellt IT Management die Grundlage dar, um IT Governance in einem Unternehmen gezielt umzusetzen.

Auslagerung von IT-Dienstleistungen

Als Auslagerung (*Outsourcing*) wird die externe Bereitstellung von Diensten durch einen externen Dienstleister bezeichnet. Die grundlegende Motivation für jede Form der Auslagerung stellt die Annahme dar, dass der gebündelte Erfahrungsschatz und die Ressourcenausstattung des Dienstleisters es ermöglichen, über den externen Betrieb von Informationstechnologie und Geschäftsprozessen eine Reihe von Vorteilen zu erzielen. Die Auswertung einer Studie aus dem Jahr 2009, die im Rahmen einer Dissertation aus Wirtschaftsinformatik an der technischen Universität München erstellt wurde, ergab dabei vier primäre Kundengruppen mit unterschiedlichen, zum Teil überlappenden Zielsetzungen: [23, S. IX]

- Auslagernde Unternehmen, die nach Service-Orientierung, Flexibilität und Effizienz im IT-Betrieb streben
- Institutionen, die über Auslagerungen strategische Ziele zu erreichen oder Innovationen umzusetzen versuchen
- Unternehmen auf der Suche nach Mitteln zur Kostensenkung

- Kunden mit der Absicht, durch Auslagerungen die Qualität und Zuverlässigkeit des IT-Betriebs zu steigern

Die hohe Bedeutung von Outsourcing lässt sich unter anderem anhand der Ergebnisse einer vom IT Governance Institute (ITGI) durchgeführten Studie zum Stand der IT Governance ermessen, bei der 95% der weltweit über 800 befragten Unternehmen angaben, ihren IT-Betrieb vollständig oder zum Teil ausgelagert zu haben. [24, S. 35ff.]

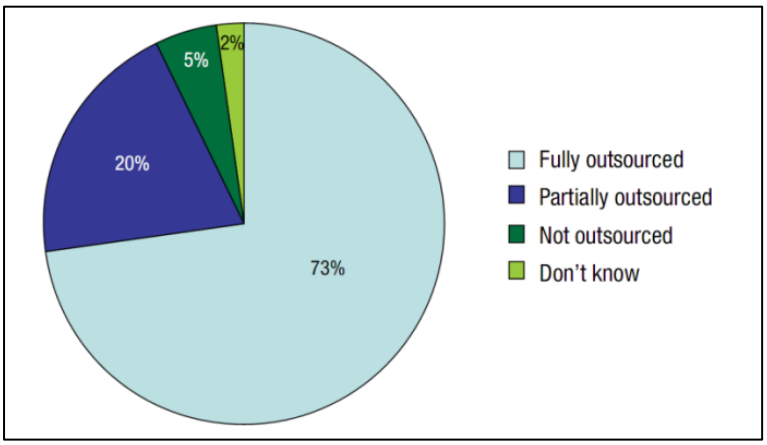

Abbildung 1.3: Verbreitung von IT-Outsourcing nach ITGI[10]

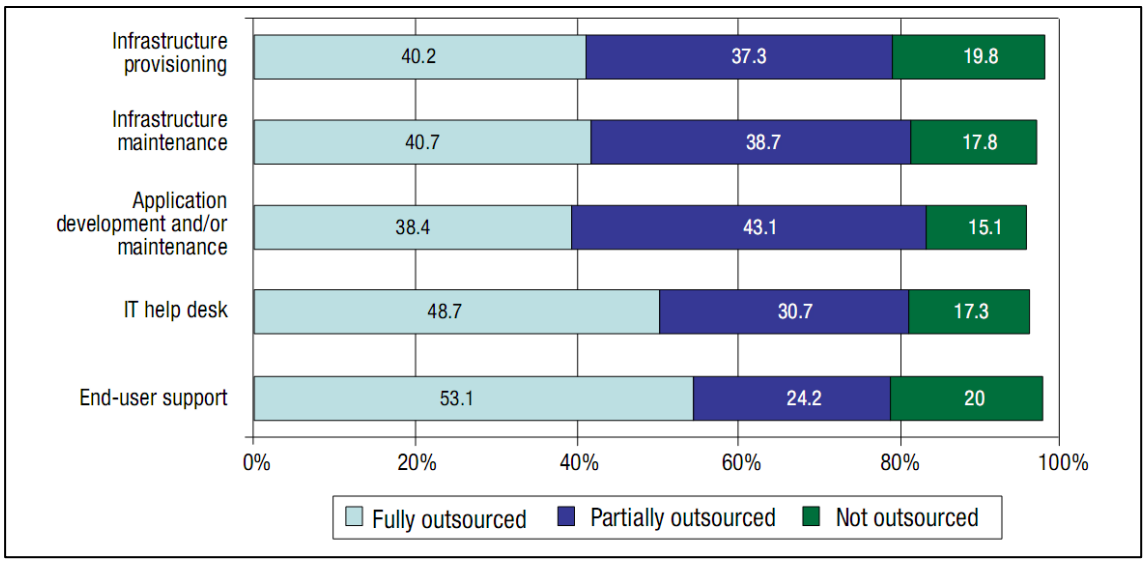

Abbildung 1.4: Ausgelagerte Aktivitäten nach ITGI[11]

Wie aus Abbildung 1.4 erkennbar, werden dabei sowohl die Bereitstellung von Infrastruktur als auch deren Wartung, die Entwicklung von Anwendungen und der Support ausgelagert, wobei insbesondere Letzterer bei rund der Hälfte der Befragten zur Gänze von Dritten betrieben wurde.

[10] Quelle: [24, S. 35]
[11] Quelle: [24, S. 36]

Werden die weltweit aggregierten Volumina von Outsourcing-Verträgen nach Branchen gegliedert, bildet laut dem regelmäßig veröffentlichten *TPI Index* des dritten Quartals 2011 der Finanzdienstleistungssektor das mit Abstand größte Marktsegment (über 30% des Vertragsvolumens), gefolgt von Produktionsbetrieben (rund 20%) und der Energiebranche (10%). [25, S. 8] [12]

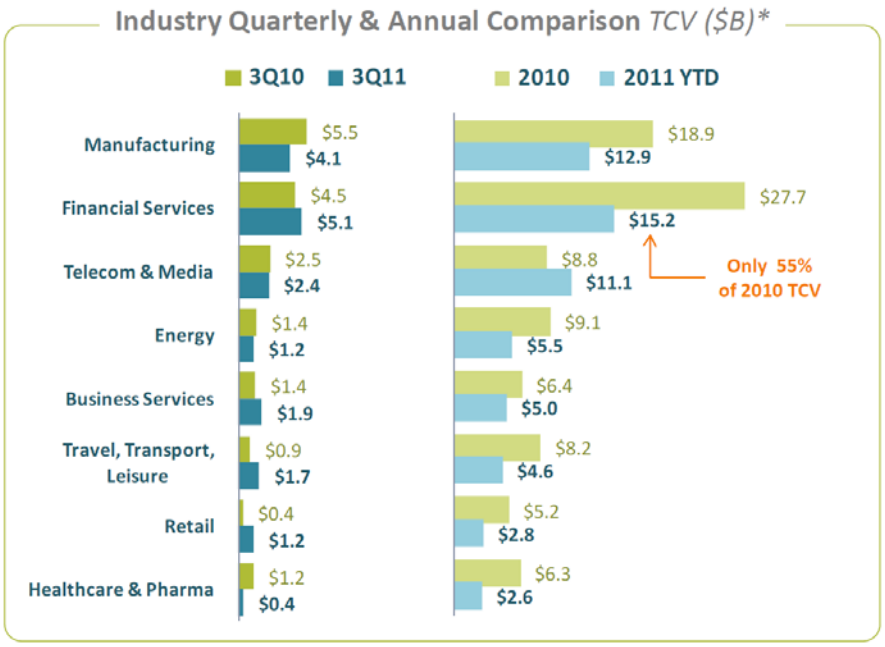

Abbildung 1.5: Vergleich von Outsourcing-Verträgen[13]

Dem Themengebiet Outsourcing ist eine ganze Reihe von Werken der aktuellen Literatur gewidmet, die die Komplexität des Themas speziell in Bezug auf die Finanzdienstleistungsbranche eingehend beschreiben: So zeigt *Andrea Marlière* die Herausforderungen des in der Praxis oft bestehenden *Sourcing-Patchworks* in Banken auf und unterstreicht die Notwendigkeit der zielgerichteten *Governance von Sourcing-Architekturen*, um deren Werterbringung zu optimieren. [26, S. 27ff.]

Die Auslagerung von IT-Diensten und Geschäftsprozessen stellt jedoch auch das betriebliche Risikomanagement vor neuartige Herausforderungen: So ist die Einhaltung von entsprechenden Niveaus an Informationssicherheit beim Dienstleister im gleichen Maße sicherzustellen, wie dies beim internen Betrieb notwendig wäre, wobei besonderes Augenmerk auf die Absicherung neu entstehender Schnittstellen zwischen den Organisationen zu legen ist. Infolgedessen ist eine Adaption der bestehenden technischen Lösungen ebenso nötig wie Ergreifung entsprechender organisatorischer Maßnahmen, zu denen beispielsweise genaue vertragliche Regelungen zu zählen sind. (vgl. bspw. [27, S. AT9.6])

[12] Die Statistik bezieht lediglich Verträge mit einem Volumen von mindestens 25 Mio. US-Dollar ein
[13] Vergleich des Total Contract Value von IT- und Geschäftsprozess-Auslagerungen in Mrd. US-Dollar 2010/11 nach Branchen

Laut *IT Governance Institute* steigt auch die Verwendung von *Cloud Computing* beim IT-Outsourcing konstant an, [24, S. 37] was diese Problematik noch verschärft: Da bei der Erbringung fertiger Dienste über das Internet die technische Umsetzung beim Dienstleister für den Kunden praktisch transparent wird, ist es für das auslagernde Unternehmen noch schwieriger, die Einhaltung von Maßnahmen zur Informationssicherheit zu überprüfen.

In Anbetracht der hohen Bedeutung von Auslagerungen und der Implikationen für den Bereich des Risikomanagements setzt sich die vorliegende Arbeit zum Ziel, die analysierten Ansätze eingehend auf deren explizite Rücksichtnahme auf Outsourcing zu untersuchen und auf dieses Themengebiet bei der Modellbildung gesondert einzugehen.

1.3 Die Modellbildung und ihr wissenschaftstheoretischer Hintergrund

Eine Modellbildung stellt nach Herbert Stachowiak eine verkürzende, pragmatische Abbildung eines Originals dar, also eine vereinfachte Darstellung von Zusammenhängen, die einem klar definierten Zweck dient, sowie zu einer bestimmten Zeit für einen bestimmten Benutzerkreis erstellt wurde. [28]

Die in der vorliegenden Arbeit vorgenommene Modellbildung basiert auf dem Prinzip der *Induktion*, d.h. sie schließt aus einer Reihe von Beobachtungen (im konkreten Fall: durch die Analyse der einfließenden Ansätze) auf ein allgemeingültiges Modell, das aus einer Menge an Axiomen (grundlegenden Sätzen) besteht.

Hierbei liegt ein der Modellierung inhärentes erkenntnistheoretisches Problem vor, das als *Induktionsproblem* bezeichnet wird und erstmals 1740 von David Hume beschrieben wurde: [29] Ein Schluss aus einer Beobachtung auf eine Allgemeinheit kann zwar widerlegt, aber niemals verifiziert werden, da die beobachteten Beispiele lediglich eine Stichprobe aus einer Grundgesamtheit darstellen, deren Eigenschaften nicht bekannt sind, sondern nur abgeschätzt werden können.

Somit kann nicht ausgeschlossen werden, dass bei einer Erweiterung der Stichprobe Beispiele beobachtet werden, die den bisherigen Schlüssen widersprechen und damit das Modell widerlegen.

Ein bekanntes Beispiel für das Induktionsproblem liefert Sir Karl Popper unter anderem in seinem 1935 erschienenen Werk *Logik der Forschung*: [30] So ließe sich aus der Beobachtung eines weißen Schwanes zwar der Satz ableiten, dass es weiße Schwäne gebe (*Existenzsatz*). Durch die Beobachtung vieler weißer Schwäne (einer großen Stichprobe) ließe sich nun durch Induktion auf die Hypothese (den *Allsatz*) schließen, dass jeder Schwan (die Grundgesamtheit der Schwäne) weiß sei, die jedoch nur so lange Gültigkeit besitze, bis ein einziger Schwan auftauche, der nicht weiß, sondern beispielsweise schwarz sei – in diesem Moment werde die Hypothese widerlegt (falsifiziert). Eine Verifizierung der Hypothese sei prinzipiell nicht möglich, da niemals ausgeschlossen werden könne, dass eines Tages ein schwarzer Schwan beobachtet werde.

Im Rahmen der vorliegenden Arbeit ist weiterhin die Besonderheit zu beachten, dass die meisten der analysierten Ansätze selbst bereits eine Modellbildung darstellen und damit der Induktionsproblematik unterliegen – durch die Bündelung eines entsprechend großen Erfahrungsschatzes bei der Erstellung und Verwaltung dieser Standards sowie durch deren meist langjährigen Einsatz im praktischen Betrieb kann das Risiko von Fehlschlüssen jedoch minimiert werden, da Fehler auffallen und einen Verbesserungsprozess anstoßen würden, was bei den meisten dieser Ansätze auf interativ-inkrementelle Art und Weise (und in begrenztem Umfang) auch regelmäßig durch Überarbeitungen geschieht.

Aus dieser Tatsache ergibt sich jedoch die Notwendigkeit für das Integrationsmodell, Veränderungen in den Ansätzen ohne unverhältnismäßig hohen Aufwand integrieren zu können.

1.4 Related Work

Dieser Abschnitt behandelt die Verfügbarkeit von Literatur zum Thema IT-Risikomanagement, beschreibt bestehende Integrationsansätze, und grenzt die in dieser Arbeit vorgestellte Modellbildung von jenen ab.

1.4.1 Literatur

Zum Themenbereich des allgemeinen Risikomanagements ist eine durchaus beträchtliche Zahl an Literaturwerken – auch in deutscher Sprache – vorhanden, die die verschiedenen Aspekte des Gebietes eingehend behandeln. So ergibt eine Suche im Gesamtkatalog des österreichischen Bibliothekenverbundes für den Begriff *Risikomanagement* nicht weniger als 4.800 Treffer, davon alleine mehr als 960 Hochschulschriften. Eine Einschränkung auf *IT Risikomanagement* zeigt noch knapp über 740 treffende Ergebnisse, wohingegen der exakte Begriff *IT-Risikomanagement* in lediglich 45 Titeln auftaucht. [31]

Eine umfassende Recherche in den Universitätsbibliotheken der Stadt Wien ergibt im Jahr 2011 nur rund 30 verwertbare Literaturquellen zu diesem Themengebiet, von denen jedoch ein großer Teil lediglich IT-Risikomanagement nach einzelnen Standards behandelt, und weder Vergleiche noch Integrationsbemühungen vornimmt.

Als Beispiel für ein ganzheitliches risiko-getriebenes Informationssicherheitsmodell mit hohem Strukturierungsgrad und langjähriger Abstimmung mit praktischen Erfahrungen sei hier die Sicherheitspyramide nach *Klaus-Rainer Müller* genannt, die der Autor in seinem Werk *IT-Sicherheit mit System* vorstellt (siehe Abbildung 1.6). [32]

Wie für derartige Lösungen symptomatisch, werden in dieser Veröffentlichung zwar einige der relevanten Rahmenwerke und Standards genannt, die einen thematischen Bezug zum beschriebenen Modell besitzen, wohingegen jedoch nicht nachvollziehbar ist, ob und inwiefern diese Ansätze bei der Modellbildung einflossen.

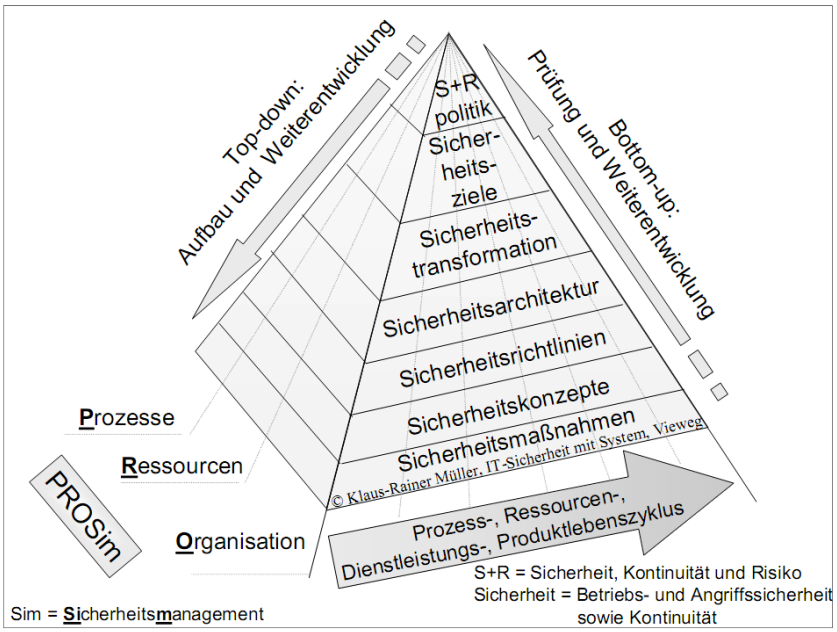

Abbildung 1.6: Sicherheitspyramide IV nach Klaus-Rainer Müller[14]

1.4.2 Integrationsbemühungen der ENISA

Eine umfangreiche Informationssammlung zum Themenkomplex Informationssicherheit und Risikomanagement stellt auch die *Europäische Agentur für Netz- und Informationssicherheit* (*European Network and Information Security Agency, ENISA*) auf ihrer Webseite bereit. [33]

Neben einer Datenbank zu bestehenden Ansätzen für Risikoassessment und Risikomanagement [34], die anhand von über zwanzig verschiedenen Attributen beschrieben werden, finden sich dort auch Beschreibungen relevanter Prozessmodelle, die ebenfalls aus einer Reihe an Ansätzen zusammengesetzt wurden. Diese weisen zwar gegenüber anderer Literatur einen überwiegend hohen Grad an Strukturierung auf, besitzen jedoch zwei entscheidende Nachteile:

- Es liegt kein klar dokumentiertes Vorgehensmodell vor, welches die vorgenommenen Harmonisierungsschritte genau beschreibt – dadurch ist die Nachverfolgbarkeit der eingearbeiteten Ansätze nur in sehr geringem Ausmaß gegeben.
- Die Dokumente unterliegen offensichtlich keiner ausreichenden Pflege, sodass bereits viele veraltete Quellen referenziert werden.

[14] Quelle: [32, S. 70]

1.4.3 Abgrenzung und Mehrwert der vorliegenden Arbeit

Um die vorliegende Arbeit von anderen Werken aus dem gleichen Themenbereich abzuheben, wurde bei deren Erstellung auf einige Besonderheiten Wert gelegt:

- Die Arbeit beinhaltet nicht nur die Präsentation einer Musterlösung für ein idealtypisches IT-Risikomanagementsystem, sondern fokussiert vor allem auf die umfassende Vorstellung eines wiederverwendbaren Integrationsmodells zur Harmonisierung bestehender Ansätze und beschreibt die dazu notwendigen Schritte und die im Rahmen des Prozesses entstehenden Artefakte.

- Sowohl das Integrationsmodell als auch die Musterlösung weisen einen hohen Strukturierungsgrad auf und legen besonderen Wert auf die durchgängige Nachverfolgbarkeit der aus den Ansätzen entnommenen Inhalte.

- Abschließend findet eine umfangreiche Evaluierung des Integrationsmodells statt, die sowohl inhaltliche Aspekte im Vergleich zu den eingeflossenen Ansätzen betrachtet, als auch eine Kritik vom wissenschaftstheoretischen Standpunkt aus vornimmt.

Kapitel 2: Entwicklung eines Vorgehensmodells

Das für diese Arbeit entwickelte Vorgehensmodell zur Harmonisierung von Ansätzen zur Steuerung und Kontrolle in Bezug auf Risiken gliedert sich in vier Phasen, die im Folgenden überblicksmäßig vorgestellt werden.

2.1 Das Vorgehensmodell im Überblick

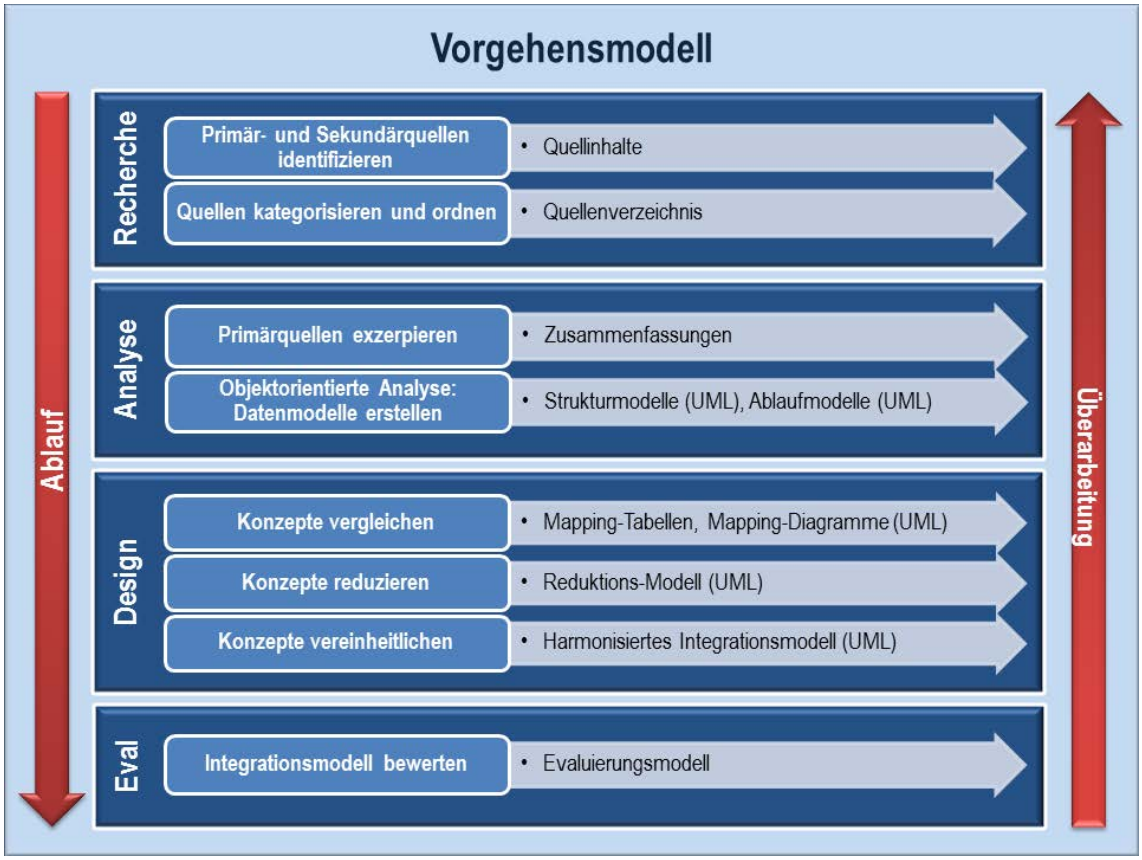

Abbildung 2.1: Vorgehensmodell zur Erstellung der vorliegenden Arbeit[15]

Im Zuge der Recherche wurden dabei zunächst jene Ansätze identifiziert, die als Primärquellen für die vorliegende Arbeit dienen sollten. Bei deren Auswahl wurde auf eine Reihe an Kriterien Wert gelegt, wie beispielsweise auf deren Bekanntheitsgrad und die Verbreitung in der Praxis, die Verwendung prozessorientierter Ansätze, sowie die Verfügbarkeit entweder über das Internet oder über lokale Bibliotheken. Des Weiteren erfolgte eine Kategorisierung und Ordnung der gewählten eingeflossenen Ansätze zur Erstellung eines Quellenverzeichnisses.

[15] Quelle: eigene Darstellung

Im Anschluss daran folgte die Phase der Analyse, die zunächst eine gründliche Exzerption der Primärquellen erforderte, um mit den oft komplexen und zudem trocken beschriebenen Inhalten eingehend vertraut zu werden, wonach die Hierarchien und Abläufe nach einem objektorientierten Ansatz analysiert wurden. Hierbei wurden mithilfe der *Unified Modeling Language* (UML) Klassen- und Aktivitätsdiagramme erstellt, um die statischen und dynamischen Aspekte der betrachteten Ansätze abzubilden. Kapitel 3 beschäftigt sich eingehend mit diesem Vorgehen und den Ergebnissen der Analysephase.

Die identifizierten Inhalte und Strukturen wurden in der nun folgenden Designphase unter Verwendung entsprechender Mapping-Tabellen und -Diagrammen einander gegenübergestellt und im Hinblick auf deren Eignung als Bausteine für ein integriertes Gesamtmodell bewertet. Der Zusammenführung der Bausteine sowie eventueller Ergänzungen folgte deren anschließende Reduktion und Harmonisierung, die sich der Bereinigung von Widersprüchen ebenso widmete wie der strukturellen und inhaltlichen Anpassung der übernommenen Bausteine, worauf Kapitel 4 im Detail eingeht.

Abschließend wurden das zuvor erarbeitete Integrationsmodell bewertet und die dabei gefundenen Verbesserungspotenziale im Rahmen einer Überarbeitung der entsprechenden Dokumente umgesetzt. Die Evaluierung wird zusammen mit einer kritischen Betrachtung der durchgeführten Modellbildung in Abschnitt Kapitel 5 behandelt.

Kapitel 3: Recherche und Objektorientierte Analyse

In diesem Abschnitt werden das Vorgehen sowie die Ergebnisse aus den Phasen der Recherche und Analyse beschrieben. Nach einem Überblick über die durchgeführten Schritte sowie die erstellten Artefakte findet eine umfassende Vorstellung von Ansätzen zur Steuerung und Kontrolle von Risiken statt, die die für die vorliegende Arbeit ausgewählten Primärquellen sowie einige weitere bedeutende Rahmenwerke zum Themenkreis beinhaltet. Abschließend findet eine erste Einordnung dieser Ansätze im Rahmen einer Grobstrukturierung statt.

3.1 Vorgehen

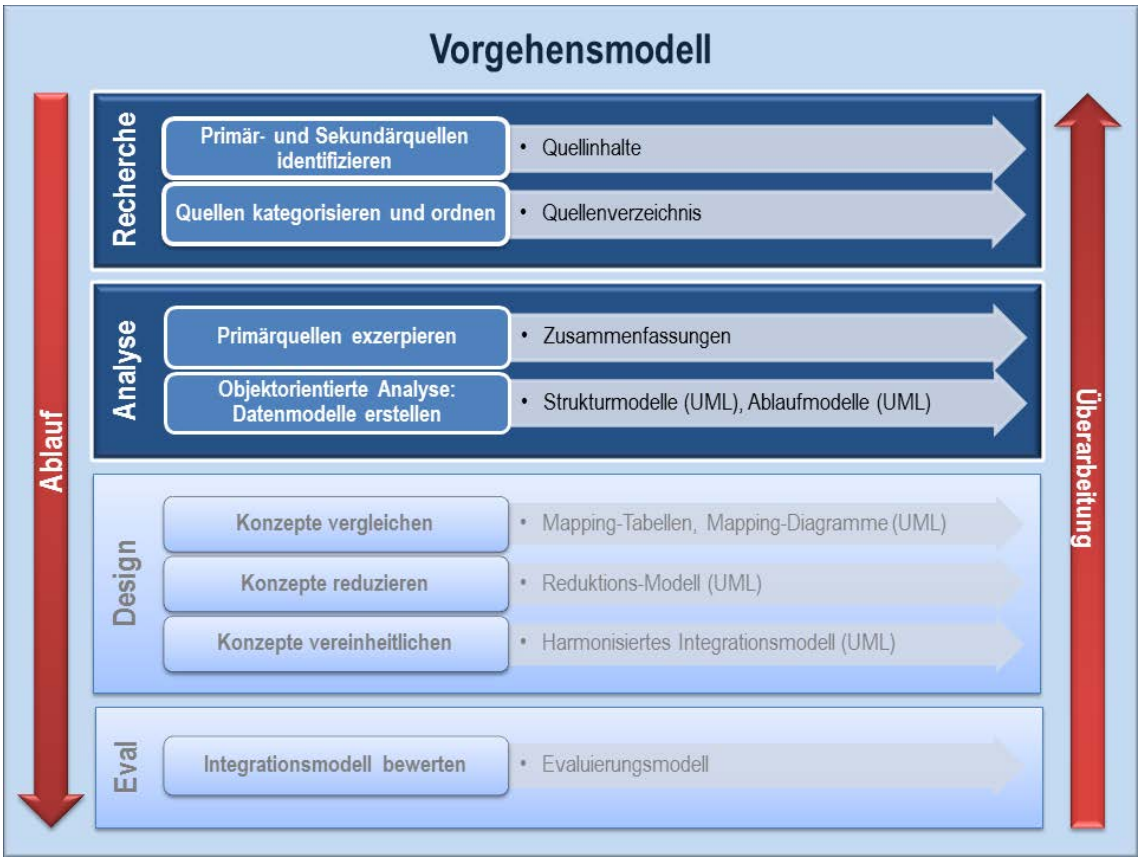

Abbildung 3.1: Vorgehensmodell: Analysephase[16]

Für die vorliegende Arbeit wurde eine Reihe an Primärquellen ausgewählt, wobei auf die Erfüllung der genannten Kriterien sowie die Abdeckung der in Abschnitt 1.1.1 genannten Aspekte Wert gelegt wurde. Zu diesen Primärquellen zählen:

[16] Quelle: eigene Darstellung

- Die Normen-Reihe *ISO/IEC 2700x*, die auf die Sicherstellung von Informationssicherheit im Unternehmensbetrieb ausgelegt ist und auch einen Standard zum IT-Risikomanagement enthält.

- Die Norm *ISO 31000*, die von den Konzepten aus *ISO/IEC 2700x* weiter abstrahiert und die dort vorgestellten Ansätze auf den allgemeinen Unternehmensbetrieb überträgt.

- Das Good-Practice-Framework *COSO ERM*, das als de-facto-Standard für die Ausgestaltung von Internen Kontrollsystemen (IKS) gilt.

- Das Framework *Risk IT* der ISACA, das ebenfalls auf das Vorgehen beim IT-Risikomanagement fokussiert.

- Der für Finanzdienstleistungsinstitute gültige Komplex an Regelungen aus *Basel II*, dem deutschen *Kreditwesengesetz* (*KWG*), der *Solvabilitätsverordnung* (*SolvV*) und dem Rundschreiben *Mindestanforderungen an das Risikomanagement* (*MaRisk*), die auch für den branchenunabhängigen Einsatz sinnvolle Konzepte zum Risikomanagement definieren.

- Der US-Amerikanische *Sarbanes-Oxley Act* (SOX), der unter anderem Anforderungen an die Ausgestaltung von Internen Kontrollsystemen (IKS) stellt.

- Die weit verbreiteten IT-Management-Standards *ITIL* und *COBIT*, die detaillierte Steuerungs- und Kontrollziele sowie Maßnahmen beschreiben, mithilfe deren Informationssicherheit durch IT-Risikomanagement erreicht werden kann.

Diese Ansätze wurden zunächst exzerpiert, wobei Textdokumente entstanden, die die wesentlichen Bestandteile und Kernaussagen zusammenfassten und dadurch die weitere Bearbeitung erleichterten.

3.1.1 Modellierung der statischen Aspekte: Hierarchien

Im Zuge des für diese Arbeit vorgenommenen Harmonisierungsprozesses wurde im Anschluss an die zuvor beschriebene Exzerpierung der Ansätze eine objektorientierte Analyse in Bezug auf statische Inhalte durchgeführt, deren Ergebnisse in Form von UML-Klassendiagrammen festgehalten wurden. Dabei wurde versucht, mithilfe typischer UML-Konstrukte wie *Paketen*, den verschiedenen *Assoziationsklassen* und einem eigenen System an *Stereotypen* eine einheitliche Strukturierung zu erreichen, die die spätere Vergleichbarkeit erleichtern sollte. Zur Verdeutlichung der Hierarchien wurde des Weiteren ein System zur farblichen Kodierung der einzelnen Hierarchieebenen entwickelt.

Der folgende Überblick über die verschiedenen Ansätze zur Steuerung und Kontrolle von Risiken der Informationssicherheit basiert unmittelbar auf dieser Analyse und stellt die dabei erarbeiteten Inhalte in textueller, tabellarischer und grafischer Form dar.

Da die erstellten UML-Diagramme vor allem bei umfangreichen Anästzen wie *ITIL*, *COBIT* oder der *ISO/IEC 27002* jedoch eine sehr große Zahl an Elementen enthalten – insgesamt wurden in der Analysephase vom Autor mehr als 3.300 Klassen in 14 Diagrammen modelliert –, wird auf eine vollständige Darstellung dieser Modelle verzichtet, und stattdessen eine darauf basierende vereinfachte grafische Darstellung präsentiert. Zur Verdeutlichung der Vorgehensweise und des dabei eingehaltenen Detaillierungsgrads werden im Folgenden lediglich die Originaldiagramme zur *ISO/IEC 27005* dargestellt.

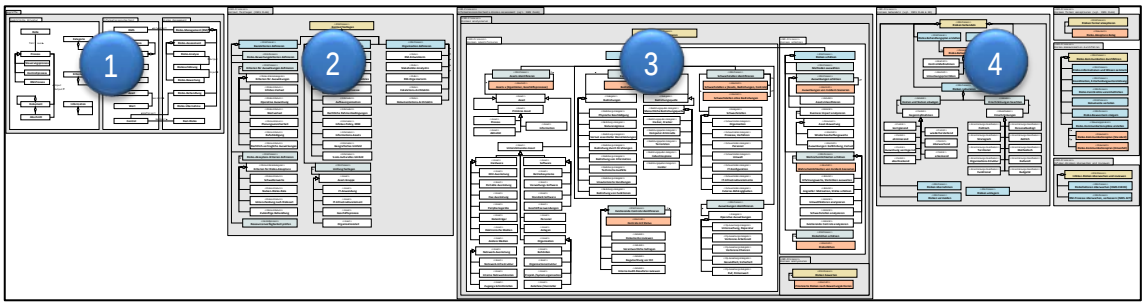

Abbildung 3.2: Gesamtmodell zur ISO/IEC 27005 – Überblick[17]

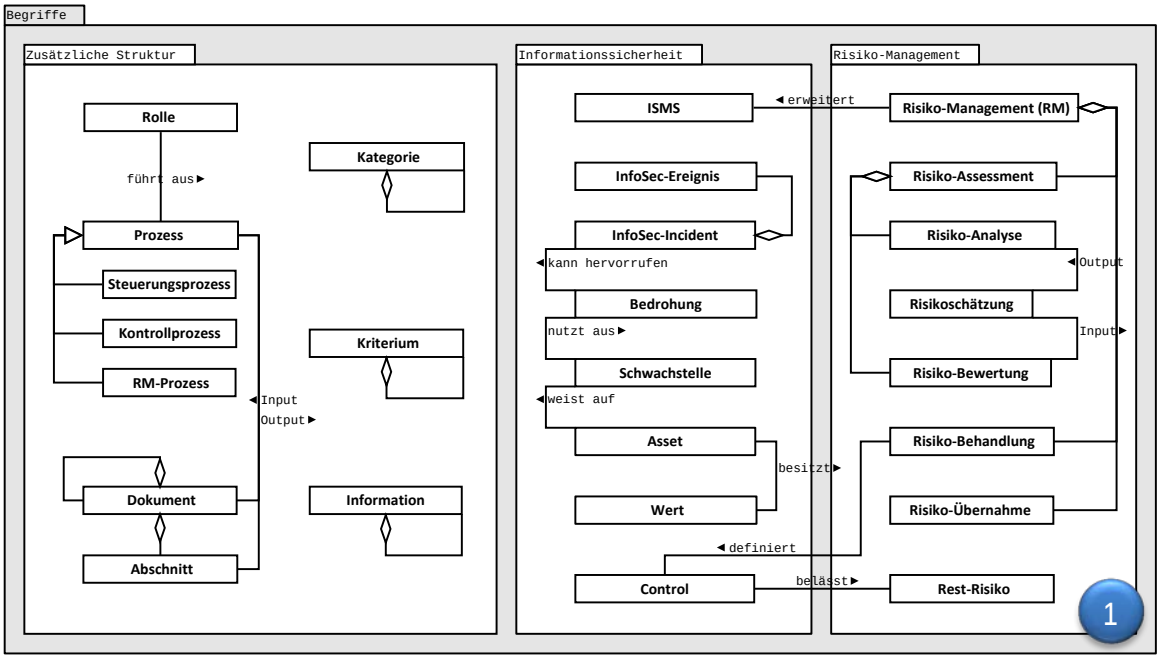

Abbildung 3.3: (1) IT-Risikomanagement nach ISO/IEC 27005[18]

[17] Quelle: eigene Darstellung
[18] Quelle: eigene Darstellung

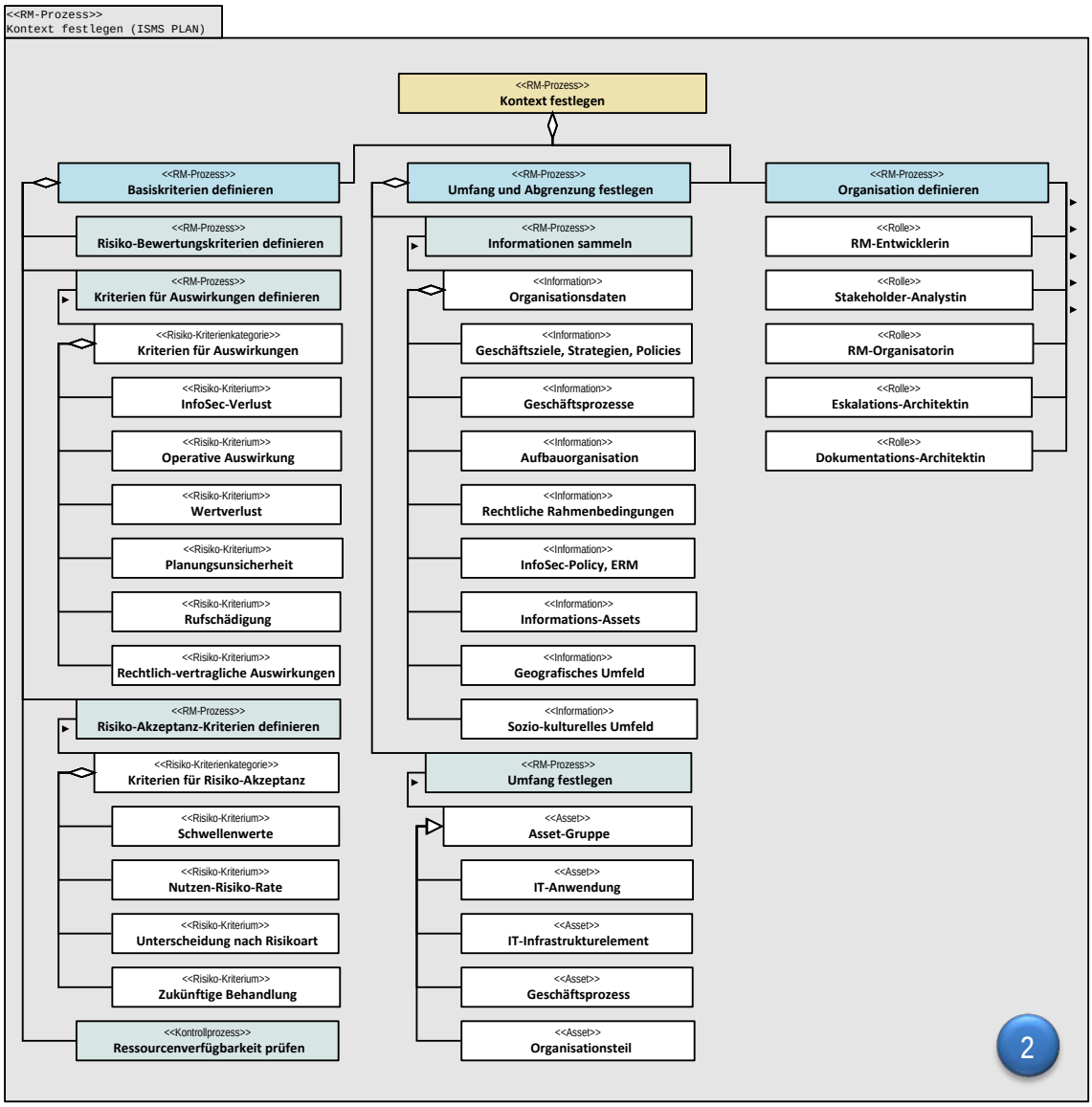

Abbildung 3.4: (2) IT-Risikomanagement nach ISO/IEC 27005

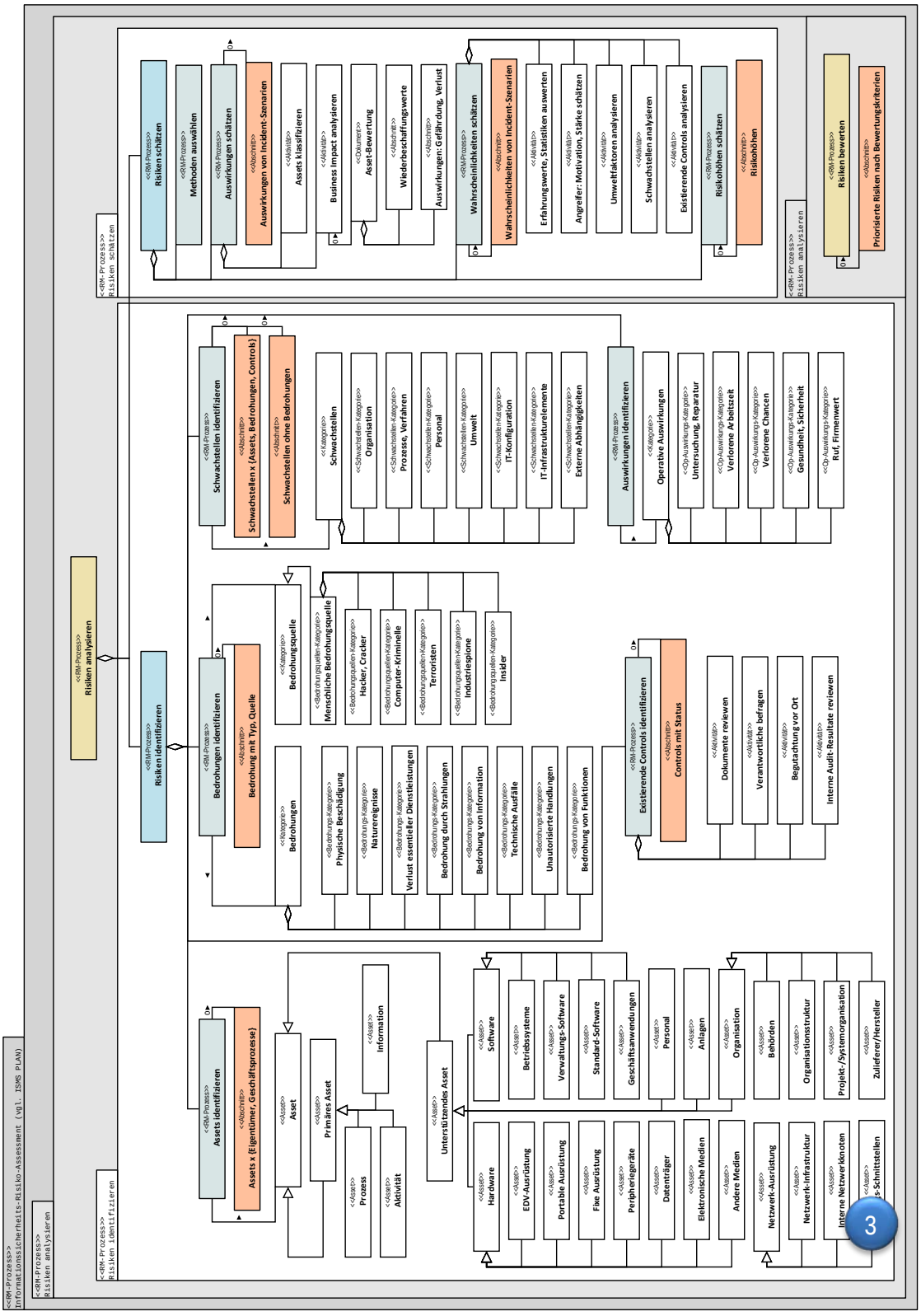

Abbildung 3.5: (3) IT-Risikomanagement nach ISO/IEC 27005[19]

[19] Quelle: eigene Darstellung

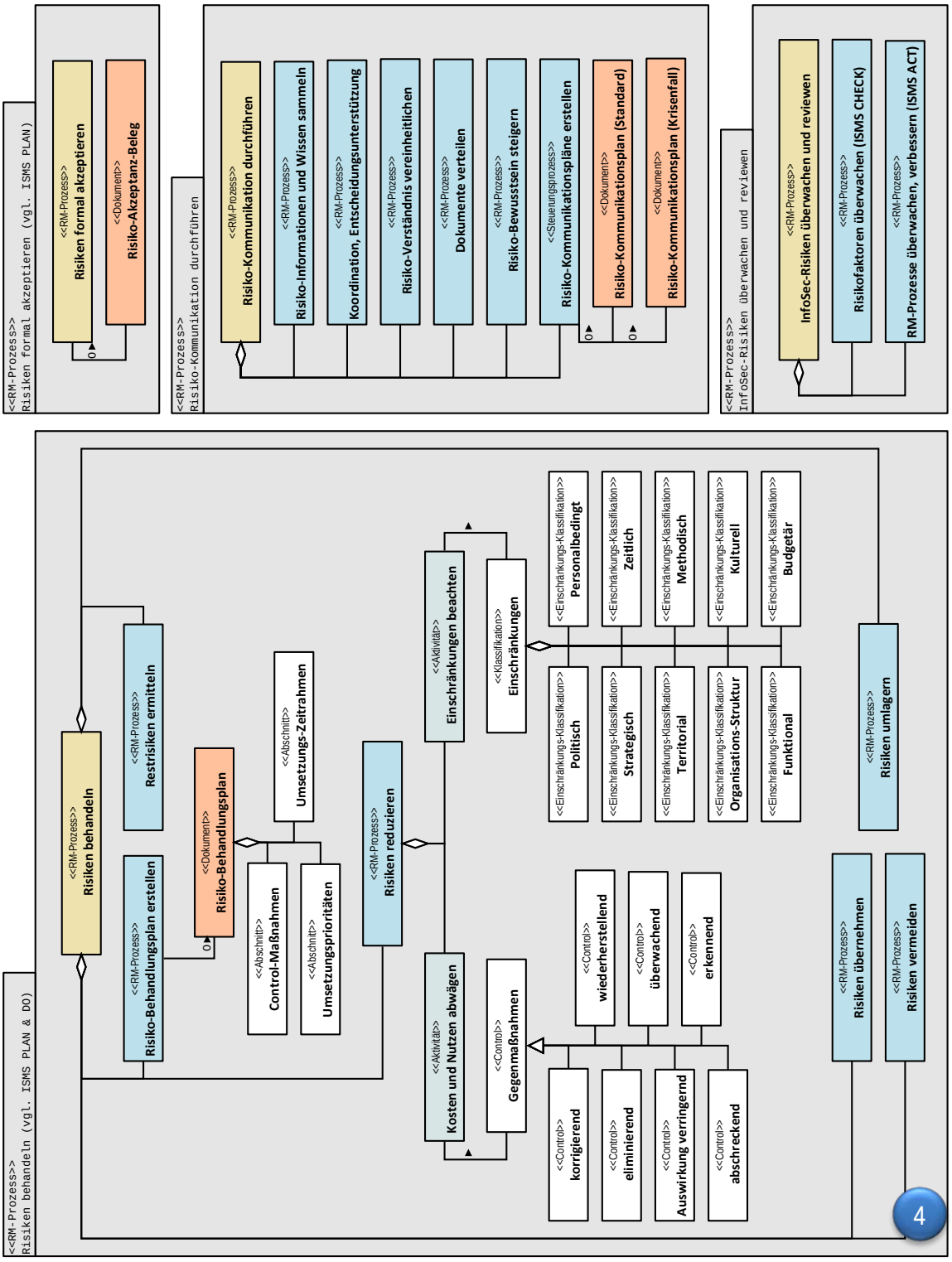

Abbildung 3.6: (4) IT-Risikomanagement nach ISO/IEC 27005[20]

[20] Quelle: eigene Darstellung

3.1.2 Modellierung der dynamischen Aspekte: Abläufe

Analog zur Modellierung der statischen Aspekte wurden die in den eingeflossenen Ansätzen beschriebenen Abläufe mithilfe von UML-Aktivitätsdiagrammen abgebildet. Dabei wurde offensichtlich, dass nur wenige Quellen die Abläufe auf einem ausreichend hohen Detaillierungsgrad definieren, um explizite Kontrollflüsse ableiten zu können, oder an verschiedenen Stellen sogar widersprüchliche Angaben liefern.[21] Die meisten der erstellten Aktivitätsdiagramme entsprechen daher streng genommen nicht unmittelbar der Syntax der UML, sondern sind lediglich an diese angelehnt. Wo dennoch sinnvoll, wurden diese Diagramme direkt in die folgenden Beschreibungen übernommen.

3.2 Vorstellung der relevanten Ansätze

Die ebenfalls enthaltene tabellarische Kurzbeschreibung dient der ersten groben Einordnung der verwendeten Ansätze, um dem Leser die Orientierung zu erleichtern. Die dabei verwendeten Kategorien und Inhalte wurden zum Großteil vom Autor erarbeitet, orientieren sich ergänzend jedoch an den von der ENISA gebrauchten (siehe Abschnitt 1.4.2, [34]). Es werden folgende Attribute verwendet, wobei für die Beschreibung der *weiteren Ansätze* in Abschnitt 3.2.12 lediglich ein eingeschränkter Satz an Kriterien zur Anwendung gelangt:

Erklärung der in der Kurzbeschreibung verwendeten Attribute	
Vollständige Bezeichnung	Name der Quelle; bei Gesetzen wird hier dennoch der verkürzte Titel angegeben[22]
Herkunft	• Standardisierungsgremium: Nationales oder internationales Gremium für Normung oder Standardisierung. • Private Institution: Nicht-öffentliche Organisation außer Standardisierungsgremien, schließt auch private Non-Profit-Organisationen mit ein. • Öffentliche Institution, Gesetzgeber: Alle öffentlichen Organisationen und staatliche Gesetzgeber.
Erscheinungsjahr	Jahr der Veröffentlichung, falls vorhanden der ersten und letzten Version bzw. der letzten Überarbeitung
Seitenzahl	Ungefährer Umfang der Quelle. Richtet sich nach der Seitenzahl der offiziellen Publikationen bzw. nach einem Ausdruck in 12-Punkt-Schrift auf Seitengröße A4, falls keine gedruckte Publikation vorhanden ist
Ziel	• IT-Sicherheit: Es wird lediglich die Absicherung technischer Bausteine betrachtet.

[21] Vergleiche dazu bspw. den Abschnitt zu Risk IT (3.2.6)
[22] Dieser ist in Bezug auf die Aussagekraft dem vollen Titel in den meisten Fällen ebenbürtig

Erklärung der in der Kurzbeschreibung verwendeten Attribute	
	• Informationssicherheit: Ziel des Ansatzes ist es, Information unabhängig von technischen Geräten zu schützen, wobei technische und organisatorische Aspekte betrachtet werden. • Sicherer Unternehmensbetrieb: Der Ansatz ist nicht speziell auf IT- oder Informationssicherheit ausgerichtet, sondern zielt auf den sicheren Unternehmensbetrieb im Allgemeinen ab.
Schwerpunkt	• Risikomanagement: Der Ansatz stellt ein Management-System vor, welches zur Steuerung und Kontrolle von Risiken geeignet ist. • Steuerung und Kontrolle: Der Ansatz beinhaltet eine Sammlung an Maßnahmen oder Vorschriften zur Steuerung und Kontrolle von Risiken, jedoch kein Management-System oder vergleichbare Prozessdefinitionen. • Qualitätsmanagement/Reifegrade: Der Ansatz definiert Reifegradmodelle zur Beurteilung der Qualität von Systemen oder Prozessen.
Art	• Standard: Nationaler oder internationaler Standard eines Normungs- oder Standardisierungsgremiums mit oder ohne Zertifizierungsmöglichkeit auf institutioneller Basis. • Good-Practice-Framework/Referenzmodell: Sammlung an Verfahrensweisen oder Ähnlichem, die aus beispielhaften Erfahrungen im Praxisbetrieb zusammengestellt wurden. • Gesetz/Verpflichtende Regelung: Der Ansatz definiert bindende Vorschriften gesetzlicher oder anderer Natur, stellt jedoch keinen Standard eines Normungs- oder Standardisierungsgremiums dar.
Detaillierungsgrad	• Niedrig: Nach Einschätzung des Autors geringe Detaillierung – beispielsweise werden Maßnahmen lediglich namentlich angeführt, enthalten jedoch keine genauere Beschreibung (z.B. SOX). • Mittel: Nach Einschätzung des Autors mittlere Detaillierung – Maßnahmen werden beispielsweise zueinander in Beziehung gesetzt sowie notwendige Rollen und Verantwortlichkeiten oder In- und Output-Artefakte genannt (z.B. COSO ERM). • Hoch: Nach Einschätzung des Autors hohe Detaillierung – Maßnahmen werden beispielsweise samt umfangreichen Hinweisen zur Umsetzung beschrieben und zueinander in Beziehung gesetzt, sowie notwendige Rollen und Verantwortlichkeiten oder In- und Output-Artefakte

Erklärung der in der Kurzbeschreibung verwendeten Attribute	
	beschrieben (z.B. ITIL V3).
Strukturierungsgrad	• Niedrig: Nach Einschätzung des Autors geringe Strukturierung – Strukturierungskomponenten (logische Klassen) sind auch im Rahmen einer detaillierten objektorientierten Analyse kaum erkennbar oder werden nicht konsequent eingesetzt (z.B. SOX). • Mittel: Nach Einschätzung des Autors mittlere Strukturierung – es liegt beispielsweise eine Zahl an Strukturierungskomponenten (logischer Klassen) vor, die im Rahmen einer objektorientierten Analyse leicht erkennbar sind und überwiegend verwendet werden (z.B. Basel-II-Konglomerat). • Hoch: Nach Einschätzung des Autors starke Strukturierung – es liegt beispielsweise eine große Zahl an Strukturierungskomponenten (logischer Klassen) vor, die explizit beschrieben, zueinander in Beziehung gesetzt und durchgängig verwenden werden (z.B. COBIT 4.1).

Tabelle 3.1: Attribute für die Kurzbeschreibungen der verwendeten Ansätze[23]

Im Folgenden werden die verschiedenen Ansätze zur Steuerung und Kontrolle von Risiken der Informationssicherheit vorgestellt und deren Inhalte in textueller, tabellarischer und grafischer Form aufbereitet.

3.2.1 ISO/IEC 27001

Die internationale Norm *ISO/IEC 27001* [14] definiert Anforderungen an ein *Informationssicherheits-Managementsystem (ISMS)*, das die Bedürfnisse der jeweiligen Organisation und deren Aufbau- und Ablauforganisation ebenso berücksichtigt wie spezifische Sicherheitsanforderungen und die kontinuierliche Veränderung dieser Elemente. [14, S. v] Die Zertifizierungsmöglichkeit für die ISO/IEC 27001 wurde mit Stand November 2011 von weltweit über 7.500 Institutionen genutzt, davon rund 230 in Deutschland, Österreich und der Schweiz. [35]

Kurzbeschreibung ISO/IEC 27001	
Vollständige Bezeichnung	ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements
Herkunft	Standardisierungsgremium: International Organization for Standardization, International Electrotechnical Commission (ISO/IEC, Schweiz)

[23] Quelle: eigene Darstellung

Kurzbeschreibung ISO/IEC 27001	
Erscheinungsjahr	Erste Version 1993, letzte Überarbeitung 2008
Seitenzahl	34
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Internationaler Standard (zertifizierbar)
Detaillierungsgrad	Mittel
Strukturierungsgrad	Hoch

Tabelle 3.2: Kurzbeschreibung der ISO/IEC 27001[24]

Das ISMS wird nach ISO/IEC 27001 prozessorientiert aufgebaut und basiert auf dem bekannten *Deming-Zyklus*, der hier als *Plan-Do-Check-Act-Modell (PDCA)* bezeichnet wird und die klassischen Aufgaben des Managements anhand dieser vier Phasen gliedert.

Der starke Fokus dieses Standards auf den Bereich des Risikomanagements wird bereits durch die angeführten Begriffsdefinitionen deutlich, die beinahe zur Hälfte Termini erläutern, die das Wort *Risiko* enthalten. [14, S. 2f.] In den weiteren Kapiteln werden überblicksmäßig die Prozesse und Aktivitäten zum Aufbau und Betrieb sowie zur Überwachung, Begutachtung, Wartung und kontinuierlichen Verbesserung eines ISMS beschrieben. Ein eigener Abschnitt geht zudem auf die Anforderungen zur Verwaltung der zugehörigen Dokumentation und Belege ein, was im Kreis der analysierten Ansätze eine Seltenheit darstellt.

Zudem werden die Verantwortlichkeiten der Management-Ebene genannt und interne ISMS Audits beschrieben. Die Anforderungen für die regelmäßige Prüfung des ISMS durch das Management fallen insbesondere durch die genaue Spezifikation der Input- und Output-Dokumente auf, [14, S. 10f.] wohingegen das Kapitel zur kontinuierlichen Verbesserung des Systems nicht mehr als eine Seite umfasst. [14, S. 11f.]

Eine überblicksmäßige Darstellung der Inhalte und Struktur der ISO/IEC 27001 findet sich in Abbildung 3.7.

[24] Quelle: eigene Darstellung

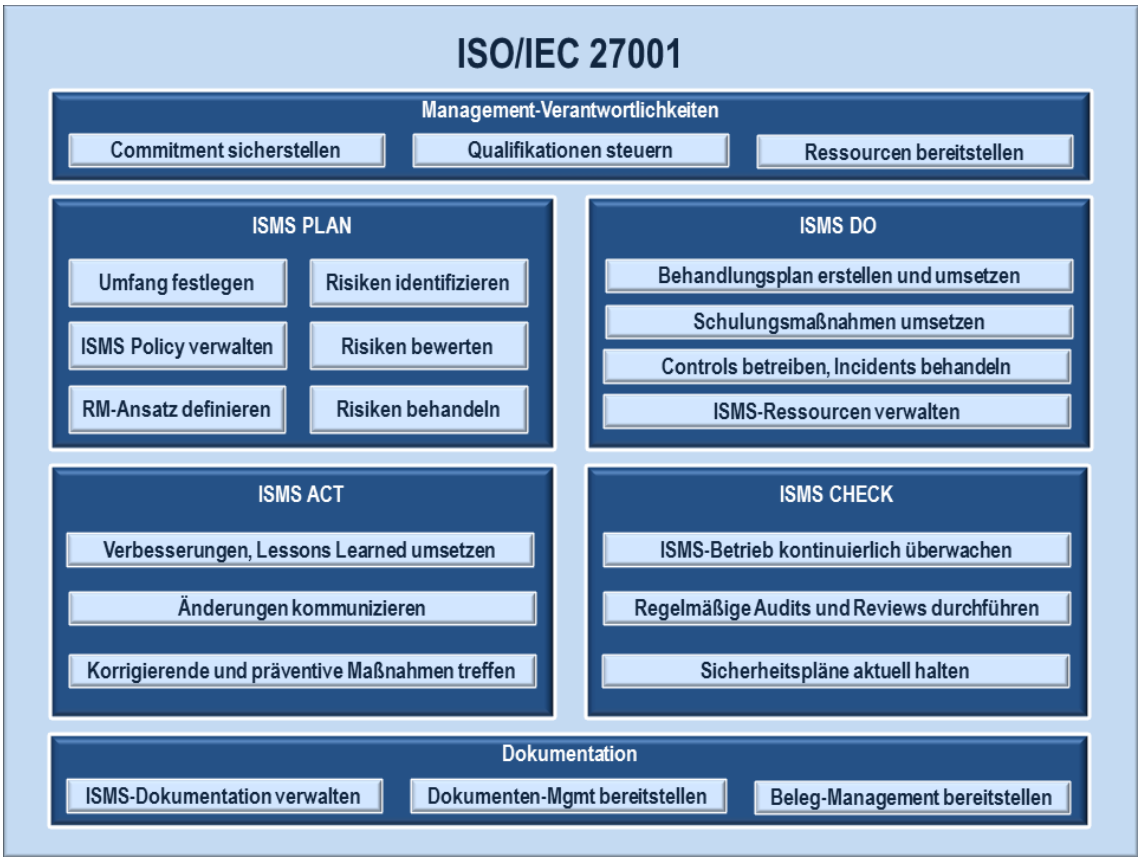

Abbildung 3.7: Inhalt und Struktur der ISO/IEC 27001 (grobe Übersicht)[25]

[25] Quelle: Eigene Darstellung nach [14]

3.2.2 ISO/IEC 27002

Der Standard *ISO/IEC 27002* [19] mit dem Titel *Leitfaden für das Informationssicherheits-Management* definiert eine umfangreiche Sammlung an Sicherheitsmaßnahmen und steht in direkter Beziehung zur ISO/IEC 27001, in deren normativem Anhang A explizit auf die Maßnahmen aus ISO/IEC 27002 verwiesen wird.

Kurzbeschreibung ISO/IEC 27002	
Vollständige Bezeichnung	ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management
Herkunft	Standardisierungsgremium: International Organization for Standardization, International Electrotechnical Commission (ISO/IEC, Schweiz)
Erscheinungsjahr	Erste Version 2000, letzte Überarbeitung 2008
Seitenzahl	115
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Internationaler Standard (nicht zertifizierbar)
Detaillierungsgrad	Mittel
Strukturierungsgrad	Hoch

Tabelle 3.3: Kurzbeschreibung ISO/IEC 27002[26]

Der Standard gliedert die vorgestellten Maßnahmen in insgesamt elf Überwachungsbereiche, die überblicksmäßig in Abbildung 3.8 visualisiert werden und eine einheitliche Struktur aufweisen: So werden pro Kategorie zunächst *Steuerungs- und Kontrollziele* definiert (insgesamt 39), welche durch die Umsetzung der anschließend beschriebenen *Sicherheitsmaßnahmen* (insgesamt 133) erreicht werden soll. Für jede dieser Maßnahmen finden sich neben einer Beschreibung auch eine Anleitung zu deren Implementierung sowie weiterführende Informationen.

[26] Quelle: eigene Darstellung

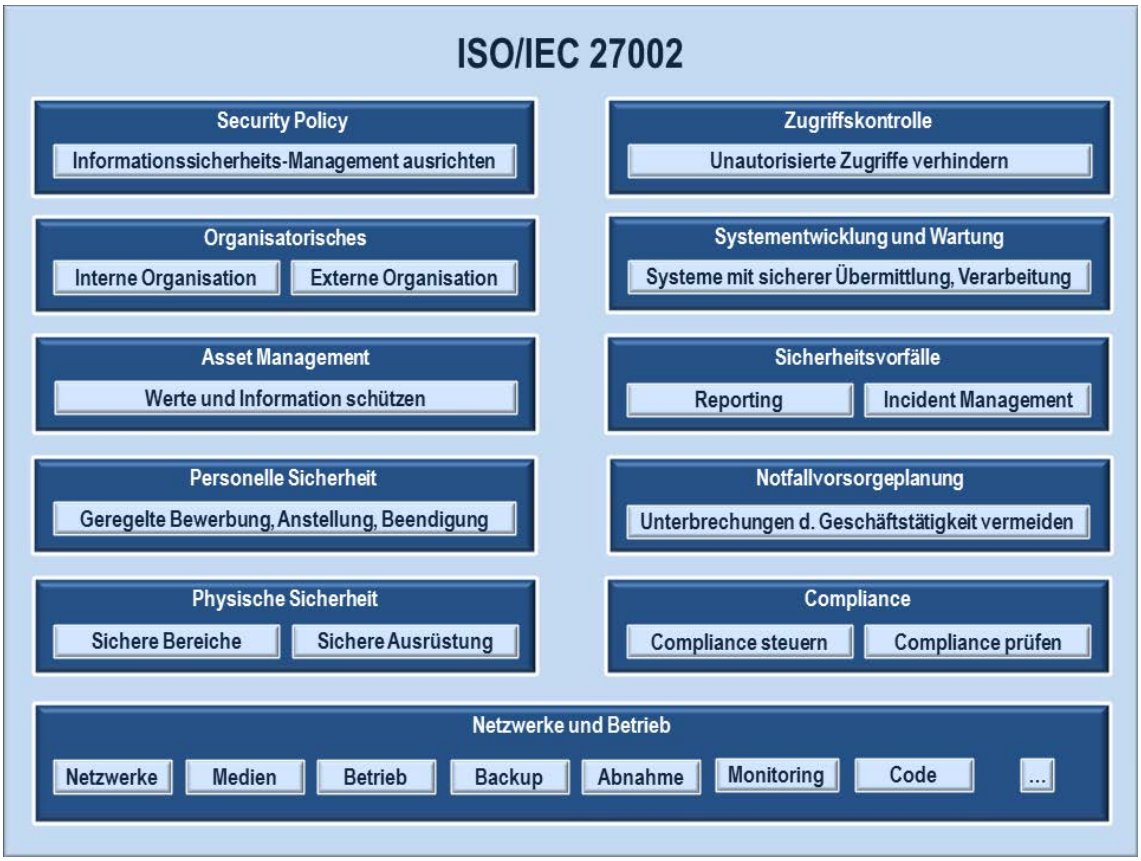

Abbildung 3.8: Inhalt und Struktur der ISO/IEC 27002 (grobe Übersicht)[27]

Zwar ist die ISO/IEC 27002 grundsätzlich auf die Sicherstellung von Informationssicherheit im Bereich der IT ausgerichtet, jedoch finden sich zahlreiche Überschneidungen zu anderen umfangreichen Rahmenwerken wie ITIL aus dem IT Service Management oder COBIT aus dem Bereich der IT Governance. Aus diesem Grund existiert eine Reihe an Dokumenten, die diese Ansätze zueinander in Beziehung setzen (*mappen*), wie beispielsweise die entsprechende Initiative von OGC und ITGI (den Autoren von ITIL und COBIT), die auch für die vorliegende Arbeit als Grundlage verwendet wurde, um diese drei Ansätze zu harmonisieren. [36]

3.2.3 ISO/IEC 27005

Die *ISO/IEC 27005* [18] stellt Leitlinien für das Management von Risiken der Informationssicherheit bereit und ist auf volle Kompatibilität zu den in der ISO/IEC 27001 und 27002 beschriebenen Konzepten, Modellen, Prozessen und Begrifflichkeiten ausgelegt.

[27] Quelle: Eigene Darstellung nach [19]

Kurzbeschreibung ISO/IEC 27005	
Vollständige Bezeichnung	ISO/IEC 27005:2008 – Information technology – Security techniques – Information security risk management
Herkunft	Standardisierungsgremium: International Organization for Standardization, International Electrotechnical Commission (ISO/IEC, Schweiz)
Erscheinungsjahr	Erste Version 2008, letzte Überarbeitung 2011[28]
Seitenzahl	2008: 55; 2011: 68
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Internationaler Standard (nicht zertifizierbar)
Detaillierungsgrad	Mittel
Strukturierungsgrad	Hoch

Tabelle 3.4: Kurzbeschreibung der ISO/IEC 27005[29]

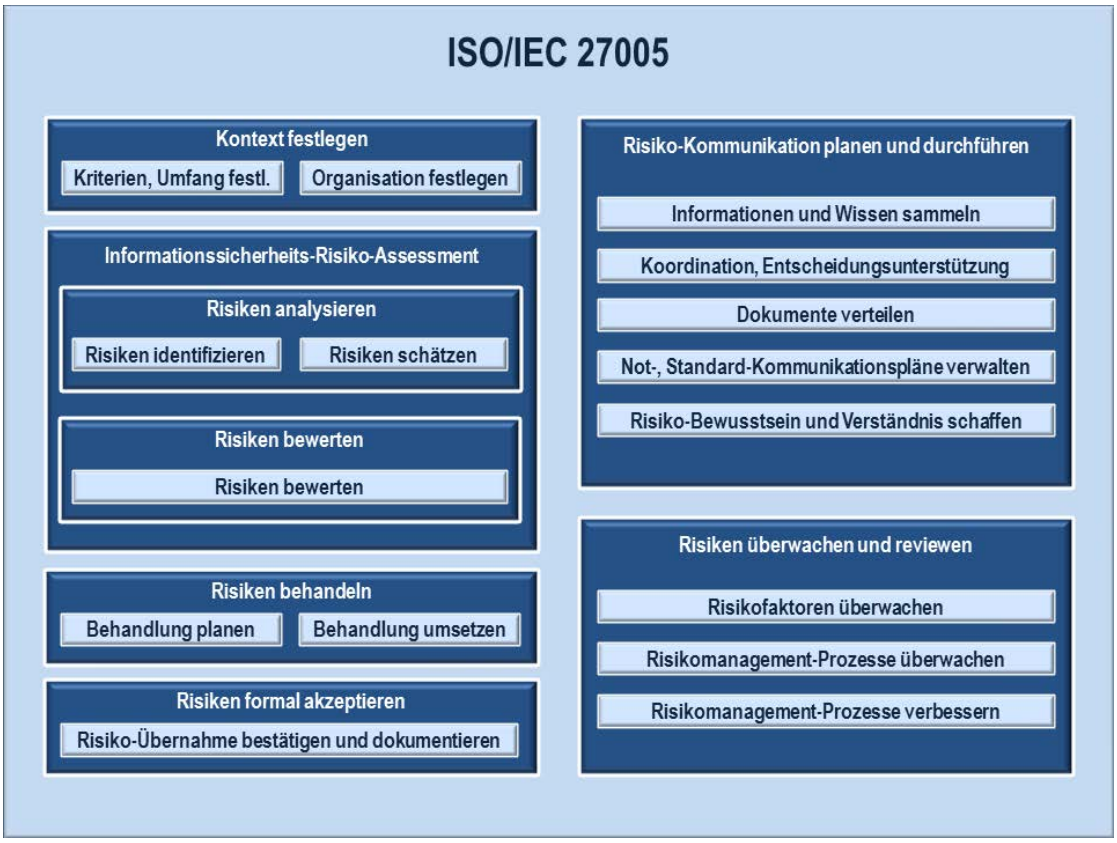

Abbildung 3.9: Inhalt und Struktur der ISO/IEC 27005 (grobe Übersicht)[30]

[28] Als Grundlage für die vorliegende Arbeit dient die Version von 2008
[29] Quelle: eigene Darstellung

Bei einer Analyse des Standards fällt auf, dass in der Tat starke inhaltliche Überschneidungen zwischen der ISO/IEC 27005 und den ersten beiden Standards der Reihe 2700x bestehen – so werden beispielsweise die Festlegung des Kontextes, die Identifikation und Bewertung von Risiken und deren Behandlung und Überwachung auch in ISO/IEC 27001 als Anforderungen an ein ISMS genannt.

Allerdings werden diese Inhalte nun nicht aus der Perspektive eines Informationssicherheits-Managementsystems nach dem PDCA-Modell dargestellt, sondern anhand eines klar strukturierten Risikomanagement-Prozesses betrachtet, der in Abbildung 3.10 veranschaulicht wird. Die ISO/IEC 27005 geht im Rahmen der Prozessbeschreibung explizit auf diesen inhaltlichen Dualismus ein und ordnet die Prozessschritte von ISMS und Risikomanagement-Prozess einander tabellarisch zu, wobei auffällt, dass die Zuordnung der Prozessschritte des Risikomanagements zu den PDCA-Phasen in der ISO/IEC 27005 deutlich von der Zuordnung aus der ISO/IEC 27001 abweichen, obwohl in beiden Normen die gleichen Inhalte integriert werden (vgl. [18, S. 6], [14, S. vi ff.]).

Der Strukturierungsgrad der ISO/IEC 27005 ist wie in der gesamten Reihe 2700x als durchgängig hoch zu bezeichnen; für die meisten Prozessschritte werden nötige In- und Output-Informationen und Dokumente ebenso beschrieben wie Hinweise zur Umsetzung und Rollen- und Verantwortlichkeitsdefinitionen. Zudem sind im Text durchgängig Querverweise zu den korrespondierenden Abschnitten der ISO/IEC 27001 vorhanden.

Neben der klaren Strukturierung bestehen auch inhaltliche Auffälligkeiten, wie die große Zahl an unterschiedlichen Klassifikationen, die in diesem Standard vorgestellt werden. Dazu zählen Kriterien für die Art und Höhe der Auswirkungen von Risiken ebenso wie Klassifikationen für Assets, Bedrohungen und Bedrohungsquellen, Schwachstellen, Sicherheits- und Risikobehandlungsmaßnahmen sowie Einschränkungen, denen eine Organisation bei der Implementierung von Risikomanagement unterworfen sein kann.

Allerdings wird im Standard explizit auf die Tatsache hingewiesen, dass aufgrund dessen generischer Natur, die die Anwendbarkeit unabhängig von Branchen und Organisationstypen sicherstellt, die verwendeten Artefakte und die Prozesse selbst an den jeweiligen Kontext anzupassen sind; damit sind auch die unterschiedlichen Klassifikationen als Vorschläge zu verstehen, die bei Bedarf vereinfacht werden können. Im Anhang zur Norm werden unter diesem Gesichtspunkt auch unterschiedliche Möglichkeiten vorgestellt, um im Zuge eines detaillierten Risikoassessments die Höhe von Risiken zu bestimmen.

[30] Quelle: Eigene Darstellung nach [18]

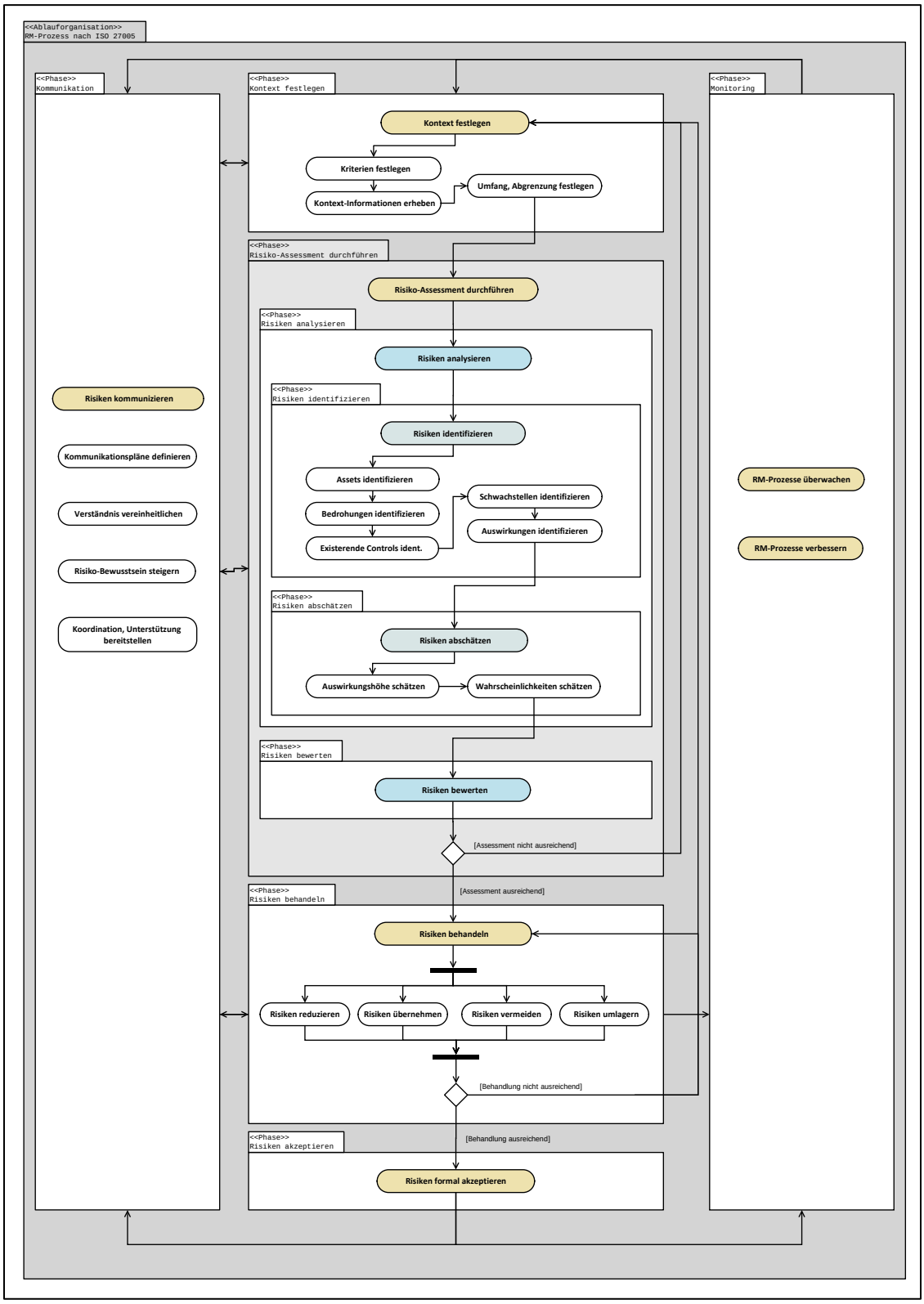

Abbildung 3.10: Der Risikomanagement-Prozess nach ISO/IEC 27005[31]

[31] Quelle: Eigene Darstellung nach [18, S. 5]

3.2.4 ISO 31000

Der Standard *ISO 31000* [15] stellt Prinzipien und Leitlinien zum Risikomanagement vor und ist im Gegensatz zu den bisher vorgestellten Normen aus der Reihe ISO/IEC 2700x nicht auf das Management von Informationssicherheit beschränkt.

Kurzbeschreibung ISO 31000	
Vollständige Bezeichnung	ISO 31000:2009 – Risk management – Principles and guidelines
Herkunft	Standardisierungsgremium: International Organization for Standardization (ISO, Schweiz)
Erscheinungsjahr	2009
Seitenzahl	24
Ziel	Operativer Unternehmensbetrieb
Schwerpunkt	Risikomanagement
Art	Internationaler Standard (nicht zertifizierbar)
Detaillierungsgrad	Niedrig
Strukturierungsgrad	Mittel

Tabelle 3.5: Kurzbeschreibung der ISO 31000[32]

Eine inhaltliche Analyse lässt jedoch die Abstammung des Standards deutlich erkennen, für den die Konzepte des ISMS aus ISO/IEC 27001 und des Risikomanagement-Prozesses nach ISO/IEC 27005 vom Themenbereich Informationssicherheit losgelöst und anschließend zusammengefasst wurden. Dementsprechend stellt die ISO 31000 ein *Risikomanagement-Framework* und einen zugehörigen *Risikomanagement-Prozess* vor, die getrennt beschrieben werden, wobei das *Framework* grob dem ISMS aus ISO/IEC 27001 und der *Prozess* annähernd jenem aus ISO/IEC 27005 entspricht (siehe Abbildung 3.11 und Abbildung 3.12).

Nach Meinung des Autors weist die ISO 31000 trotz der grundsätzlichen Brauchbarkeit des gewählten Ansatzes eine Reihe von Nachteilen struktureller wie inhaltlicher Natur auf, die die Anwendbarkeit dieses Standards in der Praxis deutlich einschränken: So ist der Detaillierungsgrad des Inhalts deutlich geringer ausgefallen als bei der Reihe ISO/IEC 2700x, was keinesfalls durch die Erweiterung der Zielsetzung vom IT- zum allgemeinen Unternehmensbetrieb gerechtfertigt werden kann (in der Tat wäre mit diesem Schritt nach Meinung des Autors eher eine Erweiterung des Umfangs zu erwarten, um beispielsweise jenem von COSO ERM zu entsprechen).

Zudem wird nicht ausreichend auf inhaltliche Überschneidungen eingegangen, die einerseits zwischen *Framework* und *Prozess* bestehen, und andererseits zwischen den verschiedenen Teilen des *Frameworks* selbst (man beachte beispielsweise das doppelte

[32] Quelle: eigene Darstellung

Vorkommen von *Verantwortlichkeiten zuweisen* in *Management-Auftrag und Commitment* sowie der Plan-Phase in Abbildung 3.11

Schließlich schlägt ISO 31000 im Vergleich zur ISO/IEC 27005 wiederum nur sehr wenige Klassifikationen für den Risikomanagement-Prozess vor, und vereinfacht den Kontrollfluss insofern zu weit, als sowohl die nach Meinung des Autors wichtigen Entscheidungspunkte (*Risk Decision Points*, [18, S. 5]) als auch die *formelle Akzeptanz von Risiken* als letzter Schritt des Prozesses ausgespart werden (vergleiche dazu Abbildung 3.10 und Abbildung 3.12).

Aus diesen Gründen besteht im Falle der ISO 31000 nach Meinung des Autors dringender Überarbeitungsbedarf, um einen Einsatz in der Praxis in Zukunft rechtfertigen zu können.

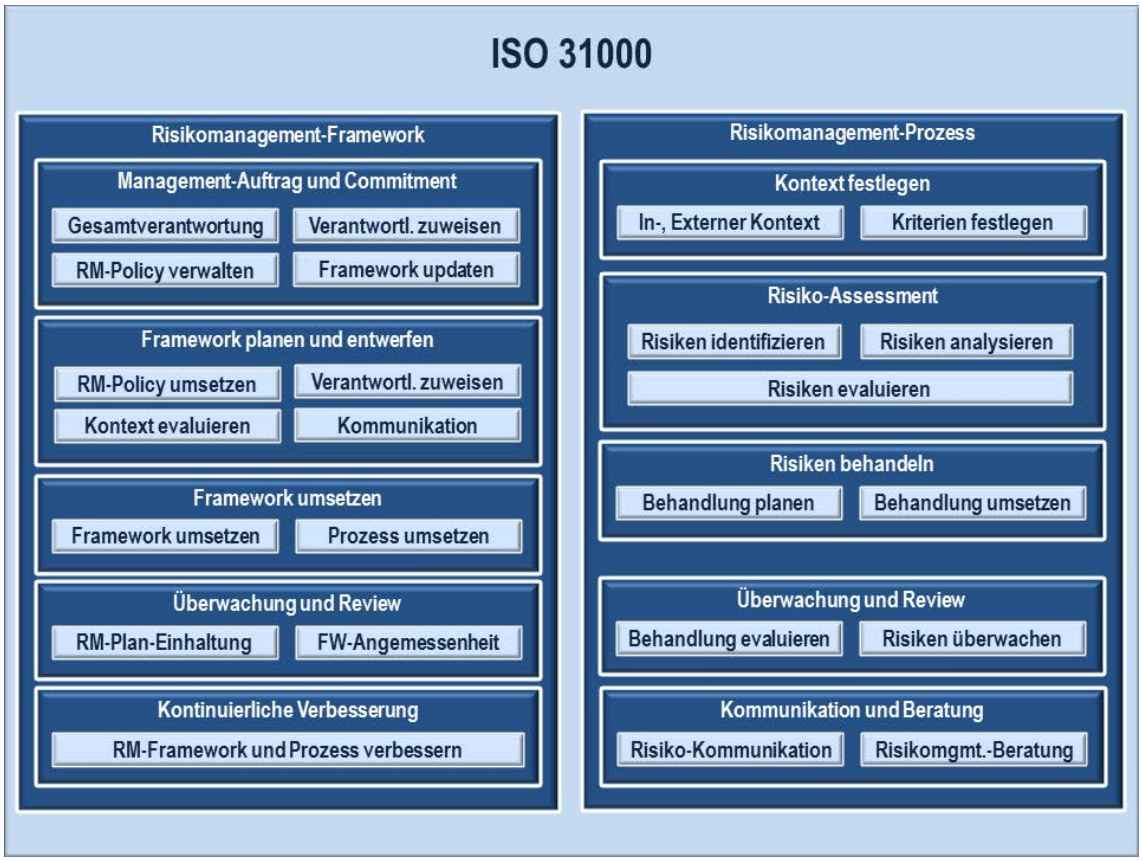

Abbildung 3.11: Inhalt und Struktur der ISO 31000 (grobe Übersicht)[33]

[33] Quelle: Eigene Darstellung nach [15]

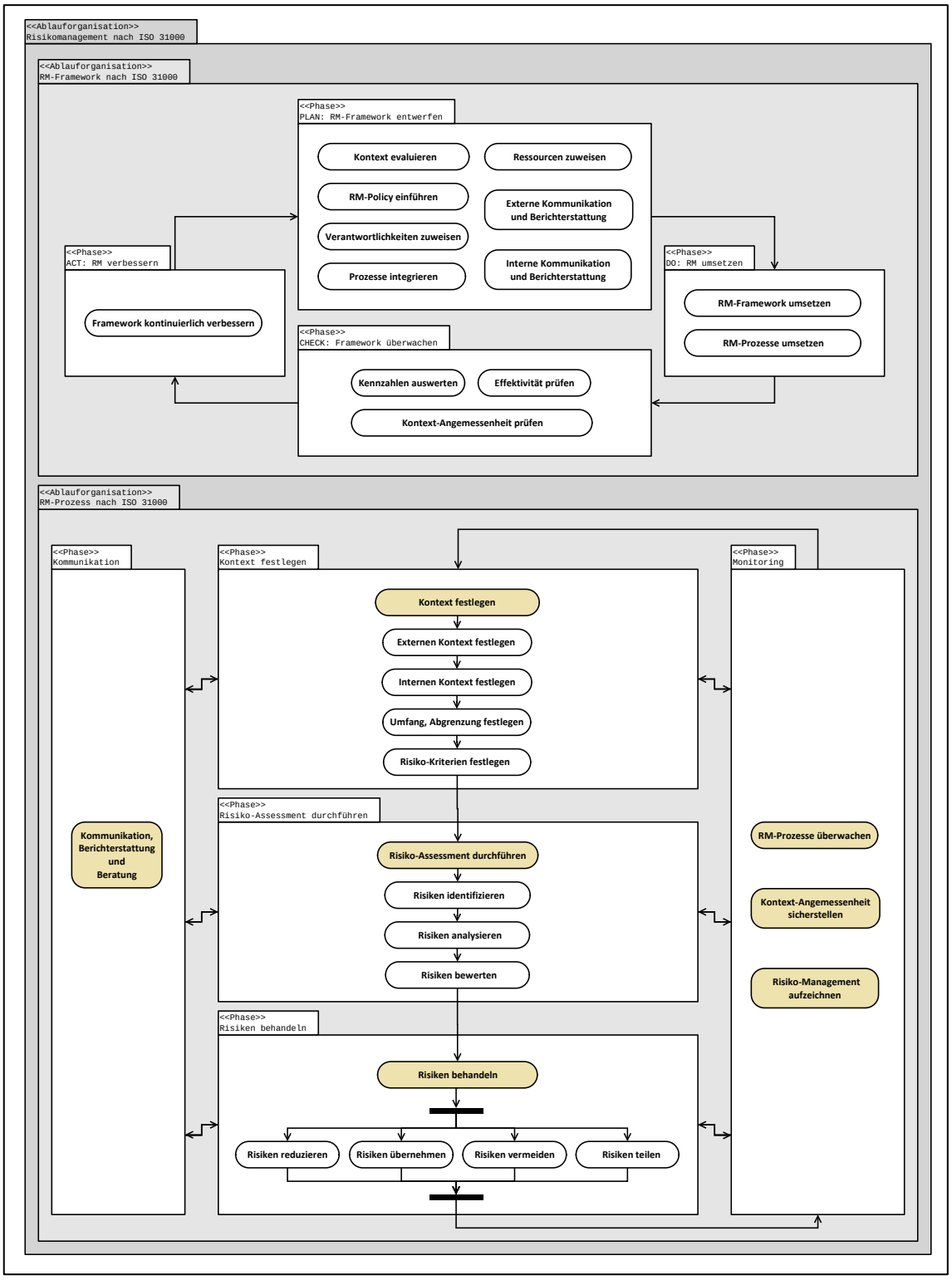

Abbildung 3.12: Risikomanagement-Framework und -Prozess nach ISO 31000[34]

[34] Quelle: Eigene Darstellung nach [15, S. vii]

3.2.5 COSO ERM – Integrated Framework

Das Good-Practice-Framework *COSO ERM* [9] (*Enterprise Risk Management*) bündelt die Vorstellungen und Erfahrungen von fünf US-amerikanischen Institutionen aus dem Bereich der Kontrolle des betrieblichen Finanzwesens und gilt als Standard-Referenzmodell für die Ausgestaltung von Internen Kontrollsystemen (IKS). [37]

Kurzbeschreibung COSO ERM	
Vollständige Bezeichnung	Enterprise Risk Management – Integrated Framework
Herkunft	Private Institution: The Committee of Sponsoring Organizations of the Treadway Commission (COSO, USA)
Erscheinungsjahr	Erste Version: 1992, letzte Überarbeitung 2004
Seitenzahl	246 (Framework und Application Techniques)
Ziel	Operativer Unternehmensbetrieb
Schwerpunkt	Risikomanagement
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.6: Kurzbeschreibung von COSO ERM[35]

Im Rahmen der 2004 fertiggestellten Erweiterung wurde der bisherige Titel *Internal Control – Integrated Framework* auf *Enterprise Risk Management – Integrated Framework* geändert, was die enge Beziehung von Risikomanagement und Internem Kontrollsystem verdeutlicht. Die aktuelle Publikation ist in die Beschreibung des Frameworks sowie die *Application Techniques* gegliedert, wobei letztere die Anwendung des Referenzmodells anhand von Beispielen näher erläutert.

Obwohl COSO ERM allgemein gehalten und nicht rein auf Informations- bzw. IT-Sicherheit fokussiert, ist der Detaillierungsgrad des Frameworks deutlich höher als beispielsweise bei ISO 31000, die ebenfalls auf Risikomanagement im allgemeinen Unternehmensbetrieb ausgerichtet ist.

Zwar ist die Strukturierung hier weniger stark ausgeprägt als etwa bei der Reihe ISO/IEC 2700x, jedoch zeigen sich im Rahmen einer objektorientierten Analyse relativ schnell durchgängig verwendete Klassen wie Prozesse und Aktivitäten, Werkzeuge, Rollendefinitionen und Dokumente, die vorgeschlagen werden, um die Zielsetzungen der acht Aspekte von ERM zu erreichen, die aus Abbildung 3.13 ersichtlich sind. Außerdem existieren verschiedene Klassifikationen für Unternehmensziele, Risiko-Behandlungsoptionen, Steuerungs- und Kontrollmaßnahmen (Controls) sowie Einflussfaktoren auf Ereignisse.

[35] Quelle: eigene Darstellung

Die Publikation erläutert zudem sinnhafte Bestandteile einer Dokumentation des ERM-Systems und beschreibt auch den Prozess zu dessen Einführung. Für die wichtigen Bereiche der *Ereignis-Identifikation* sowie für das *Risikoassessment* werden mögliche Werkzeuge zur Umsetzung genannt und zum Teil genauer beschrieben.

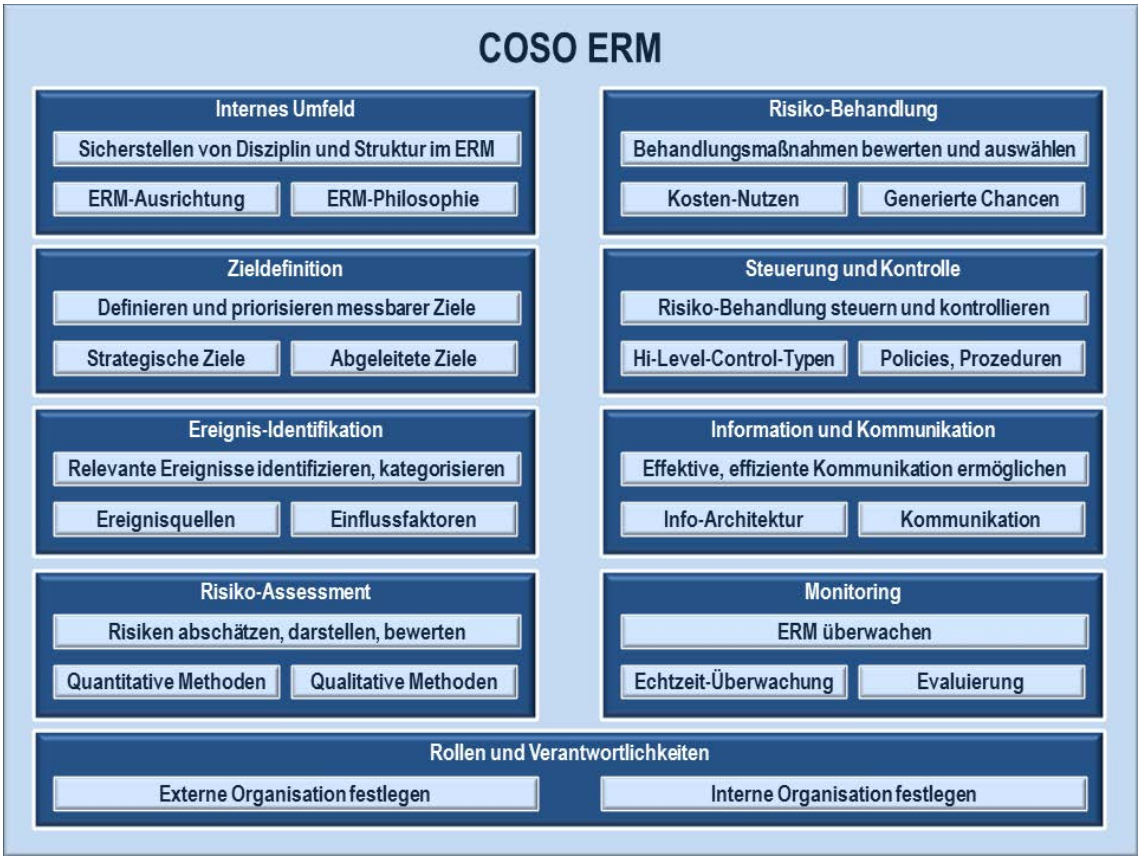

Abbildung 3.13: Inhalt und Struktur von COSO ERM (grobe Übersicht)[36]

Der große Einfluss von COSO ERM zeigt sich auch in der Tatsache, dass die Inhalte dieses Referenzmodells in die Entwicklung des weit verbreiteten IT-Governance-Frameworks COBIT einflossen und somit Kompatibilität zwischen diesen beiden Ansätzen herrscht, da COBIT die von COSO ERM geforderte Steuerung und Kontrolle im Bereich der IT umzusetzen hilft (vergleiche dazu beispielsweise [5, S. 8]).

[36] Quelle: Eigene Darstellung nach [9]

3.2.6 Risk IT

Unter der Bezeichnung *Risk IT* [17] veröffentlicht die *Information Systems Audit and Control Association (ISACA)* ein Good-Practice-Framework zum IT-Risikomanagement, das unter anderem in Zusammenarbeit mit der Unternehmensberatung *PricewaterhouseCoopers* entwickelt wurde.

Kurzbeschreibung Risk IT	
Vollständige Bezeichnung	The Risk IT Framework
Herkunft	Private Institution: Information Systems Audit and Control Association (ISACA, USA)
Erscheinungsjahr	2009
Seitenzahl	244 (Framework und Practitioner Guide)
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.7: Kurzbeschreibung von Risk IT[37]

Ähnlich wie bei COSO ERM existiert neben dem eigentlichen Framework ein durch Beispiele gestützter *Practitioner Guide* zu Risk IT, der dessen Anwendung detaillierter erklärt.

Das Risk IT Framework basiert auf einer prozessorientierten Architektur, die aus den Bereichen *Risiko-Governance*, *Risiko-Evaluierung* und *Risiko-Behandlung* aufgebaut wird und deren Strukturierung an jene von COBIT 4.1 angelehnt ist, das durch Risk IT erweitert wird.

Zwar definiert Risk IT eine große Zahl an Klassen, wie Prinzipien, Prozesse, Aktivitäten, Ziele, Metriken, Rollen- und Verantwortlichkeitsdefinition und ein Reifegradmodell, die auch durchgehend verwendet werden, jedoch findet im Vergleich zu anderen Ansätzen (allen voran der ISO/IEC 27005, COSO ERM, COBIT oder den BSI-Standards) eine Integration dieser Komponenten nur in sehr begrenztem Umfang statt, sodass deren Zusammenhänge weitgehend unklar bleiben.

Beispielsweise sind im Gegensatz zur ISO/IEC 27005 für die vorgestellten Prozesse keine unmittelbar verbundenen Kontrollflüsse bzw. Flowcharts verfügbar, die mögliche Reihenfolgebeziehungen klar festlegen. Stattdessen finden sich gerade im Bereich der Risikoanalyse sogar mehrere Ablaufmodelle in unterschiedlichen Darstellungen, für

[37] Quelle: eigene Darstellung

deren Integration die Fantasie des Lesers verantwortlich bleibt (vergleiche dazu z.B. [38, S. 32] und [38, S. 82]).

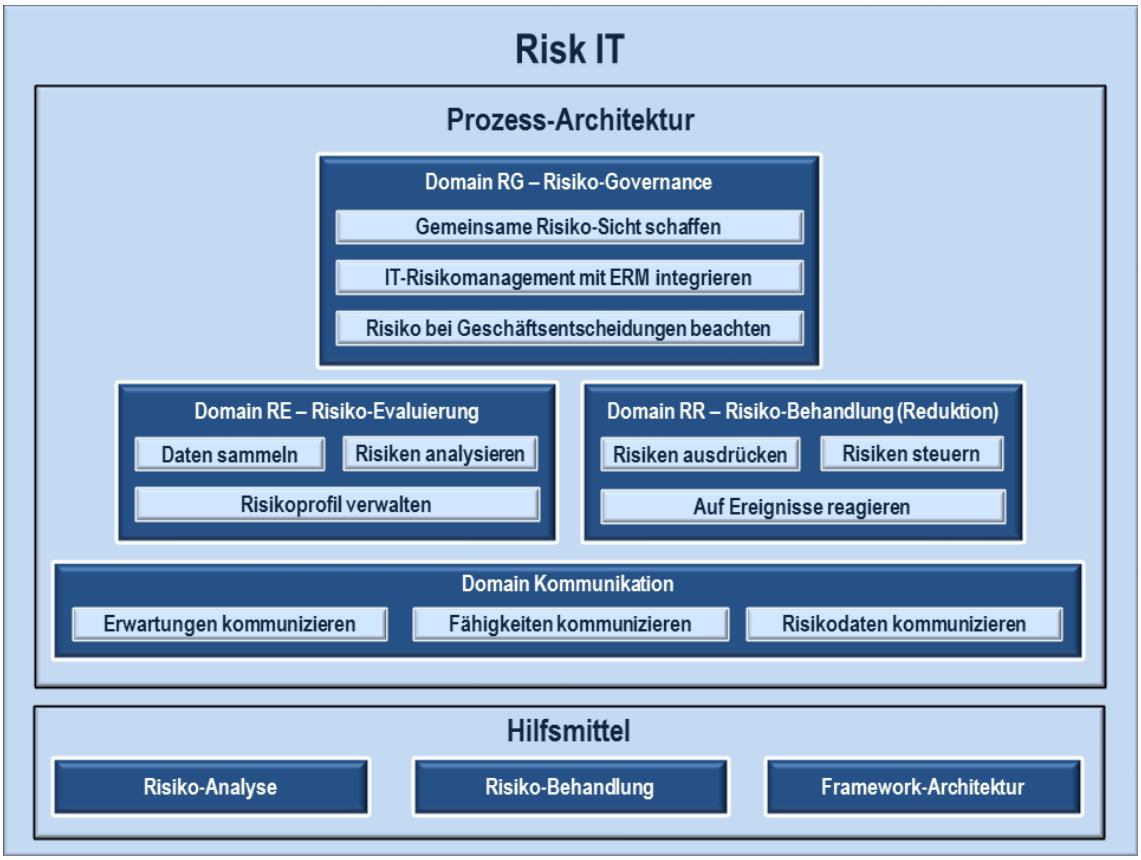

Abbildung 3.14: Inhalt und Struktur von Risk IT (grobe Übersicht)[38]

[38] Quelle: Eigene Darstellung nach [17]

3.2.7 Basel-II-Konglomerat – Basel II, KWG, SolvV, MaRisk

Die Rahmenvereinbarung des Baseler Ausschusses für Bankenaufsicht bezüglich der Eigenkapitalanforderungen im Finanzdienstleistungsbereich wurde erstmals im Jahr 1988 als *Baseler Akkord* (*Basel I*) veröffentlicht. Als Vorbeugung gegen Risiken enthielt diese Regelung ein fixes System an Risikogewichten, die auf die Forderungen der Bank anzuwenden waren, um die notwendige Eigenkapitalunterlegung zu errechnen. [39]

Die 2004 erschienene Überarbeitung des Baseler Akkords – *Basel II* genannt [2] – erweitert dieses Bewertungssystem, um der Forderung nach höherer Flexibilität bei der Berücksichtigung bestehender Risikomanagement-Ansätze nachzukommen. [39] Der Fokus von Basel II richtet sich dabei auf drei Hauptbereiche (*Säulen*), zu denen neben den Mindestkapitalanforderungen auch das bankaufsichtliche Überprüfungsverfahren sowie die Marktdisziplin zählen. [2, S. 7]

Bei der Berechnung der Mindestkapitalanforderungen stellt die Berücksichtigung der sogenannten *operationellen Risiken* eine wesentliche Neuerung dar, welche Risiken bezeichnen, die durch interne Verfahren, Menschen, Systeme oder externe Ereignisse hervorgerufen werden. [2, S. 157] Damit fließen erstmals Risiken in die Bewertung mit ein, die direkt mit dem Betrieb von Informationssystemen verbunden sind.

Da die Regelungen aus Basel II in der Europäischen Union von allen Banken verpflichtend umzusetzen sind, mussten diese in die jeweiligen nationalen Gesetzgebungen integriert werden, wobei aufgrund des hohen Strukturierungs- und Detaillierungsgrads die Umsetzung der Bundesrepublik Deutschland als Quelle für die vorliegende Arbeit herangezogen wurde.

Diese setzt sich aus dem *Kreditwesengesetz* (*KWG*, [40]), der *Solvabilitätsverordnung* (*SolvV*, [41]) sowie dem Rundschreiben *Mindestanforderungen an das Risikomanagement* (*MaRisk*, [27]) zusammen, die in Tabelle 3.8 kurz beschrieben werden.

Kurzbeschreibung Basel-II-Konglomerat	
Vollständige Bezeichnung	• Basel II – Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen – Überarbeitete Rahmenvereinbarung • KWG – Kreditwesengesetz • SolvV – Solvabilitätsverordnung • MaRisk – Rundschreiben 11/2010 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk
Herkunft	Öffentliche Institutionen, Gesetzgeber • Basel II – Baseler Ausschuss für Bankenaufsicht • KWG – Bundesrepublik Deutschland • SolvV – Bundesrepublik Deutschland • MaRisk – Bundesanstalt für Finanzdienstleistungsaufsicht

Kurzbeschreibung Basel-II-Konglomerat	
	(BaFin), Deutschland
Erscheinungsjahr	2004 – 2010
Seitenzahl	• Basel II – gesamt 284, relevanter Teil ~25 • KWG – gesamt ~160, relevanter Teil ~20 • SolvV – gesamt ~210, relevanter Teil ~30 • MaRisk ~ 25
Ziel	Sicherer Unternehmensbetrieb
Schwerpunkt	Risikomanagement
Art	Gesetz/Verpflichtende Regelung
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.8: Kurzbeschreibung des Basel-II-Konglomerats[39]

Wie aus Abbildung 3.15 ersichtlich, definiert das *Basel-II-Konglomerat* drei Ansätze zur Bewertung von Risiken mit steigender Komplexität, wodurch den unterschiedlichen Möglichkeiten von Banken Rechnung getragen wird, Risikomanagement zu betreiben. Dabei ist umso mehr Eigenkapital vorzuhalten, je ungenauer die eingesetzten Verfahren in der Lage sind, die Risikotragfähigkeit des Unternehmens zu steuern und zu beurteilen.

Insbesondere die MaRisk definiert hierbei detaillierte Anforderungen an die jeweiligen Prozesse zur Strategiefindung, zur Beurteilung, Behandlung, Überwachung und Berichterstattung in Bezug auf Risiken sowie zur Prüfung von Risikomanagement und Internem Kontrollsystem, und geht auch auf die Risikosteuerung im Zusammenhang mit Auslagerungen ein. Zudem werden die Dokumentation der Prozesse und Verfahren, sowie die Verwaltung von Ressourcen behandelt, wobei das Rundschreiben insbesondere das Management von Informationssystemen im Hinblick auf die Gewährleistung von Informationssicherheit berücksichtigt.

[39] Quelle: eigene Darstellung

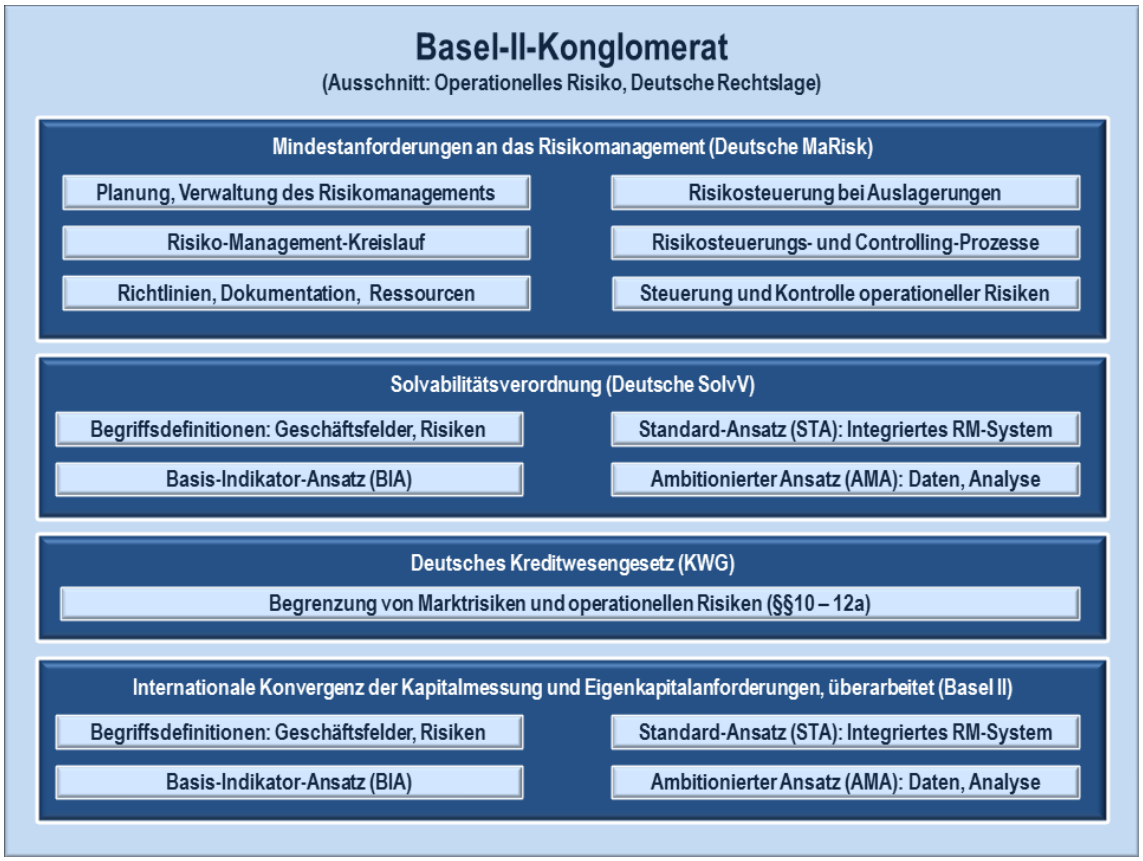

Abbildung 3.15: Inhalt und Struktur des Basel-II-Konglomerats (grobe Übersicht)[40]

Ende 2010 wurde mit *Basel III* eine Erweiterung der Baseler Regelungen vorgestellt, die angesichts der Wirtschafts- und Finanzkrise der vorangegangenen Jahre entwickelt wurde. [42] Zur Zeit der Verfassung dieser Arbeit ist allerdings die Zustimmung des EU-Ministerrats und des Europäische Parlaments noch ausständig, die eine Umsetzung des Rahmenwerks in der Europäischen Union ermöglichen würden. [43]

[40] Quelle: Eigene Darstellung nach [2], [40], [41], [27]

3.2.8 Sarbanes-Oxley Act

Der amerikanische *Sarbanes-Oxley Act* (*SOX*, [8]) wurde im Jahr 2002 als Reaktion auf eine Reihe von Bilanz- und Betrugsskandalen bei großen Unternehmen, wie dem Energieversorger *Enron* und dem Telekommunikationskonzern *WorldCom*, als Bundesgesetz der USA verabschiedet. Er gilt für alle Unternehmen – US-Amerikanisch wie international – die von der *United States Securities and Exchange Commission* (*SEC*, die amerikanische Börsenaufsichtsbehörde) beaufsichtigt werden, was bei einer Listung an der New Yorker Börse (*Wall Street*) der Fall ist. [6], [7]

Kurzbeschreibung Sarbanes-Oxley Act	
Vollständige Bezeichnung	Sarbanes-Oxley Act of 2002
Herkunft	Öffentliche Institution: Kongress der Vereinigten Staaten (USA)
Erscheinungsjahr	2002
Seitenzahl	Gesamt ~ 65, relevanter Teil ~ 2
Ziel	Sicherer Unternehmensbetrieb
Schwerpunkt	Steuerung und Kontrolle
Art	Gesetz/Verpflichtende Regelung
Detaillierungsgrad	Niedrig
Strukturierungsgrad	Niedrig

Tabelle 3.9: Kurzbeschreibung des Sarbanes-Oxley Act of 2002[41]

SOX stellt die umfangreichste Reform des Kapitalmarktrechts in den USA seit den dreißiger Jahren des vorigen Jahrhunderts dar und hat zum Ziel, durch eine Erweiterung der Finanzberichterstattungspflichten für Unternehmen das Vertrauen von Investoren zu stärken. Daraus ergeben sich zusätzliche Anforderungen in Bezug auf Risikomanagement und Internes Kontrollsystem sowie an deren Überprüfung im Rahmen von Audits, wobei für den Bereich des IT-Risikomanagements vor allem die beiden Abschnitte 302 und 404 hohe Bedeutung besitzen, deren Inhalte grob aus Abbildung 3.16 ersichtlich sind. [6], [7]

Als Grundlage für eine Umsetzung dieser Anforderungen können die meisten anderen verwendeten Ansätze der vorliegenden Arbeit herangezogen werden – in der Literatur werden in diesem Zusammenhang beispielsweise COSO ERM und COBIT erwähnt, die bei gemeinsamem Einsatz unmittelbar geeignet sind, die von SOX geforderten Systeme aufzubauen (siehe dazu z.B. die Publikation *IT Control Objectives for Sarbanes-Oxley* des *IT Governance Institute* [44]).

[41] Quelle: eigene Darstellung

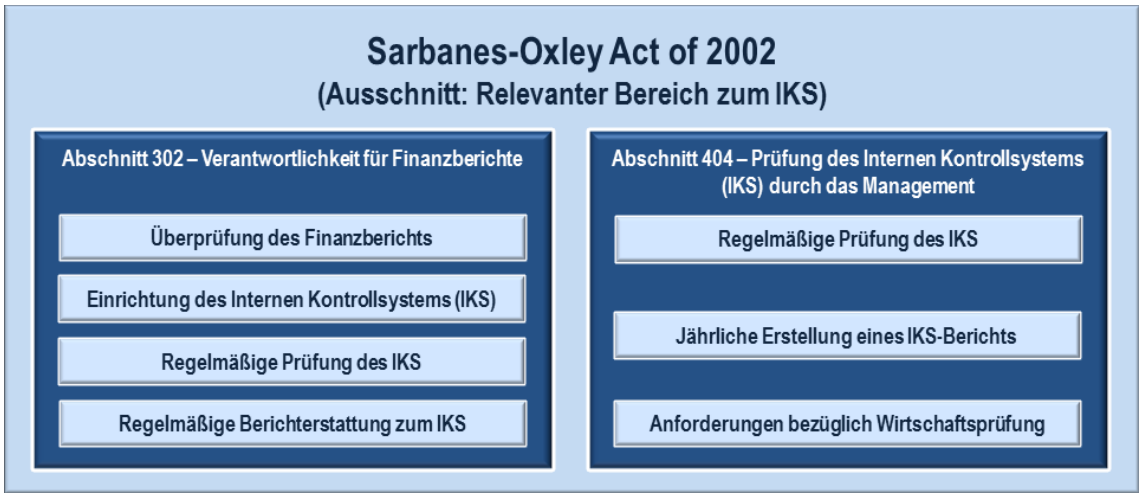

Abbildung 3.16: Inhalt und Struktur des SOX (grobe Übersicht)[42]

3.2.9 BSI-Standards und IT Grundschutz

Das seit 1991 bestehende deutsche *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*) entwickelt mit einer Reihe von Standards sowie den *IT-Grundschutzkatalogen* eine Sammlung an Leitlinien zur Informationssicherheit mit durchgehend hoher Komplexität.

Kurzbeschreibung BSI-Standards und IT-Grundschutzkataloge	
Vollständige Bezeichnung	• BSI-Standard 100-1: Managementsystem für Informationssicherheit (ISMS) • BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise • BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz • BSI-Standard 100-4: Notfallmanagement • IT-Grundschutzkataloge
Herkunft	Öffentliche Institution: Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland)
Erscheinungsjahr	Erste Version: 2005, letzte Überarbeitung der Standards 2008, laufende Überarbeitung der IT-Grundschutzkataloge
Seitenzahl	• BSI-Standard 100-1: 37 • BSI-Standard 100-2: 95 • BSI-Standard 100-3: 23 • BSI-Standard 100-4: 123 • IT-Grundschutzkataloge ~ 4.000
Ziel	Informationssicherheit

[42] Quelle: Eigene Darstellung nach [8]

Kurzbeschreibung BSI-Standards und IT-Grundschutzkataloge	
Schwerpunkt	Steuerung und Kontrolle
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.10: Kurzbeschreibung der BSI-Standards und IT-Grundschutzkataloge[43]

Das Konzept des *IT-Grundschutzes* [45] ist dabei von der Annahme getrieben, dass die meisten IT-Architekturen aus einer Zahl an sehr ähnlichen Bausteinen bestehen, die typischen Gefährdungen ausgesetzt sind und mit ähnlichen Maßnahmen abgesichert werden können. Dadurch könne ein gewisses Grundmaß an Informationssicherheit hergestellt werden, ohne detaillierte Prozesse zur Analyse von Risiken durchlaufen zu müssen.

Abbildung 3.17: Inhalt und Struktur der BSI-Dokumente (grobe Übersicht)[44]

[43] Quelle: eigene Darstellung
[44] Quelle: Eigene Darstellung nach [72], [73], [16], [13], [45]

Ein im Zuge der objektorientierten Analyse für diese Arbeit erstelltes UML-Aktivitätsdiagramm, das die Vorgehensweise nach BSI 100-1 bis 3 visualisiert, findet sich in Abbildung 3.18.

Nach Einschätzung des Autors schlagen die BSI-Standards und IT-Grundschutzkataloge in ihrer Gesamtheit jedoch ein System vor, das im Vergleich zu Ansätzen mit ähnlicher Zielsetzung (insbesondere der Reihe ISO/IEC 2700x sowie ITIL und COBIT) eine überaus hohe Komplexität bei geringem Spielraum für Anpassungen besitzt (siehe dazu bspw. auch [46]).

Diese Komplexität wird vor allem bei Betrachtung der beispielhaft angeführten Dokumentationsschemata offensichtlich, deren Aussagen bereits bei der wenig umfangreichen Beispielorganisation oft nur mühsam nachzuvollziehen sind, während auf die Notwendigkeit, die Verfahren und Systeme im praktischen Einsatz auf den Kontext der jeweiligen Organisation zuzuschneiden, nur in geringem Umfang eingegangen wird.

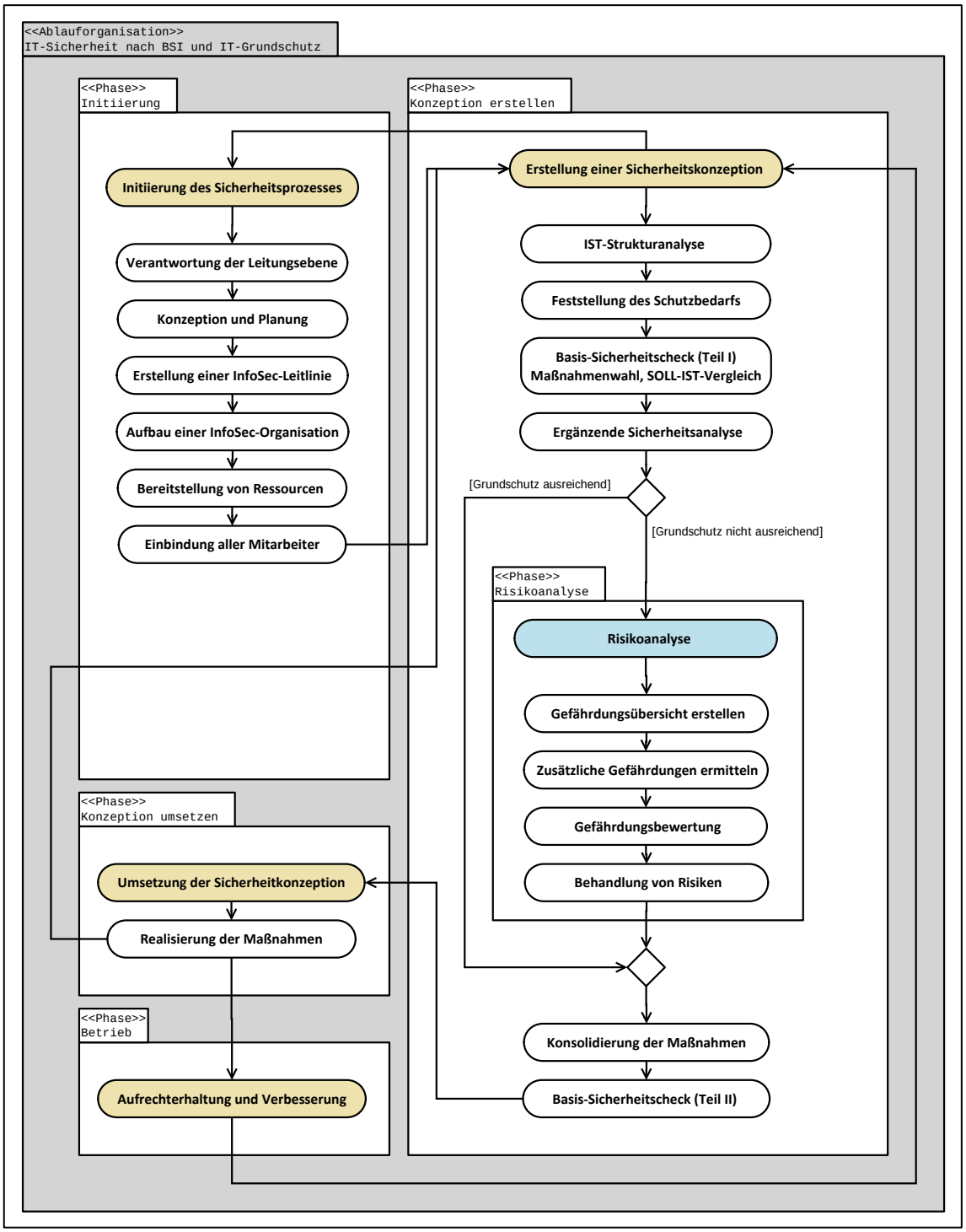

Abbildung 3.18: IT-Sicherheitsprozess nach BSI und IT-Grundschutz[45]

[45] Quelle: Eigene Darstellung nach [72], [73], [16], [13]

3.2.10 COBIT

Die *Control Objectives for Information and Related Technology* (*COBIT*) wurden seit Mitte der neunziger Jahre unter Federführung der US-amerikanischen *Information Systems Audit and Control Association* (*ISACA*) entwickelt. Nach den ersten beiden Veröffentlichungen gründete diese 1999 das *IT Governance Institute* (*ITGI*) – eine Non-Profit-Organisation, die seither die Entwicklung des Frameworks vorantreibt. Dieses liegt mittlerweile in der Version 4.1 vor, während sich die Version 5 zur Zeit der Erstellung dieser Arbeit nach wie vor in der Entwurfsphase befindet.

Kurzbeschreibung COBIT	
Vollständige Bezeichnung	Control Objectives for Information and Related Technology (COBIT 4.1)
Herkunft	Private Institution: IT Governance Institute (ITGI, USA)
Erscheinungsjahr	Erste Version: 1996, Veröffentlichung von Version 4.1: 2007
Seitenzahl	213
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.11: Kurzbeschreibung von COBIT 4.1[46]

In Anlehnung an COSO ERM gliedern sich die von COBIT 4.1 [5] vorgestellten Inhalte in vier *Kontrollbereiche* (Domains), die eine Gesamtzahl von 34 Prozessen mit jeweils klar definierten *Steuerungs- und Kontrollzielen* (den namensgebenden *Control Objectives*) und *Aktivitäten* beinhalten. Diese sollen den Einsatz von *Ressourcen* (Anwendungen, Information, Infrastruktur und Menschen) dahingehend optimieren, dass sieben *Geschäftsanforderungen* (auch: *Informationskriterien*) erfüllt werden, zu denen Effektivität, Wirtschaftlichkeit und Informationssicherheit zählen.

Zudem ist ein hierarchisches Modell an *Zielen* vorhanden, deren Erreichung anhand von *Metriken* gemessen wird, wobei Ziele „top down“ ausgehend von der Geschäftsebene gesetzt und durch IT-Aktivitäten und -Prozesse erfüllt werden. Für die Evaluierung der IT-Prozesse ist überdies ein fünfstufiges *Reifegradmodell* vorhanden, das sich an CMM/CMMI orientiert (siehe Abschnitt 3.2.12).

Abbildung 3.19 stellt die Bestandteile von COBIT 4.1 schematisch dar, während Abbildung 3.20 das zugehörige System aus Zielen und Metriken veranschaulicht.

[46] Quelle: eigene Darstellung

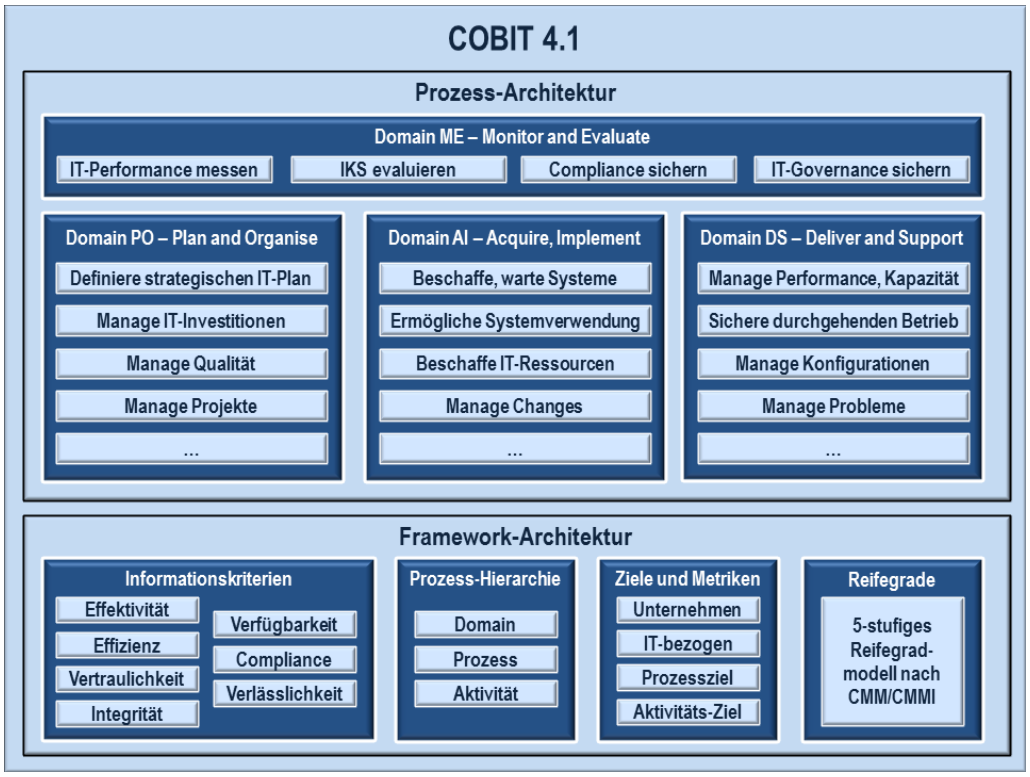

Abbildung 3.19: Inhalt und Struktur von COBIT 4.1 (grobe Übersicht)[47]

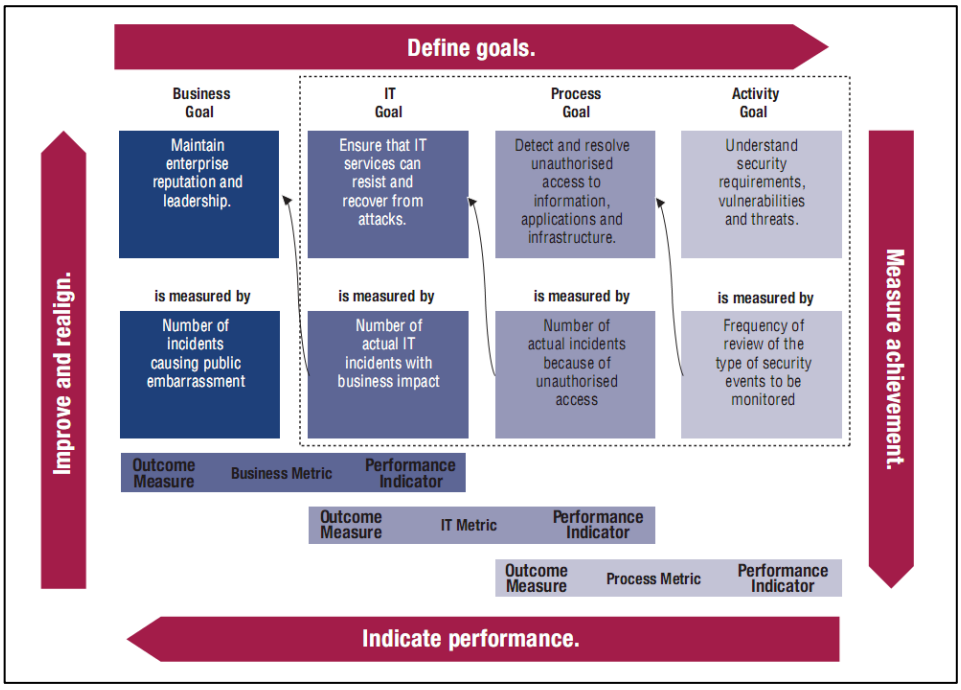

Abbildung 3.20: Ziele und Metriken nach COBIT 4.1 – IT follows business[48]

[47] Quelle: Eigene Darstellung nach [5], [21]
[48] Quelle: [5, S. 23]

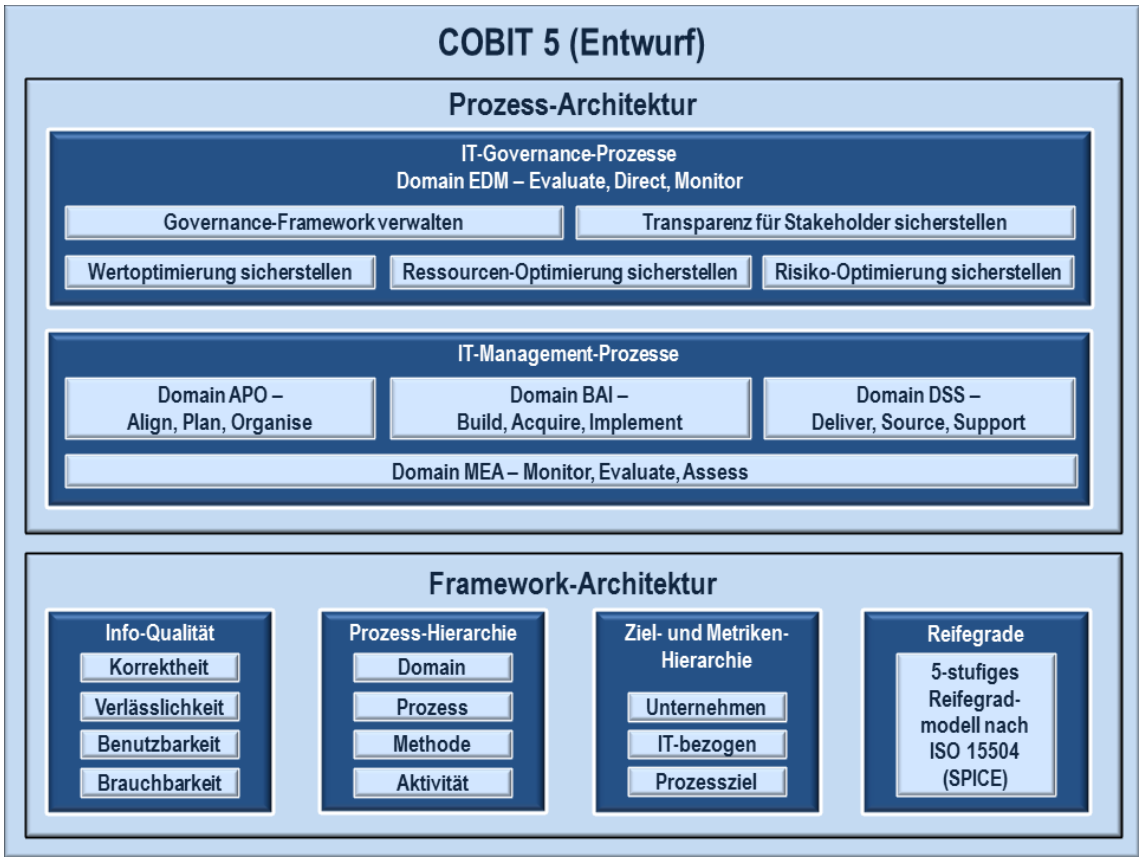

Abbildung 3.21: Inhalt und Struktur von COBIT 5 (grobe Übersicht)[49]

Für die vorliegende Arbeit wurde des Weiteren ein Entwurf zu COBIT 5 analysiert, das eine Reihe bedeutender Änderungen im Vergleich zu den bisherigen Versionen beinhalten soll (siehe Abbildung 3.21). Dazu zählt beispielsweise eine grundlegende Überarbeitung der Informationskriterien sowie des Reifegradmodells, das nun nach ISO/IEC 15504 organisiert ist.

Zudem soll künftig zwischen IT-Governance- und IT-Management-Prozessen unterschieden werden, was durch eine Anpassung der Domain-Architektur unterstützt wird. Schlussendlich enthält der analysierte Entwurf eine Erweiterung der bisherigen Hierarchie für Ziele und Metriken auf Basis eines komplexen *Governance-Enabler-Modells*, dessen Bestandteile anhand einer Reihe eigener Attribute beschrieben werden sollen. [22], [47], [48]

[49] Quelle: Eigene Darstellung nach [22], [47], [48]

3.2.11 ITIL

Die *IT Infrastructure Library* (*ITIL*), die seit den achtziger Jahren des vorigen Jahrhunderts von der britischen Regierungsbehörde *Office of Government Commerce (OGC)* entwickelt wird, ist mit einem Umfang von rund 1.400 Seiten in der aktuellen Version V3 nicht nur eine der umfassendsten Quellen dieser Arbeit, sondern stellt zurzeit einen der beliebtesten Standards zum IT Management dar.[50]

Kurzbeschreibung ITIl V3	
Vollständige Bezeichnung	IT Infrastructure Library (ITIL V3)
Herkunft	Öffentliche Institution: Office of Government Commerce (OGC, Großbritannien)
Erscheinungsjahr	Erste Version: 1989, V3: 2007, letzte Überarbeitung 2011[51]
Seitenzahl	~ 1.400 (5 Hauptpublikationen)
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Mittel

Tabelle 3.12: Kurzbeschreibung der ITIL V3[52]

ITIL nennt das sogenannte *IT Service Management* als zentrale Zielsetzung, wobei als *Service* nach ITIL alle Leistungen gelten, die der Werterbringung für den Kunden dienen, während die dabei entstehenden Kosten und Risiken direkt vom Dienstleister optimiert werden. [4, S. 5]

Die detaillierten Good-Practice-Prozesse aus den fünf Hauptpublikationen der ITIL V3 erlauben, IT-bezogene Dienstleistungen über ihren gesamten Lebenszyklus hinweg strukturiert zu planen, steuern und kontrollieren, was auch im Rahmen von Auslagerungen geschehen kann. Die in jenem Kreislauf ausgeführten Prozesse und Aktivitäten werden dazu in die drei Phasen *Service Design*, [49] *Service Operation* [50] sowie *Service Transition* [51] gegliedert, die nach *Service Strategy* [52] ausgerichtet werden und im Rahmen des *Continual Service Improvement* [53] kontinuierliche Verbesserungen erfahren. Jeder dieser in Abbildung 3.22 schematisch dargestellten Phasen wird in ITIL V3 eine eigene Publikation gewidmet, deren Inhalte aus Abbildung 3.23 grob ersichtlich sind.

[50] Siehe dazu z.B. die Studie des ITGI aus dem Jahre 2011 [24], wonach ITIL bzw. ISO/IEC 20000 bei 28% der über 800 befragten Unternehmen eingesetzt werden und damit die am weitesten verbreiteten Frameworks und Standards zum IT Management darstellen
[51] Als Grundlage für die vorliegende Arbeit dient die Version von 2007
[52] Quelle: eigene Darstellung

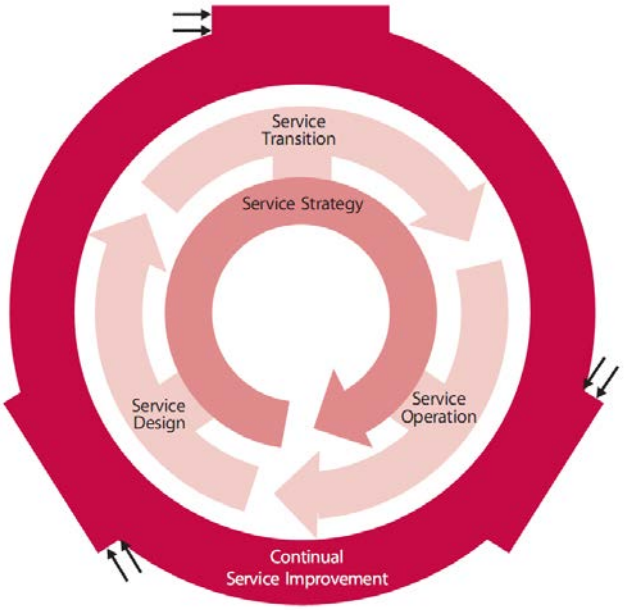

Abbildung 3.22: Der Service-Lebenszyklus nach ITIL V3[53]

Abbildung 3.23: Inhalt und Struktur der ITIL V3 (grobe Übersicht)[54]

[53] Quelle: [4, S. 19]
[54] Quelle: Eigene Darstellung nach [52], [49], [51], [50], [53]

Die Beziehung zwischen ITIL und COBIT

Vergleicht man die Bestandteile von ITIL V3 mit den Kontrollbereichen (Domains) und Prozessen von COBIT 4.1, wird schnell eine weitgehende thematische Übereinstimmung offensichtlich. Eine Analyse der Inhalte zeigt jedoch, dass COBIT eine eher in sich geschlossene, durchgängige und homogene Strukturierung aufweist, während ITIL weit detaillierte Beschreibungen beinhaltet.

Zudem wird COBIT in der zu diesem Themenbereich verfügbaren Literatur eine deutlich stärkere strategische Ausrichtung bescheinigt, wohingegen ITIL eher den Betrieb der IT-Infrastruktur in den Vordergrund stellt. [54] Diese Divergenz kann auch durch einen Vergleich der Begriffe IT Governance und IT Service Management veranschaulicht werden.

Damit liegt es nahe, die beiden Frameworks ergänzend zu verwenden, indem COBIT vorgibt, *was* zu tun ist, während ITIL erklärt, *wie* die nötigen Maßnahmen umgesetzt werden können. Eine Reihe von Initiativen widmet sich einer derartigen Abstimmung, woraus unter anderem ein Mapping von ITGI und OGC entstanden ist. [36] Wie bereits in Abschnitt 3.2.2 zur Norm ISO/IEC 27002 beschrieben, bildet dieses Dokument die Grundlage des entsprechenden Harmonisierungsversuchs in der vorliegenden Arbeit.

ISO/IEC 20000

Aufgrund der fehlenden Zertifizierungsmöglichkeit für Unternehmen nach ITIL wurde vom *IT Service Management Forum (itSMF)* und der britischen Standardisierungsbehörde (*British Standards Institution, BSI*) eine Norm zum IT Service Management entwickelt, die mittlerweile als internationaler Standard *ISO/IEC 20000* vorliegt. [55] Dieser definiert in drei Teilen Anforderungen an die entsprechenden Prozesse, die bei der Erstellung der ITIL V3 explizit berücksichtigt wurden. Eine Implementierung von ITIL kann somit als Grundlage für eine Zertifizierung nach ISO/IEC 20000 dienen, wird vom Standard jedoch nicht zwingend vorgeschrieben.

3.2.12 Weitere Ansätze

Im Folgenden wird eine Reihe weiterer Ansätze vorgestellt, die zwar ebenfalls dem Risikomanagement und angrenzenden Themenbereichen entstammen, jedoch nicht als Primärquellen für die vorliegende Arbeit dienen. Zum Teil – wie beispielsweise im Fall der Reifegradmodelle von CMM/CMMI und ISO/IEC 15504 – werden diese allerdings aus Primärquellen unmittelbar referenziert; die restlichen Ansätze wurden in diesen Abschnitt aufgenommen, um den Überblick über bekannte Standards und Rahmenwerke zum Risikomanagement zu komplettieren und deren große Zahl neuerlich zu unterstreichen.

CRAMM

Die britische *Central Computer and Telecommunications Agency (CCTA),* die mittlerweile in das *Office of Government Commerce (OGC)* integriert wurde, entwickelte in ihrer Rolle als IT-Provider für Regierungsinstitutionen nicht nur die IT Infrastructure Library (ITIL), sondern auch die Risikoanalyse- und Risikomanagement-Methode *CRAMM*. Der Standard, der mittlerweile vom Unternehmen *Siemens* verwaltet wird, liegt aktuell in Version 5 vor, und findet unter anderem im Verteidigungsbereich Verwendung. [56]

Kurzbeschreibung CRAMM	
Vollständige Bezeichnung	CCTA Risk Analysis and Management Method
Herkunft	Öffentliche Institution: Central Computing and Telecommunications Agenca (CCTA, Großbritannien; heute von Siemens verwaltet)
Erscheinungsjahr	Erste Version: 1985
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.13: Kurzbeschreibung von CRAMM[55]

Wie aus Abbildung 3.24 ersichtlich, schlägt CRAMM eine ähnliche Vorgehensweise wie andere Standards vor, die nach einer Analyse von Assets, Schwachstellen und Bedrohungen Gegenmaßnahmen auswählt, implementiert und überwacht.

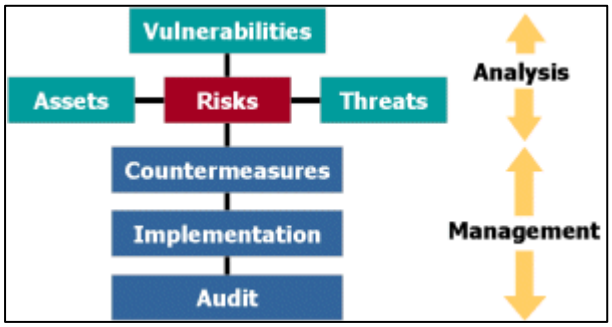

Abbildung 3.24: Aufbau von CRAMM 5[56]

[55] Quelle: eigene Darstellung
[56] Quelle: [56]

CMM/CMMI

Das Referenzmodell *Capability Maturity Model Integration* (*CMMI*) stellt einen Ansatz zur Prozessverbesserung für die Entwicklung und die Beschaffung, sowie für die Erbringung von IT-bezogenen Dienstleistungen dar. Es geht auf das *Capability Maturity Model* (*CMM*) zurück, das infolge eines Auftrags des US-amerikanischen Verteidigungsministeriums entwickelt wurde, um die Qualität von IT-Prozessen beurteilen zu können, und enthält zu diesem Zweck unter anderem fünfstufiges Reifegradmodell, das in adaptierter Form beispielsweise von COBIT 4.1 verwendet wird. [57], [58]

Kurzbeschreibung CMM/CMMI	
Vollständige Bezeichnung	Capability Maturity Model / Integration
Herkunft	Öffentliche Institution: Software Engineering Institute (SEI) der Carnegie Mellon Universität, Pittsburgh, USA
Erscheinungsjahr	CMM: 1991, CMMI: 2000
Ziel	Sicherer Unternehmensbetrieb
Schwerpunkt	Qualitätsmanagement/Reifegrade
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.14: Kurzbeschreibung von CMM/CMMI[57]

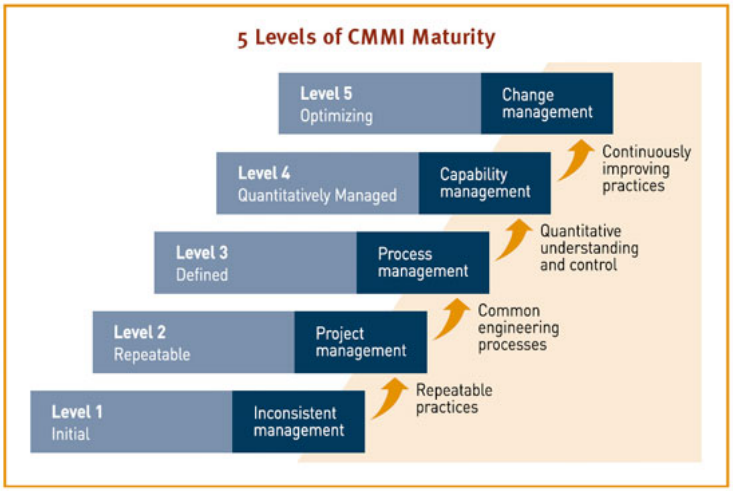

Abbildung 3.25: Reifegradmodell nach CMMI[58]

[57] Quelle: eigene Darstellung
[58] Quelle: [58]

ISO/IEC 15504 (SPICE)

Ähnlich wie CMM/CMMI stellt auch die *Software Process Improvement and Capability Determination* (*SPICE*) im Rahmen des nicht weniger als zehnteiligen internationalen Standards *ISO/IEC 15504* eine Reihe von Werkzeugen zur Prozessverbesserung und Qualitätsanalyse bereit. [59] Diese werden unter anderem im aktuellen Entwurf zum IT Governance Framework COBIT 5 referenziert.

Kurzbeschreibung ISO/IEC 15504	
Vollständige Bezeichnung	ISO/IEC 15504 – Information technology – Process assessment (Parts 1 – 10) *oder* Software Process Improvement and Capability Determination (SPICE)
Herkunft	Standardisierungsgremium: International Organization for Standardization, International Electrotechnical Commission (ISO/IEC, Schweiz)
Erscheinungsjahr	2003 – 2011
Ziel	Informationssicherheit
Schwerpunkt	Qualitätsmanagement/Reifegrade
Art	Internationaler Standard (nicht zertifizierbar)
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.15: Kurzbeschreibung ISO/IEC 15504[59]

HIPAA

Der US-amerikanische *Health Insurance Portability and Accountability Act* (*HIPAA*) stellt im Abschnitt zur Vorbeugung gegen Betrug und Missbrauch im Gesundheitssystem unter anderem Anforderungen an den Schutz vertraulicher Daten (*Privacy Rule*) und definiert mögliche Transaktionen per *Electronic Data Interchange* (*EDI, Transaction and Code Sets Rule*) sowie administrative, physische und technische Sicherheitsmaßnahmen (*Security Rule*). [60]

[59] Quelle: eigene Darstellung

Kurzbeschreibung HIPAA	
Vollständige Bezeichnung	Health Insurance Portability and Accountability Act of 1996
Herkunft	Öffentliche Institution: Kongress der Vereinigten Staaten, USA
Erscheinungsjahr	1996
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Gesetz/Verpflichtende Regelung
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.16: Kurzbeschreibung des HIPAA[60]

SAS 70

Der aus den USA stammende Audit-Standard *SAS 70* [61] dient als Grundlage für eine Überprüfung des Internen Kontrollsystems (IKS) von IT-Dienstleistern. Dabei sind zwei Typen von Audits vorgesehen, im Rahmen derer das Design und bei der umfassenderen Typ-II-Prüfung auch die operationelle Effektivität des IKS über einen festgelegten Zeitraum hinweg beurteilt werden. SAS 70 kann somit verwendet werden, um einer auslagernden Organisation die korrekte Funktion interner Kontrollen beim Dienstleister zu versichern.

Kurzbeschreibung SAS 70	
Vollständige Bezeichnung	Statement on Auditing Standards 70 – Reports on the Processing of Transactions by Service Organizations (SAS 70)
Herkunft	Öffentliche Institution: American Institute of Certified Public Accountants (AICPA, USA)
Erscheinungsjahr	1992
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Nationaler Standard ohne Zertifizierungsmöglichkeit
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.17: Kurzbeschreibung SAS 70[61]

[60] Quelle: eigene Darstellung
[61] Quelle: eigene Darstellung

IDW PS 951

Der *Prüfungsstandard 951* des *Instituts der Wirtschaftsprüfer in Deutschland* [62] definiert Anforderungen an die Prüfung des Internen Kontrollsystems bei IT-Dienstleistungsunternehmen und entspricht damit dem amerikanischen SAS 70, auf dessen beiden Audit-Typen auch die Bescheinigungen *A* und *B* des IDW PS 951 basieren.

Kurzbeschreibung IDW PS 951	
Vollständige Bezeichnung	IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen (IDW PS 951)
Herkunft	Öffentliche Institution: Institut der Wirtschaftsprüfer in Deutschland e.V.
Erscheinungsjahr	2007
Ziel	Sicherer Unternehmensbetrieb
Schwerpunkt	Steuerung und Kontrolle
Art	Nationaler Standard ohne Zertifizierungsmöglichkeit
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.18: Kurzbeschreibung des IDW PS 951[62]

ISO/IEC 16085

Die 2006 zuletzt überarbeitete Norm *ISO/IEC 16085* [63] definiert einen Risikomanagement-Prozess, der in den Lebenszyklus von Software und Systemen eingebettet wird und in Zusammenarbeit mit dem *Institute of Electrical and Electronics Engineers (IEEE)* entwickelt wurde.

[62] Quelle: eigene Darstellung

Kurzbeschreibung ISO/IEC 16085	
Vollständige Bezeichnung	ISO/IEC 16085:2006 – Systems and software engineering – Life cycle processes – Risk management
Herkunft	Standardisierungsgremium: International Organization for Standardization, International Electrotechnical Commission (ISO/IEC, Schweiz)
Erscheinungsjahr	Erste Version: 2004
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Internationaler Standard (nicht zertifizierbar)
Detaillierungsgrad	Mittel
Strukturierungsgrad	Mittel

Tabelle 3.19: Kurzbeschreibung der ISO/IEC 16085[63]

NIST SP 800-30

Der Risikomanagement-Standard des *National Institute of Standards and Technology (NIST)* der USA [64] beschreibt ein hoch strukturiertes Vorgehensmodell zur Steuerung und Kontrolle von Risiken von IT-Systemen und integriert dessen Phasen ebenso wie ISO/IEC 16085 mit dem Lebenszyklus von Software und Systemen.

Die neun Prozessschritte nach *SP 800-30* entsprechen dabei überwiegend jenen aus den Primärquellen dieser Arbeit und werden durch eine Vorstellung der jeweiligen In- und Outputs sowie anwendbarer Werkzeuge komplettiert.

Kurzbeschreibung NIST SP 800-30	
Vollständige Bezeichnung	Risk Management Guide for Information Technology Systems
Herkunft	Öffentliche Institution: National Institute of Standards and Technology (NIST, USA)
Erscheinungsjahr	2002
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Mittel
Strukturierungsgrad	Hoch

Tabelle 3.20: Kurzbeschreibung der NIST SP 800-30[64]

[63] Quelle: eigene Darstellung

OECD Guidelines

Die *OECD Guidelines for the Security of Information Systems and Networks* definieren auf lediglich 15 Seiten eine Menge an Prinzipien, um die Sicherheit von Informationssystemen und Netzwerken sicherzustellen. Dazu zählen grob beschriebene Anforderungen wie Achtsamkeit und Gewahrsein (Awareness) ebenso wie Risikoanalysen, der Entwurf und die Implementierung von Sicherheitsmaßnahmen sowie kontinuierliche *Re-Assessments*. Auffallend ist hierbei die Tatsache, dass trotz der grundlegenden Vereinbarkeit dieser Prinzipien mit anderen Standards kaum auf die grundlegende Frage eingegangen wird, warum Informationssysteme überhaupt einer Absicherung bedürfen, da keine Verbindung zur Geschäftsebene hergestellt wird. [65]

Kurzbeschreibung OECD Guidelines	
Vollständige Bezeichnung	OECD Guidelines for the Security of Information Systems and Networks
Herkunft	Öffentliche Institution: Organisation for Economic Co-operation and Development (OECD)
Erscheinungsjahr	2002
Ziel	IT-Sicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Niedrig
Strukturierungsgrad	Niedrig

Tabelle 3.21: Kurzbeschreibung der OECD Guidelines[65]

OCTAVE

Die *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (*OCTAVE*) [66] stellt eine umfangreiche prozessorientierte Methodik zum Risikomanagement vor, das auf vier Phasen mit insgesamt acht Prozessen basiert. Ähnlich wie beim IT-Grundschutz des deutschen BSI stellt das Referenzmodell eine Reihe von Katalogen zur Verfügung, die typische Bedrohungsprofile und Schwachstellen enthalten.

Bereits in der Vorbereitungsphase geht OCTAVE zudem auf die Abstimmung mit anderen Standards ein, die vor Implementierung der Methodik vonnöten sein kann, und weist auch darauf hin, dass OCTAVE selbst auf den jeweiligen Kontext anzupassen ist.

[64] Quelle: eigene Darstellung
[65] Quelle: eigene Darstellung

Kurzbeschreibung OCTAVE	
Vollständige Bezeichnung	Operationally Critical Threat, Asset, and Vulnerability Evaluation
Herkunft	Öffentliche Institution: Computer Emergency Response Team (CERT), Software Engineering Institute (SEI) der Carnegie Mellon Universität, Pittsburgh, USA
Erscheinungsjahr	Erste Version: 1999
Ziel	Informationssicherheit
Schwerpunkt	Risikomanagement
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Hoch
Strukturierungsgrad	Hoch

Tabelle 3.22: Kurzbeschreibung von OCTAVE[66]

PCI DSS

Der *Datensicherheitsstandard* der *Payment Card Industry* (*PCI*) [67] verfolgt die Zielsetzung, durch eine weltweite Vereinheitlichung von Sicherheitsmaßnahmen die Datensicherheit von Karteninhabern zu verbessern und gilt für alle Institutionen, die an der Verarbeitung derartiger Daten beteiligt sind.

Zur Minimierung der damit verbundenen Risiken werden in der Version 2.0 zwölf Anforderungen vorgegeben, die unter anderem die Erstellung und Wartung eines sicheren Netzwerks, die Implementierung von Maßnahmen zur Zugriffskontrolle sowie die Befolgung einer Informationssicherheits-Richtlinie (Security Policy) enthalten.

Kurzbeschreibung PCI DSS	
Vollständige Bezeichnung	Payment Card Industry (PCI) Datensicherheitsstandard (DSS) – Anforderungen und Sicherheitsbeurteilungsverfahren
Herkunft	Private Institution: PCI Security Standards Council
Erscheinungsjahr	Erste Version: 2008
Ziel	Informationssicherheit
Schwerpunkt	Steuerung und Kontrolle
Art	Good-Practice-Framework/Referenzmodell
Detaillierungsgrad	Niedrig
Strukturierungsgrad	Mittel

Tabelle 3.23: Kurzbeschreibung von PCI DSS[67]

[66] Quelle: eigene Darstellung

3.3 Grobstrukturierung

Wie bereits zuvor beschrieben, ergibt sich durch die große Vielfalt der im vorigen Abschnitt vorgestellten Ansätze der dringende Bedarf, diese anhand einer Reihe von Kriterien genauer einzuordnen. Die Tabellen zur Kurzbeschreibung bilden nach Meinung des Autors dazu eine geeignete Grundlage, sodass deren Attribute für den Vergleich in der folgenden Tabelle 3.24 herangezogen wurden.

Kurzvergleich der betrachteten Ansätze

Attribut	ISO 27001	ISO 27002	ISO 27005	ISO 31000	COSO ERM	Risk IT	Basel II	SOX	BSI	ITIL	COBIT	CRAMM	CMMI	ISO 15504 (Spice)	HIPAA	IDW PS 951	SAS 70	ISO 16085	NIST SP800-30	OECD Guidelines	OCTAVE	PCI DSS
Herkunft	SG	SG	SG	SG	PR	PR	PU	PU	PU	PU	PR	PU	PU	SG	PU	PU	PU	SG	PU	PU	PU	PR
Ziel	IS	IS	IS	SB	SB	IS	SB	SB	IS	IS	IS	IS	SB	IS	IS	SB	IS	IS	IS	IT	IS	IS
Schwerpunkt	RM	SK	RM	RM	RM	RM	RM	SK	SK	SK	SK	RM	QM	QM	SK	SK	SK	RM	RM	SK	RM	SK
Art	N2	N1	N1	N1	GP	GP	RE	RE	GP	GP	GP	GP	GP	N1	RE	N1	N1	N1	GP	GP	GP	GP
Detaillierungsgrad	2	2	2	1	2	2	2	1	3	3	3	3	3	3	2	2	2	2	2	1	3	1
Strukturierungsgrad	3	3	3	2	2	2	2	1	3	2	3	3	3	3	2	2	2	2	3	1	3	2
Alter	3	2	1	1	3	1	1	2	1	3	2	3	2	1	2	1	3	2	2	2	2	1

Attribut	Mögliche Ausprägungen					
Herkunft	SG	Standardisierungsgremium	PR	Private Institution	PU	Öffentliche Institution, Gesetzgeber
Ziel	IT	IT-Sicherheit	IS	Informationssicherheit	SB	Sicherer Unternehmensbetrieb
Schwerpunkt	RM	Risikomanagement	QM	Qualitätsmanagement/Reifegrade	SK	Steuerung und Kontrolle
Art	N1/2	Norm	GP	Good-Practice Framework/Referenzmodell	RE	Gesetz/Verpflichtende Regelung
Detaillierungsgrad	1	niedrig	2	mittel	3	hoch
Strukturierungsgrad	1	niedrig	2	mittel	3	hoch
Alter	1	neu (ab 2005)	2	mittel (1995 < Alter < 2005)	3	alt (bis 1995)

Tabelle 3.24: Kurzvergleich der betrachteten Ansätze[68]

[67] Quelle: eigene Darstellung
[68] Quelle: eigene Darstellung

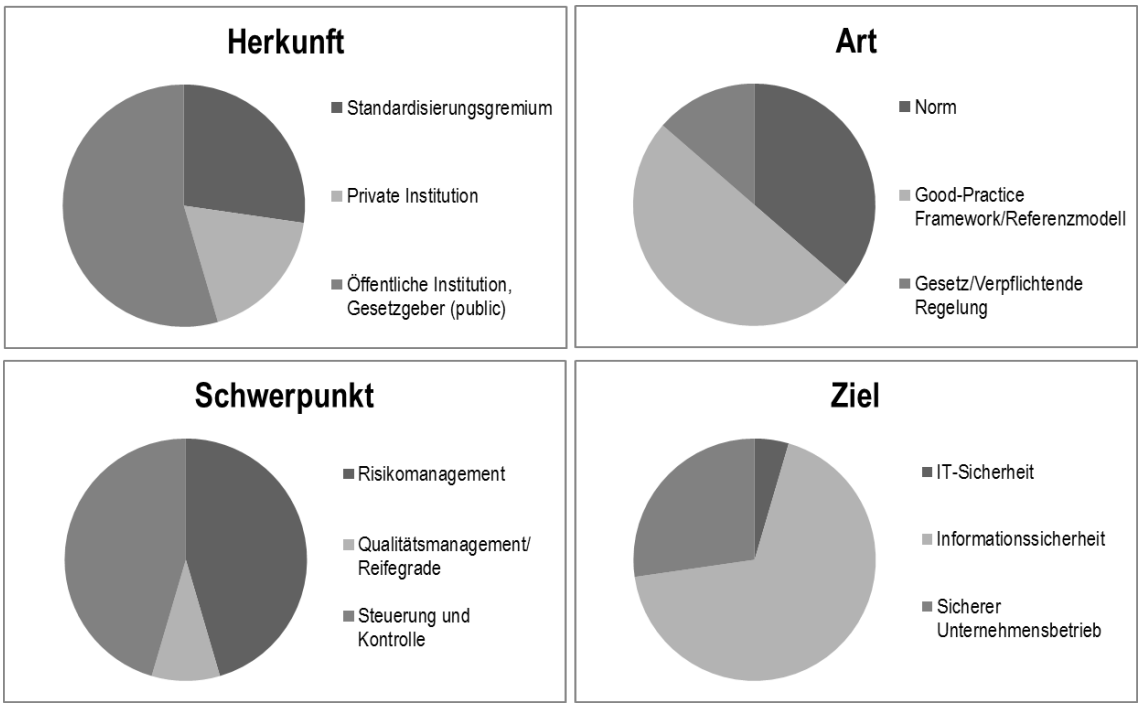

Abbildung 3.26: Kurzvergleich der betrachteten Ansätze: Auswertung [69]

Die aus den Daten des tabellarischen Vergleichs erstellten Kreisdiagramme aus Abbildung 3.26 zeigen, dass eine deutliche Mehrheit der Ansätze unter der Federführung öffentlicher Institutionen sowie Standardisierungsgremien erstellt wurde, während private Institutionen bei der Ausarbeitung von Risikomanagement-Standards eine untergeordnete Rolle zu spielen scheinen.

Genau die Hälfte der Ansätze besitzt des Weiteren den Charakter von sogenannten *Good-Practice-Frameworks*, während auch eine beträchtliche Zahl an Normen existiert. Gesetze und verpflichtende Regelungen sind in der vorliegenden Arbeit primär im Rahmen des Basel-II-Konglomerats und SOX vertreten.

Die Schwerpunkte der Ansätze sind zwischen dem Bereich des Risikomanagements sowie der Maßnahmen zur Steuerung und Kontrolle in gleicher Zahl aufgeteilt, wohingegen nur die Reifegradmodelle aus CMM/CMMI und ISO/IEC 16085 (SPICE) als Standards zum Qualitätsmanagement betrachtet wurden.

Abschließend ist erkennbar, dass die überwiegende Mehrheit der eingeflossenen Ansätze Informationssicherheit als Zielsetzung verfolgt, was sich direkt aus der Themenstellung der vorliegenden Arbeit ergibt. Einige Ansätze (wie COSO ERM) abstrahieren von der Ebene der Informationssysteme und richten ihre Aufmerksamkeit stattdessen auf den sicheren Unternehmensbetrieb an sich, während lediglich die OECD Guidelines ihren Fokus explizit nur auf die Sicherheit von IT-Systemen und Netzwerken legen.

[69] Quelle: eigene Darstellung

Eine weitere Möglichkeit zur Einordnung der betrachteten Ansätze stellt ein Vergleich deren Erscheinungsdaten dar, die durch die Zeitreihe in Abbildung 3.27 visualisiert werden.

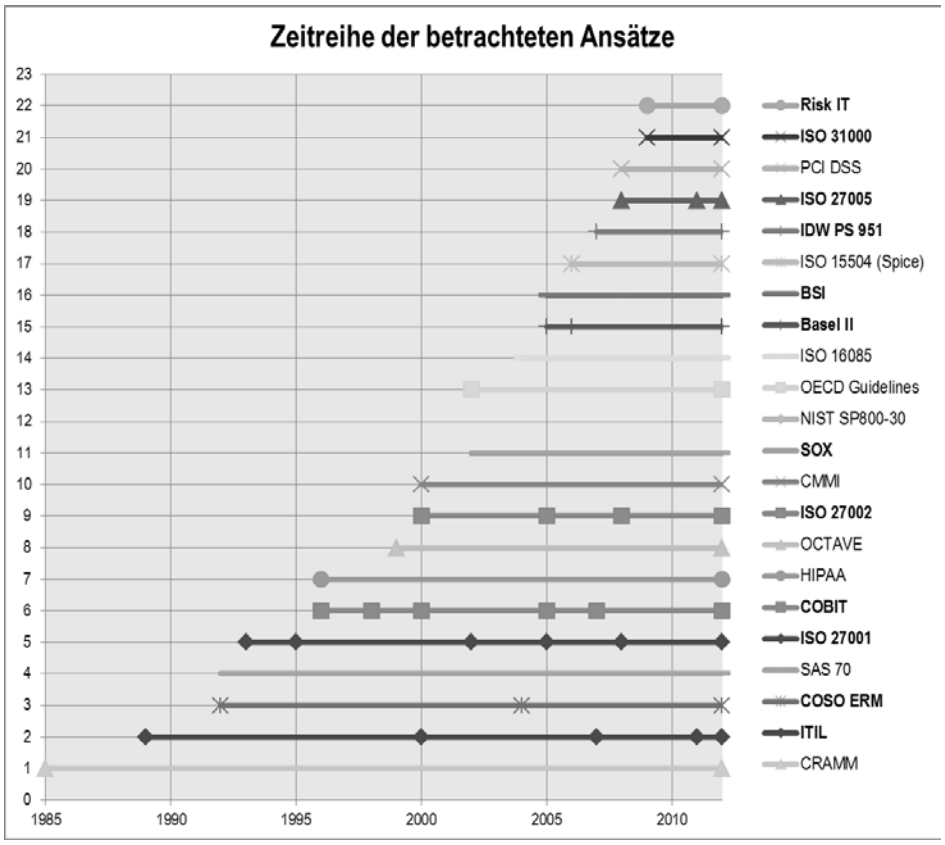

Abbildung 3.27: Zeitreihe der betrachteten Ansätze[70]

Die Jahreszahlen stellen dabei das Erscheinungsjahr der jeweiligen Erstversion dar; die im Detail analysierten Ansätze sind in der Legende zudem fett gedruckt und zeigen auch die Erscheinungsdaten neuerer Versionen als zusätzliche Datenpunkte.

Es zeigt sich, dass vor allem die Ansätze ITIL, COSO ERM, ISO 27001 und COBIT bereits eine längere Entwicklung durchlaufen haben, während SOX, das Basel-II-Konglomerat und die BSI-Standards zeitlich gesehen dem Mittelfeld zuzurechnen sind. Insbesondere die ISO/IEC 27005, die ISO 31000 sowie Risk IT zählen zu den neuesten Primärquellen der vorliegenden Arbeit.[71]

[70] Quelle: eigene Darstellung

[71] Vor allem der ISO 31000 und Risk IT wurden im vorigen Abschnitt gravierende Mängel attestiert, die möglicherweise aus deren noch nicht erfolgten Überarbeitungen resultieren; der ISO/IEC 27005 wurde hingegen ein ansprechender Detaillierungs- und Strukturierungsgrad zugesprochen – diese Attraktivität könnte darin begründet liegen, dass für diese Norm Komponenten aus bereits länger bestehenden Standards der ISO/IEC übernommen wurden

Kapitel 4: Objektorientiertes Design

Im folgenden Abschnitt werden das Vorgehen und die Ergebnisse rund um die für die vorliegende Arbeit durchlaufene Designphase beschrieben. Dabei wird zunächst auf die Vereinheitlichung der analysierten Ansätze – im Weiteren als *Komponenten* bzw. *Quellkomponenten* bezeichnet – anhand von Mapping-Tabellen und Mapping-Diagrammen eingegangen, deren Inhalte durch das anschließend erstellte Reduktionsmodell vereinfachend zusammengefasst wurden. Im harmonisierten Integrationsmodell findet die durchgeführte Transformation ihren Abschluss; die dabei erarbeiteten Inhalte werden im folgenden Abschnitt ebenfalls vorgestellt.

4.1 Vorgehen

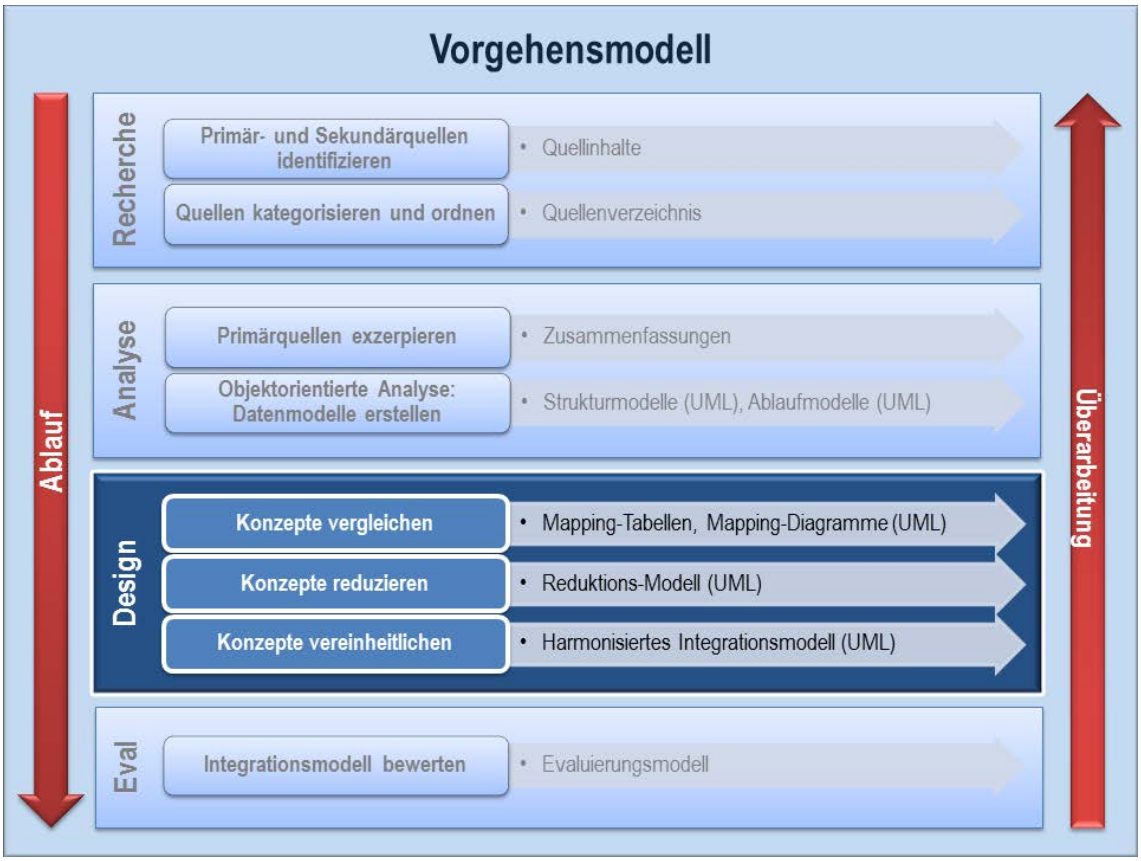

Abbildung 4.1: Vorgehensmodell: Designphase[72]

[72] Quelle: eigene Darstellung

4.1.1 Gegenüberstellung und Bewertung von Konzepten

Tabellarisches Mapping

Um die zuvor für jeden Ansatz / jede Komponente einzeln erarbeiteten Analyseergebnisse zu verbinden, wurde als nächster Schritt zur Harmonisierung zunächst ein tabellarisches Mapping erstellt, mit dessen Hilfe die gemeinsamen Konzepte identifiziert und gegenübergestellt wurden, was einen ersten Schritt zur Überwindung der strukturellen Heterogenität der Ansätze/Quellkomponenten darstellte (siehe Abbildung 4.2).

Hierbei wurde eine Tabelle für die Gesamtheit der Ansätze/Komponenten gebildet, die dem Bereich des Risiko- und Informationssicherheitsmanagements zuzurechnen sind, wie das Basel-II-Konglomerat, die ISO/IEC 27001 und 27005, die ISO 31000, die BSI-Standards, COSO ERM, Risk IT und SOX.

Eine zweite Tabelle mit knapp 1.000 Zeilen wurde hingegen den Rahmenwerken zur IT-Governance gewidmet, die nach dem Dokument *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit* von ITGI und OGC [36] sowie nach dem aktuellen Entwurf zu COBIT 5 [47, S. 205ff.] ein Mapping vornimmt, das, von den Kontrollbereichen und Prozessen aus COBIT 4.1 ausgehend, die Konzepte aus COBIT 4.1, COBIT 5, ITIL V3 und ISO/IEC 27002 einander zuordnet.[73]

Aus der Mapping-Tabelle zum Risiko- und Informationssicherheitsmanagement wurde die aus der Gegenüberstellung resultierende vorläufige Strukturierung anhand dreier umfangreicher Bereiche aufgebaut, die insgesamt 238 Elemente beinhaltet. Dazu zählen:

- **Begriffsdefinitionen**, beispielsweise zu Risiken, Ereignissen, Bedrohungen und Schwachstellen, Kategorien zur Strukturierung des Kontexts oder Reifegraden; hierbei wurden 46 verschiedene Begriffe in zehn Gruppen identifiziert.

- Ein **System bzw. Framework zur Verwaltung des Risikomanagements**, im Rahmen dessen unter anderem die Strategieplanung, die Definition von Rollen und Verantwortlichkeiten, das Management von Ressourcen, der Umgang mit Auslagerungen oder die Dokumentation des Risikomanagements festgelegt werden; hierbei wurden 151 Begriffe in fünfzehn Gruppen zusammengefasst.

- Ein **Prozess zum Management von Risiken**, der in die drei Bereiche des Risikoassessments, der Risikoüberwachung sowie der Behandlung von Risiken unterteilt wurde, die insgesamt 41 Begriffe enthalten.

Wie bereits in den vorigen Kapiteln angesprochen, erstreckt sich die Heterogenität der Ansätze/Quellkomponenten jedoch nicht nur auf die strukturelle, sondern ebenso auf die

[73] Da der primäre Fokus der vorliegenden Arbeit auf den Komponenten zum Risikomanagement liegt, wurde nach diesem Mapping keine weitere Integration der IT-Governance-Frameworks durchgeführt; stattdessen wird aus dem Integrationsmodell direkt auf deren Inhalte verwiesen, falls Vorschläge für Steuerungs- und Kontrollmaßnahmen benötigt werden

inhaltliche Ebene. Um diesem Umstand Rechnung zu tragen, wurden die innerhalb der Mapping-Tabellen gegenübergestellten Konzepte durch ein dreistufiges Gewichtungssystem bewertet, dessen Skala von *0* (Konzept ist nicht vorhanden) über *1* (Konzept ist mit niedrigem Detaillierungsgrad vorhanden) bis zur Stufe *2* (Konzept wird detailliert beschrieben) reichte.

Bereits innerhalb der Mapping-Tabellen konnte dadurch ein übergreifendes Modell erarbeitet werden, das durch die Aggregation jener Konzepte mit den jeweils höchsten Gewichten entstand, in sich jedoch weiterhin eine starke Heterogenität aufwies, weshalb wie erwartet weiterer Harmonisierungsbedarf bestand.

Gemäß der in Abschnitt 1.1.3 beschriebenen Anforderungen wurde in diesem Schritt besonderes Augenmerk auf die Nachverfolgbarkeit der Ansätze/Quellkomponenten gelegt, was durch Referenzen auf die zugehörigen Abschnitte in den Quelldokumenten auf feingranularer Ebene verwirklicht wurde (siehe Abbildung 4.2).

Mapping-Diagramme

Die – wie zuvor gezeigt – notwendige Weiterführung der Mapping-Tabelle erfolgte durch das sogenannte *Mapping-Diagramm*, das für jeden Strukturierungspunkt jene Konzepte aus den einzelnen Ansätzen/Quellkomponenten enthält, die in ihrer Gesamtheit nach Einschätzung des Autors die passendsten Gesamtdefinitionen liefern. Dabei wurden nicht lediglich auf triviale Art jene Konzepte übernommen, die zuvor die höchsten Gewichte erhalten hatten; vielmehr wurde das Hauptaugenmerk bei dieser Auswahl auf die wechselseitige Ergänzung der Beschreibungen und deren Integrierbarkeit gelegt.

Ein weiterer Zweck dieses Diagramms ist es wiederum, die Nachverfolgbarkeit zu erleichtern, indem genau gezeigt wird, aus welchem Ansatz / welcher Quellkomponente welche Konzepte in die nachfolgende Harmonisierung einfließen.

Dabei entstand eine Matrix, deren Zeilen den Strukturierungspunkten entsprechen, während jede Spalte einem einer Quellkomponente zugeordnet ist. Da die Zellen dieser Matrix genau jene Inhalte enthalten, die im Folgenden zu integrieren sind, werden diese in Anlehnung an das verwendete UML-Konstrukt als *Integrationspakete* bezeichnet (siehe den Gesamtüberblick in Abbildung 4.3 sowie die Details in Abbildung 4.4, die drei Integrationspakete darstellt).

Mapping von IT-Risikomanagement-Frameworks

	Referenz			Vergleich				
	Aggregation			ISO Standards				
				ISO 27001		ISO 27005		
#	Referenz	Kategorie	Ebene	Bezeichnung	Referenz	Ebene	Bezeichnung
227	C	**Risiko-Management-Kreislauf**		**Risiko-Management-Kreislauf**			**Risiko-Management-Kreislauf**
228	C.1	**Prozessdefinition**		**Prozessdefinition**			**Prozessdefinition**
229	(ISO 27005)	RM-Prozess	2	PLAN; DO: ISMS einführen und betreiben	8	2	RM-Prozess
230							
231	C.2	**Risiko-Assessment**		**Risiko-Assessment**			**Risiko-Assessment**
232	(ISO 27005)	ISMS PLAN: Risiko-Assessment durchführen	0		8	2	ISMS PLAN: Risiko-Assessment durchführen
233	(ISO 27005)	ISMS PLAN: Risiken identifizieren	1	PLAN: Risiken identifizieren	8.2.1	2	ISMS PLAN: Risiken identifizieren
234	(ISO 27005)	ISMS PLAN: Assets identifizieren	1	PLAN: Assets, Eigentümer identifizieren	8.2.1.2	2	ISMS PLAN: Assets identifizieren
235	(BSI 100-2)	Schutzbedarf für Assets definieren	0			1	
236	(BSI 100-2)	Asset-Gruppen zu Sicherheitszonen zusammenfassen	0			0	
237	(ISO 27005)	ISMS PLAN: Bedrohungen identifizieren	1	PLAN: Bedrohungen identifizieren	8.2.1.3	2	ISMS PLAN: Bedrohungen identifizieren
238	(ISO 27005)	ISMS PLAN: Existierende Controls identifizieren	0		8.2.1.4	2	ISMS PLAN: Existierende Controls identifizieren
239	(ISO 27005)	ISMS PLAN: Schwachstellen identifizieren	1	PLAN: Schwachstellen identifizieren	8.2.1.5	2	ISMS PLAN: Schwachstellen identifizieren
240	(ISO 27005)	ISMS PLAN: Auswirkungen identifizieren	1	PLAN: Auswirkungen identifizieren	8.2.1.6	2	ISMS PLAN: Auswirkungen identifizieren
241	(MaRisk)	Identifikation und Behandlung von Risikokonzentrationen	0			0	
242	(Basel II)	Risiko-Bewertung	1	PLAN: Risiken analysieren und bewerten	8.2 - 8.3	2	ISMS PLAN: Risiken analysieren / Risiken bewerten
243	(Basel II)	Risiko-Datensammlung	0			0	
244	(Basel II)	Erfassung, Nutzung von Risiko-Daten	1	PLAN: Geschäftsauswirkungen, Wahrscheinlichkeiten schätzen	8.2.2.3	2	ISMS PLAN: Wahrscheinlichkeiten schätzen
245	(Basel II)	Erfassung, Nutzung interner Daten	0			0	
246	(Basel II)	Kriterien für interne Verlustdaten	0			0	
247	(Basel II)	Erfassung, Nutzung externer Daten	0			0	
248	(Basel II)	Externe Prüfung der externen Datennutzung	0			0	
249	(Basel II)	Gewichtung von Risiko-Daten	0			0	
250	(MaRisk)	Stresstests, inverse Stresstests, Handlungen setzen	0		8.2.2.1	1	ISMS PLAN: Methoden zur Risikoschätzung auswählen
251	(COSO ERM)	Auswirkungen und Wahrscheinlichkeiten schätzen	0		8.2.2.4	1	ISMS PLAN: Risikohöhen schätzen
252	(COSO ERM)	Risiken visualisieren	0			0	
253	(SolvV)	Indikator-Methoden samt Verwaltung	0			0	
254	(SolvV)	Geschäftsfeldzuordnung samt Verwaltung, Prüfung	0			0	
255	C.3	**Risiko-Überwachung**		**Risiko-Überwachung**			**Risiko-Überwachung**
256	(ISO 27001)	DO: Risiko-Überwachung	2	DO: Risiko-Überwachung	12.1	1	ISMS CHECK: Risikofaktoren überwachen

Abbildung 4.2: Tabellarisches Mapping der Quellkomponenten (Ausschnitt)[74]

[74] Quelle: eigene Darstellung

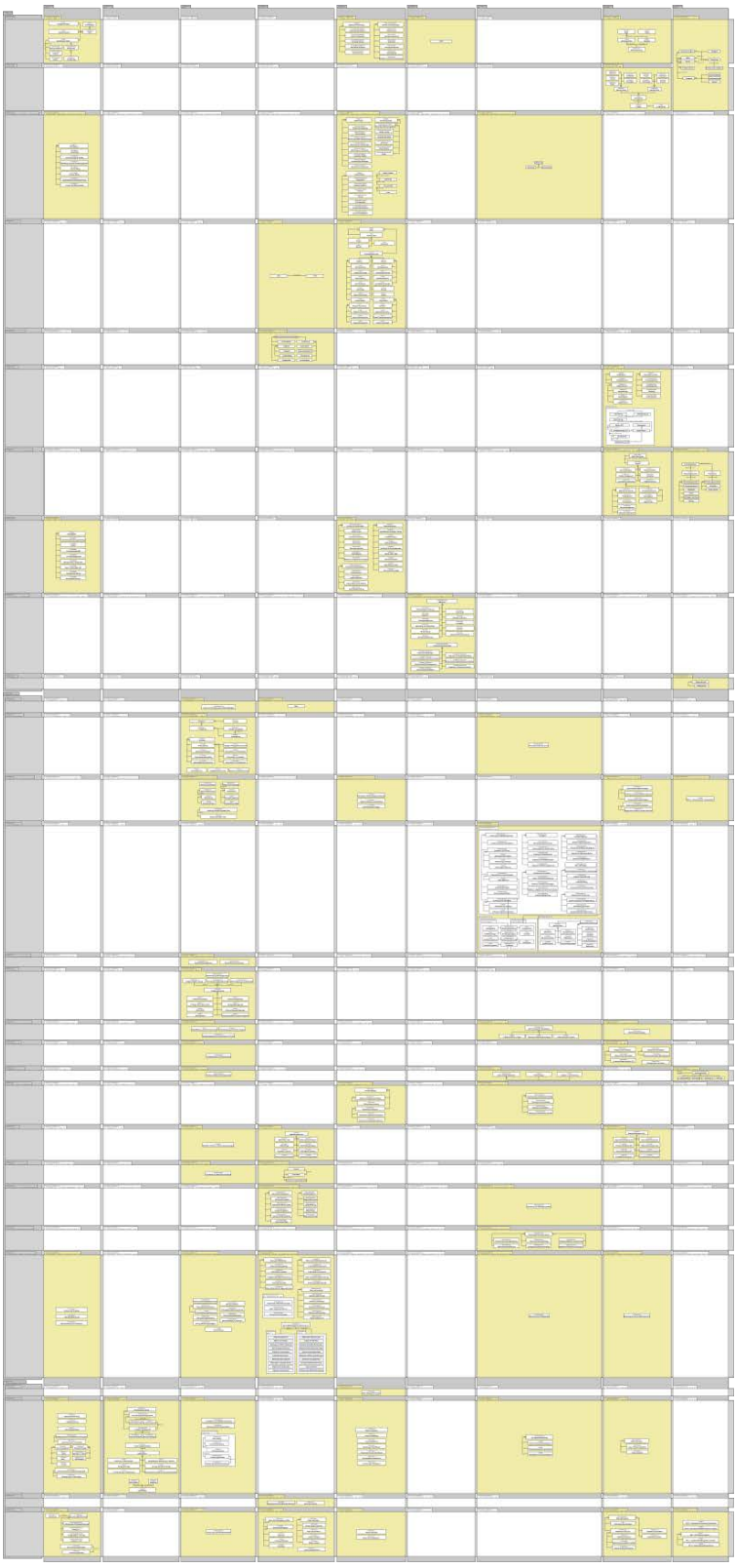

Abbildung 4.3: Mapping-Diagramm mit allen Integrationspaketen[75]

[75] Quelle: eigene Darstellung

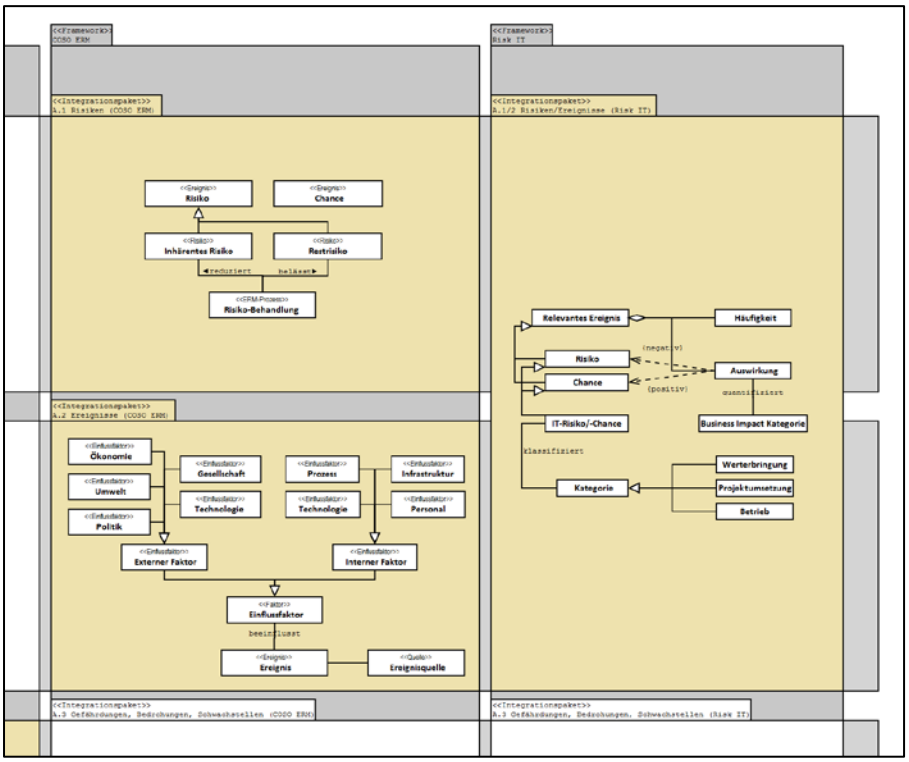

Abbildung 4.4: Mapping-Diagramm zu Risiken und Ereignissen (Ausschnitt)[76]

Mapping-Tabelle und Mapping-Diagramm: Zusammenführung

Um die Übersichtlichkeit zu erhöhen, wurden Struktur und Inhalt von Mapping-Tabelle und Mapping-Diagramm vereinfacht in Tabelle 4.1 zusammengefasst: Diese enthält ebenfalls pro Zeile einen Strukturierungspunkt, während in jeder Spalte eine eigene Quellkomponente angeführt wird. Im Gegensatz zum detaillierten Mapping-Diagramm aus Abbildung 4.3 sind in den Zellen jedoch die Detaillierungsgrade (von *0* bis *2*) dargestellt, in denen die einzelnen Standards und Rahmenwerke die verschiedenen Konzepte beschreiben; in dicker Umrandung werden zudem die Integrationspakete markiert.[77]

Aus den ebenfalls in Tabelle 4.1 dargestellten Zeilen- und Spaltensummen lässt sich auch erkennen, welche Konzepte von mehreren Komponenten beschrieben werden, bzw. wie groß der Umfang der einzelnen Quellkomponenten ist; beliebte Konzepte stellen demnach wie erwartet der Risikobegriff, ein System zur Verwaltung des Risikomanagement mit Strategieplanung, Überwachung und Optimierung, sowie ein detaillierter Risikomanagement-Kreislauf dar. Die umfangreichsten Quellkomponenten stellen die BSI-Standards, Risk IT sowie die MaRisk dar.

[76] Quelle: eigene Darstellung

[77] Dabei wird erneut offensichtlich, dass diese nicht lediglich aus den in der Mapping-Tabelle höchstgewichteten Konzepten bestehen, sondern die wechselseitige Ergänzung der Beschreibungen im Hinblick auf das endgültige Integrationsmodell und deren Integrierbarkeit im Mittelpunkt standen.

Zusammenfassung des Mappings der Komponenten

		Komponente											
#	Strukturierungspunkt	Basel II	SolvV	KWG	MaRisk	ISO 27001	ISO 27005	ISO 31000	BSI Standards	COSO ERM	Risk IT	SOX & ISACA	*Summe*
A	Begriffe												
A.1	Risiken	1	1	1	1	1	2	2	2	2	2	0	15
A.2	Ereignisse	0	0	0	0	1	1	1	1	2	2	0	8
A.3	Gefährdungen, Bedrohungen, Schwachstellen	1	1	0	0	1	2	1	2	0	1	0	9
A.4	Assets und Wert	0	0	0	0	2	2	1	2	0	2	0	9
A.5	Informationssicherheit	0	0	0	1	2	0	0	2	1	1	0	7
A.6	ERM-Struktur	0	0	0	0	0	0	0	0	2	2	0	4
A.7	Kontroll- und Steuerungsmaßnahmen	1	1	1	1	1	1	1	1	1	2	1	12
A.8	Kontext	1	1	0	0	0	2	1	0	0	0	0	5
A.9	Risikomanagement-Prinzipien, Zielsetzungen	0	0	0	0	0	0	2	0	0	1	0	3
A.10	Reifegrade	0	0	0	0	0	0	0	0	0	2	0	2
B	Management-System												
B.1	Systemdefinition	1	1	1	2	1	0	1	2	2	2	2	15
B.2	Ressourcenmanagement	1	1	1	2	1	1	1	1	0	1	0	10
B.3	Kommunikation und Berichterstattung	1	1	1	2	0	1	1	1	1	1	1	11
B.4	Notfallmananagement	0	0	1	1	0	0	0	2	0	0	0	4
B.5	Risikomanagement bei neuen Produkten/Märkten	0	0	0	2	0	0	0	0	0	0	0	2
B.6	Auslagerungen	0	0	1	2	0	0	0	0	0	0	0	3
B.7	Verantwortung und Leitungsebene	1	1	1	1	1	0	1	1	1	1	1	10
B.8	Strategieplanung	1	1	1	2	1	1	1	1	2	2	1	14
B.9	Organisationsstruktur	0	1	0	2	0	2	1	2	2	1	0	11
B.10	Kontext, Umfang und Abgrenzung	0	0	0	0	0	2	1	2	0	1	0	6
B.11	Dokumentation	1	1	0	2	2	0	1	1	1	0	1	10
B.12	Grundsatz und Leitlinien	1	1	0	2	2	0	1	1	1	1	1	11
B.13	Informations- und Dokumentenmanagement	0	0	0	1	2	1	1	1	0	0	0	6
B.14	Einführung des Management-Systems	0	0	0	0	0	0	1	2	1	1	1	6
B.15	Überwachung, Prüfung und Optimierung	1	1	1	2	2	1	1	2	2	1	1	15
C	Risiko-Management-Kreislauf												
C.1	Prozessdefinition	1	1	1	1	2	2	1	1	2	2	1	15
C.2	Risiko-Assessment	1	1	1	1	1	2	1	1	2	2	1	14
C.3	Risiko-Überwachung	1	1	1	1	2	1	1	1	1	1	0	11
C.4	Risiko-Behandlung	1	1	1	1	1	2	1	1	1	2	1	13
	Summe	16	17	14	30	26	26	25	33	27	34	13	

Legende	
0	nicht vorhanden
1	geringe Detaillierung
2	hohe Detaillierung

Tabelle 4.1: Zusammenfassung des Mappings der Komponenten.[78]

[78] Quelle: eigene Darstellung

4.1.2 Reduktion

Wie aus Abbildung 4.3 ersichtlich, weist das bislang erarbeitete Mapping-Diagramm eine enorme Größe auf, die zwar die Nachverfolgbarkeit sicherstellt, für die weitere Harmonisierung jedoch zu wenig Überblick schafft. Aus diesem Grund wurden im nächsten Schritt die Integrationspakete derart zusammengefasst, dass pro Strukturierungspunkt erkennbar ist, welche Konzepte zu harmonisieren sind; die Nachverfolgbarkeit in diesem *Reduktionsmodell* ist jedoch weiterhin durch die Benennung der Integrationspakete gegeben (siehe die Gesamtansicht in Abbildung 4.6 sowie den Ausschnitt zum Strukturierungspunkt *Risikobegriff* in Abbildung 4.5).

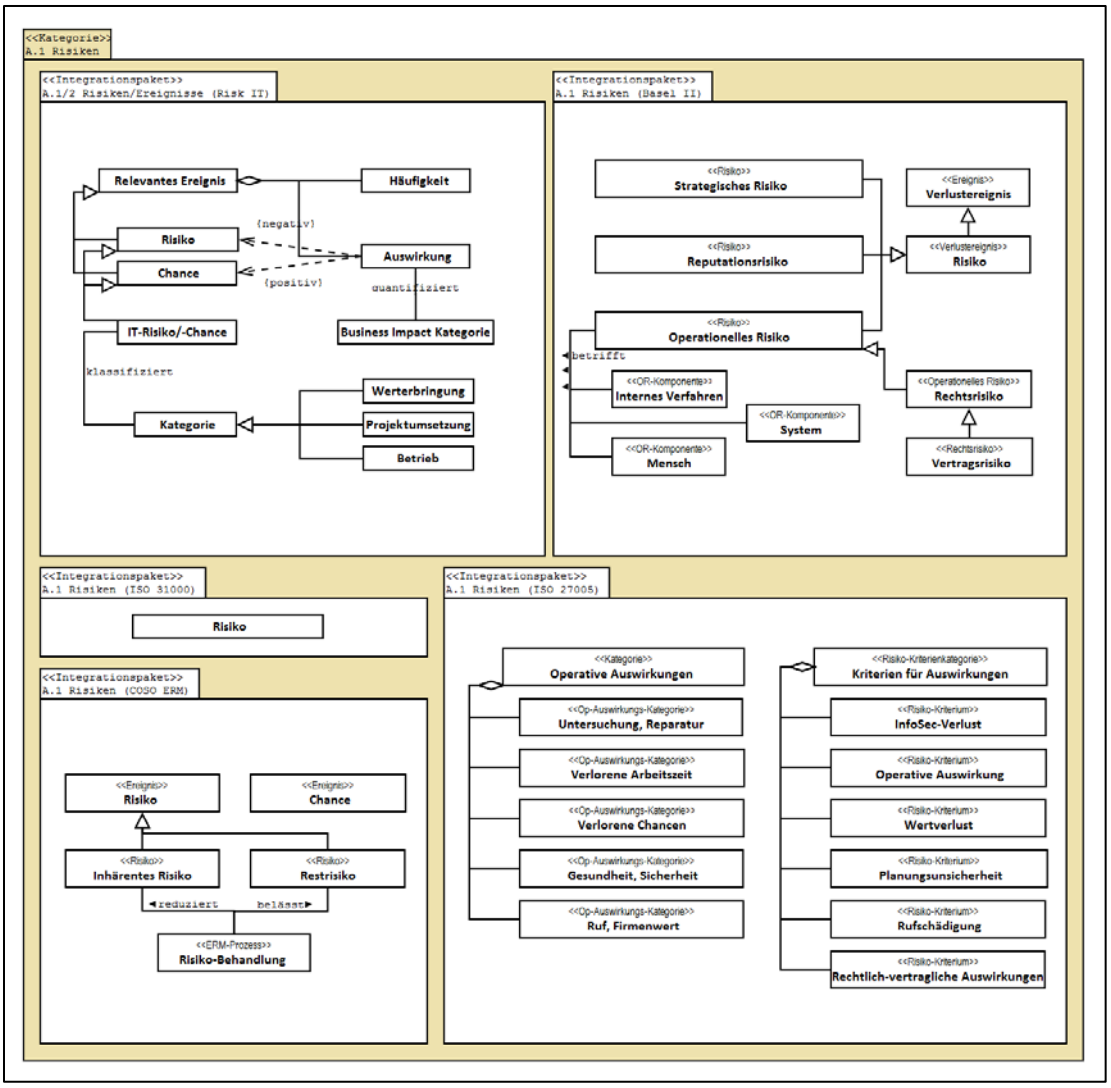

Abbildung 4.5: Reduktionsmodell: Integrationspakete zum Risikobegriff[79]

[79] Quelle: eigene Darstellung

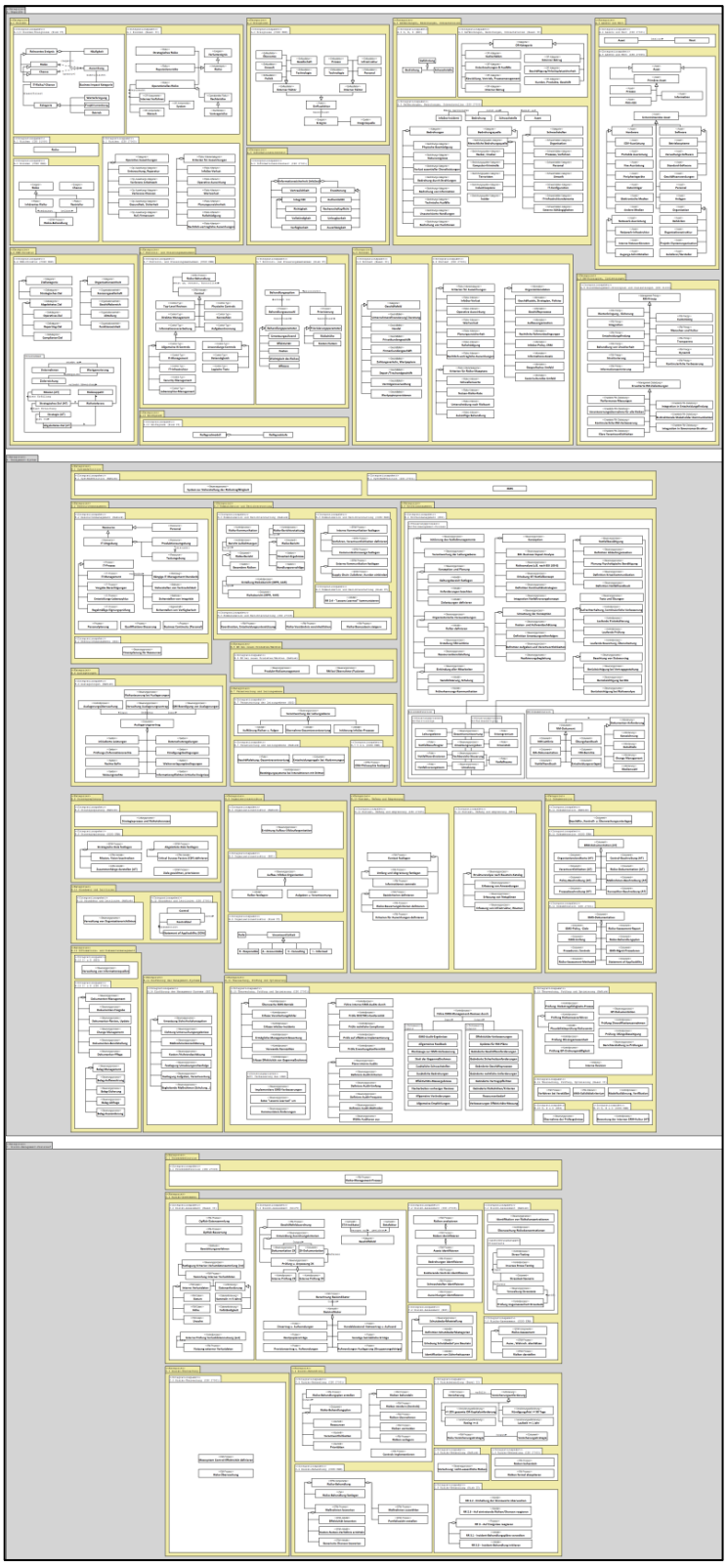

Abbildung 4.6: Reduktionsmodell[80]

[80] Quelle: eigene Darstellung

4.1.3 Vereinheitlichung

Im Rahmen der nun folgenden Vereinheitlichung wurden die Konzepte in ein einzelnes, homogenes Modell überführt. Die Integrationspakete wurden aufgelöst und derart zusammengefasst, dass ein harmonisiertes Integrationsmodell entstand, wobei auftretende Widersprüche bereinigt, Klassifikationen vereinheitlicht und Beziehungen zwischen den Konzepten gebildet wurden. Somit entstand ein Modell mit geringerer Komplexität, das die gestellten Anforderungen dennoch erfüllt.

Dieses wurde anhand einer neuartigen Strukturierung aufgebaut, die zwar an die seit der Analyse bestehenden Strukturierungspunkte angelehnt ist, diese jedoch vereinfacht. Anhand der Inhalte der harmonisierten Struktur (statischer Aspekt) wurde anschließend auch ein harmonisiertes Prozessmodell gebildet (dynamischer Aspekt)

4.2 Das harmonisierte Integrationsmodell

In diesem Abschnitt wird das erarbeitete Integrationsmodell vorgestellt und dessen Bestandteile im Detail beschrieben. Es ist wichtig zu erwähnen, dass es sich hierbei um eine generische Musterlösung handelt, die durch die Anwendung des wiederverwendbaren Vorgehensmodells aus Kapitel 2.1 entstand, das die Basis der vorliegenden Arbeit bildet und die in Abschnitt 1.1.3 gestellten Anforderungen erfüllt.

Beim Einsatz des harmonisierten Integrationsmodells im Rahmen eines Praxisprojekts ist jedoch davon auszugehen, dass Anpassungen an den spezifischen Kontext vorgenommen werden müssen – etwa wenn branchenabhängige Standards und Gesetze zum IT- oder Risikomanagement zu verwenden sind – die zu Abweichungen vom nachfolgend vorgestellten Modell führen können.

4.2.1 Vereinheitlichte Struktur – Überblick

Die vereinheitlichte Struktur enthält eine Hierarchie aus Begriffen, Prozessen und unterstützenden Konzepten, die in folgende vier Bereiche unterteilt werden:

- **SBR – Struktur und Begriffe:** Diese Begriffsgruppe definiert in insgesamt neun untergeordneten Gruppen die in den weiteren Komponenten verwendeten Grundbegriffe und beschreibt die zugrunde liegende Strukturierung im Sinne eines Metamodells.

- **FRA – Framework:** Das Framework bildet die organisatorische Basis zum IT-bezogenen Risikomanagement und definiert ein Informationssicherheits-Managementsystem (ISMS). Dieses ist an den bekannten Deming-Kreislauf angelehnt und enthält 13 Prozessgruppen, die nach den Phasen *Plan – Do – Check – Act* sowie einem Bereich für unterstützende Prozesse strukturiert sind.

- **PRO – Prozesse:** Die Prozesse zum IT-bezogenen Risikomanagement enthalten die zentralen Abläufe aus den Bereichen der Kontextdefinition und des

Risikoassessments, sowie der Evaluierung, Behandlung und Überwachung von Risiken.

- **ITM – IT-Management:** Um konkrete Maßnahmen für IT Governance sowie IT Service- und Informationssicherheits-Management anbieten zu können, werden die Frameworks COBIT 4.1, ITIL V3 sowie die internationale Norm ISO/IEC 27002 in das Integrationsmodell mit einbezogen. Als zugehöriger Integrationsmechanismus dient das in Abschnitt 4.1.1 vorgestellte tabellarische Mapping zur gegenseitigen Abstimmung dieser Komponenten.

Da die einzelnen Bereiche in sich eine hohe Komplexität aufweisen, wird das harmonisierte Integrationsmodell in Abbildung 4.7 zunächst stark vereinfacht dargestellt. Abbildung 4.8 zeigt zudem sämtliche Begriffsgruppen mit ihren Bezeichnungen, spart jedoch nach wie vor viele Prozesse aus; diese sind erst in der vollständigen Darstellung des Integrationsmodells in Abbildung 4.9 enthalten.

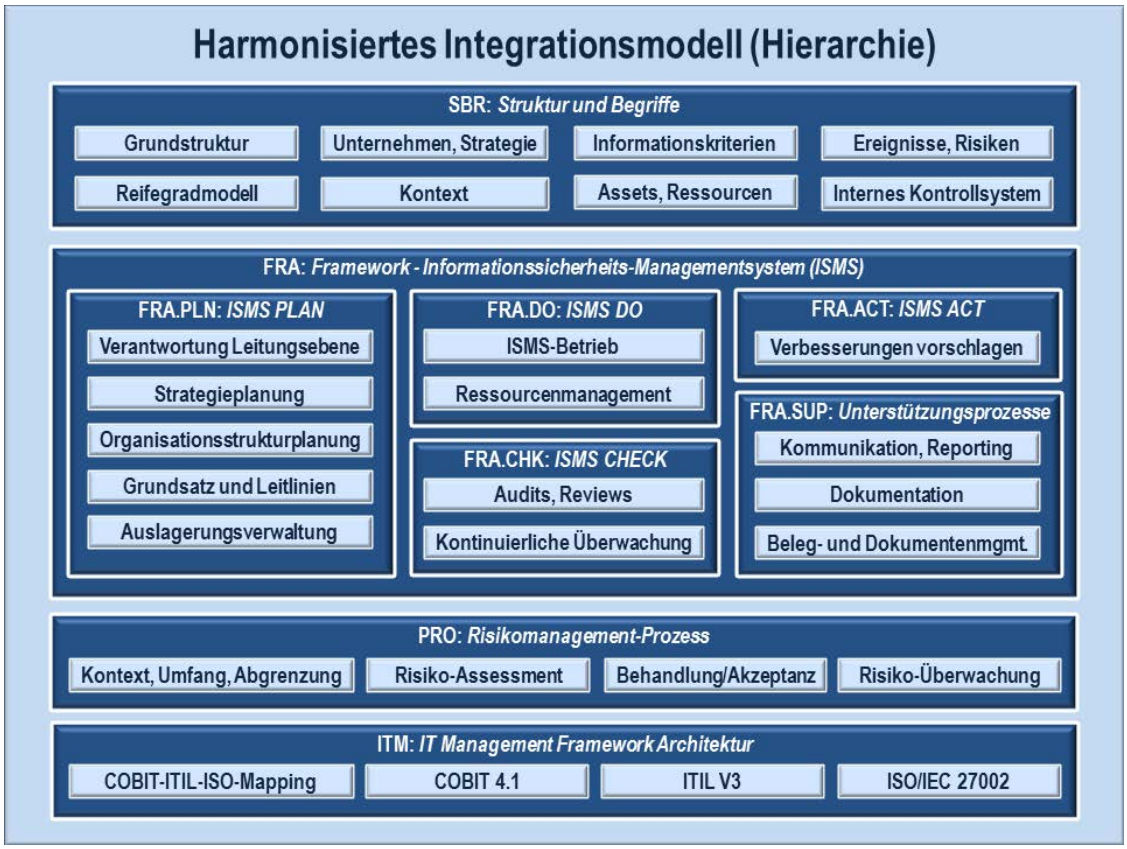

Abbildung 4.7: Harmonisiertes Integrationsmodell (stark vereinfachte Darstellung)[81]

[81] Quelle: eigene Darstellung

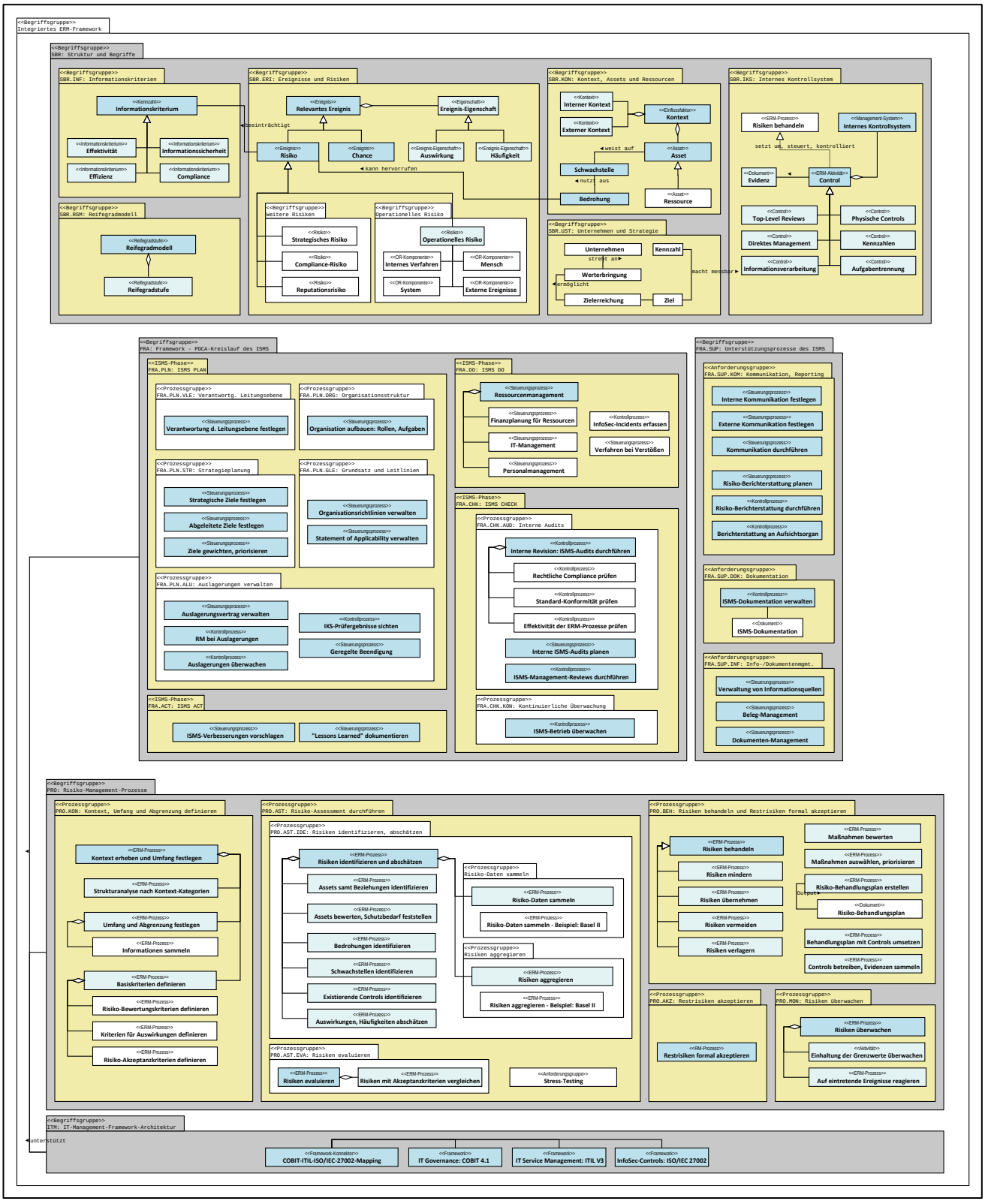

Abbildung 4.8: Harmonisiertes Integrationsmodell (vereinfachte Darstellung)[82]

[82] Quelle: eigene Darstellung

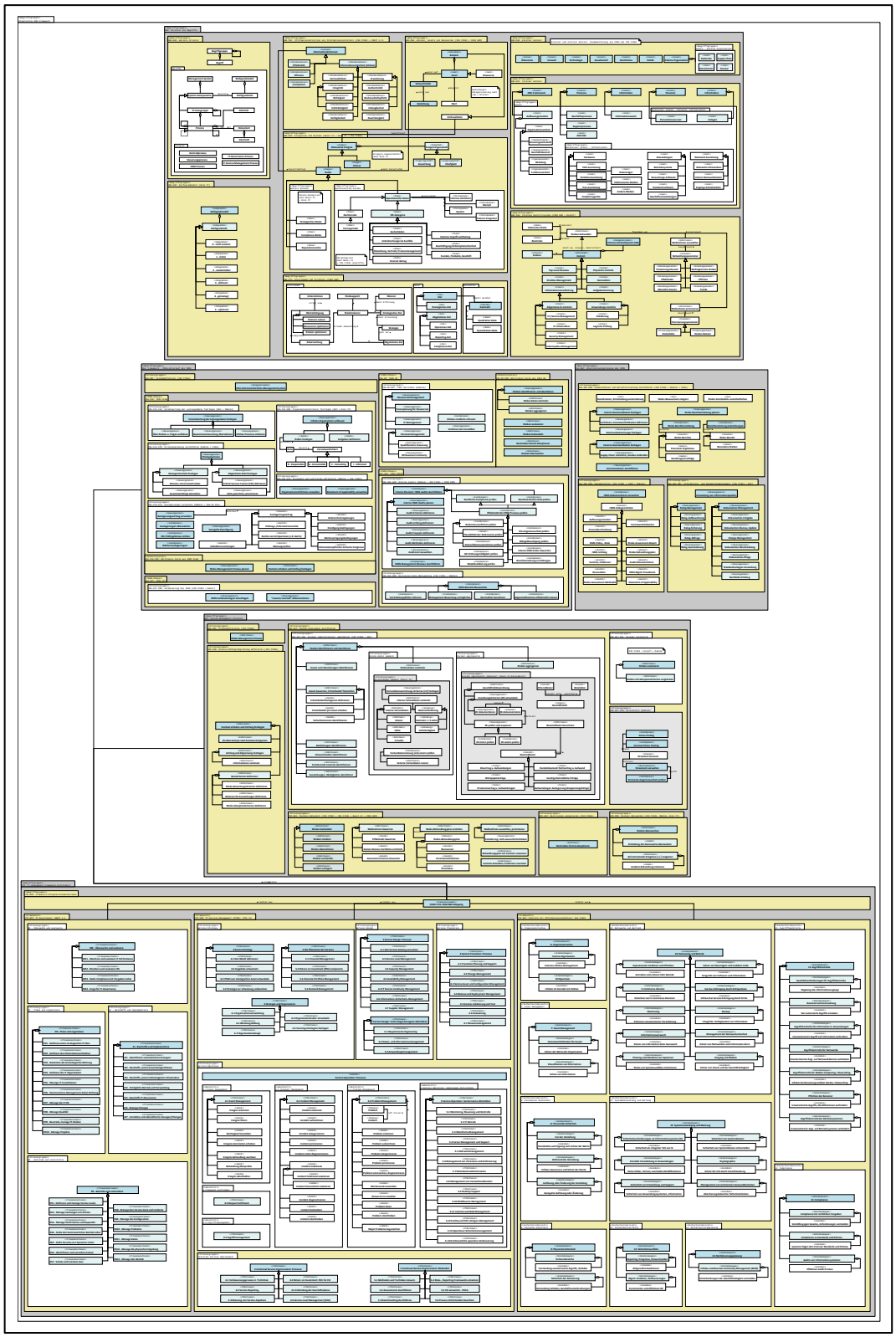

Abbildung 4.9: Harmonisiertes Integrationsmodell (vollständige Darstellung)[83]

[83] Quelle: eigene Darstellung

4.2.2 Vereinheitlichte Struktur – Details

SBR: Struktur und Begriffe

Diese Begriffsgruppe definiert in insgesamt neun untergeordneten Gruppen die in den weiteren Komponenten verwendeten Grundbegriffe und beschreibt die zugrunde liegende Strukturierung im Sinne eines Metamodells.

SBR.WSR: Grundlegende Struktur

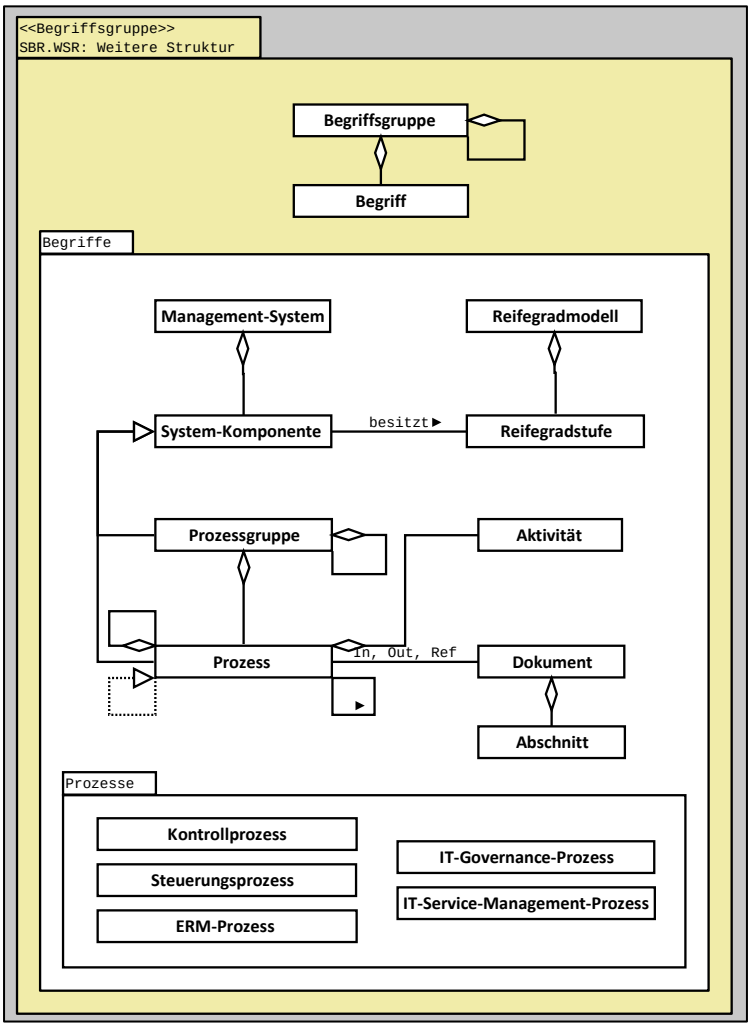

Abbildung 4.10: Begriffsgruppe SBR.WSR[84]

Als grundlegende Strukturierungselemente werden im Folgenden *Begriffe* verwendet, die in Begriffsgruppen (auch verschachtelt) zusammengefasst werden; hierfür wird das UML-Element *Paket* mit entsprechendem Stereotyp verwendet.

[84] Quelle: eigene Darstellung

Als Begriffe gelten auch Prozesse und Prozessgruppen, wobei erstere auch Teilprozesse besitzen, andere Prozesse realisieren oder mit ihnen in Verbindung stehen sowie Input-, Output- und sonstige Dokumente referenzieren können, die wiederum aus Abschnitten bestehen können. Prozesse lassen sich in Steuerungs- und Kontrollprozesse, ERM-Prozesse, IT-Governance-Prozesse sowie IT-Service-Management-Prozesse unterteilen. Prozesse stellen außerdem Teile von Management-Systemen dar, und können als solche anhand eines mehrstufigen Reifegradmodells bewertet werden.

SBR.ERI: Ereignisse und Risiken (nach Basel II, Risk IT, ISO/IEC 27005)

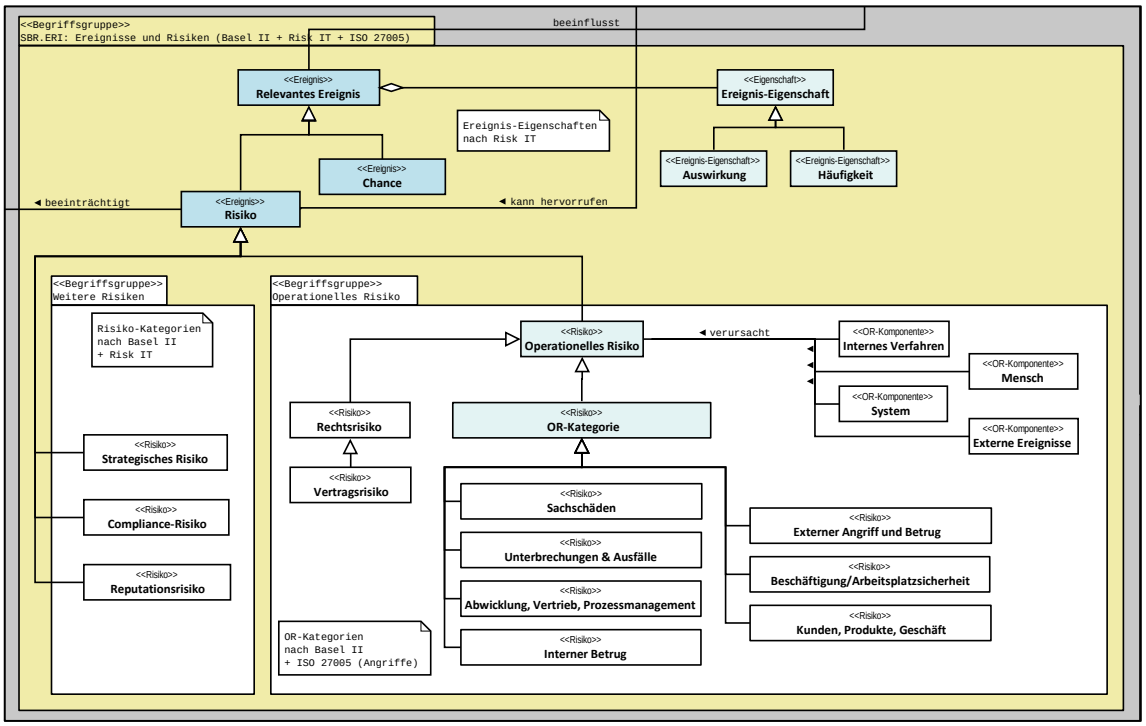

Abbildung 4.11: Begriffsgruppe SBR.ERI[85]

Sowohl *Risiken* als auch *Chancen* stellen für das IT-bezogene Risikomanagement *relevante Ereignisse* dar, die zugleich *Auswirkungen* und *Häufigkeiten* besitzen. *Operationelle Risiken*, zu denen auch *Rechtsrisiken* wie *Vertragsrisiken* zu zählen sind, werden durch *interne Verfahren*, *Systeme*, *Menschen* oder auch *externe Ereignisse* verursacht, und können nach Basel II und ISO/IEC 27005 in sieben *Kategorien* unterteilt werden.

Risiken *beeinträchtigen* Informationskriterien, werden durch Bedrohungen *hervorgerufen* und durch Einflussfaktoren wie den internen und externen Kontext *beeinflusst*.

[85] Quelle: eigene Darstellung

SBR.INF: Informationskriterien und Informationssicherheit (nach ISO/IEC 27001, COBIT 4.1)

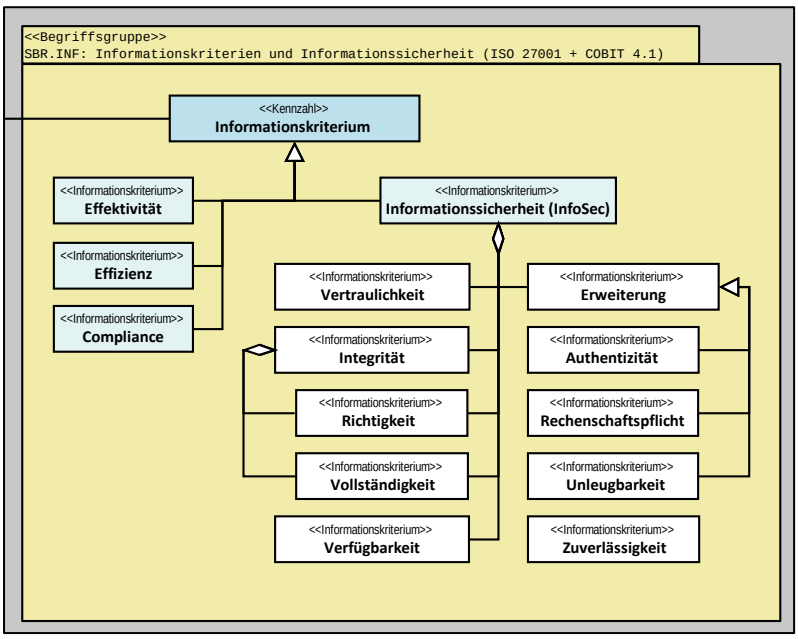

Abbildung 4.12: Begriffsgruppe SBR.INF[86]

Ziel des IT-bezogenen Risikomanagements ist es, die Erfüllung von *Informationskriterien* in festgelegten Maßen sicherzustellen, die je nach Anwendungsfall zu definieren sind. Zu diesen Kriterien zählen einerseits die *Effektivität* und *Effizienz* (Wirtschaftlichkeit) sowie die Einhaltung interner und externer Vorgaben (*Compliance*). Ein wesentliches, der Effizienz aber oft diametral gegenüberstehendes Ziel, ist zudem die *Informationssicherheit*, deren Grunddimensionen *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* nach ISO/IEC 27001 bei Bedarf um zusätzliche Komponenten erweitert werden können. Die Erfüllung der Informationskriterien wird durch Chancen begünstigt, durch Risiken jedoch *beeinträchtigt*.

[86] Quelle: eigene Darstellung

SBR.UST: Unternehmen und Strategie (nach COSO ERM)

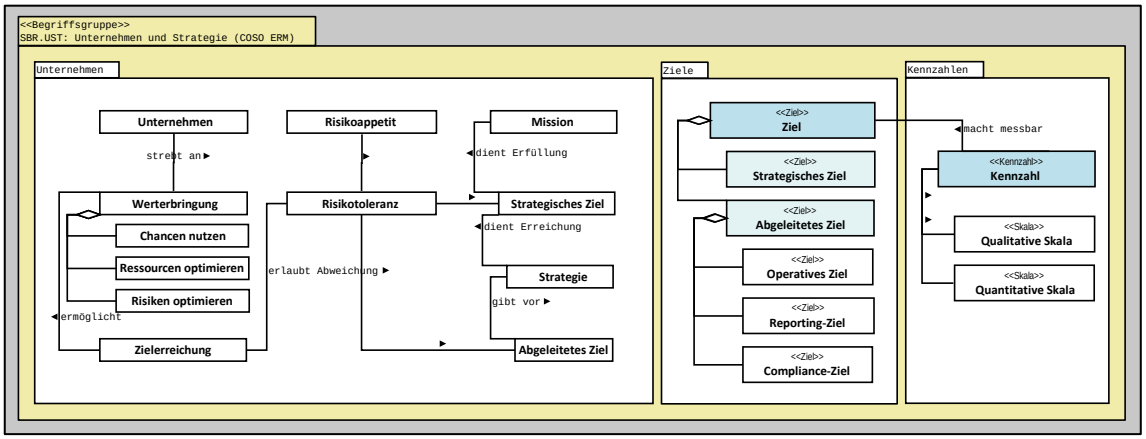

Abbildung 4.13: Begriffsgruppe SBR.UST[87]

IT-bezogenes Risikomanagement findet innerhalb eines *Unternehmens* statt. Dieses strebt grundsätzlich die *Erbringung von Leistungen und Mehrwert* an, und versucht dazu, *Chancen zu nutzen*, sowie *Ressourceneinsatz* und *Risiken zu optimieren*. Um Ziele erreichen zu können, ist zudem eine gewisse *Risikotoleranz* nötig, die – je nach *Risikoappetit* des Unternehmens – eine gewisse *Abweichung* von diesen Zielen erlaubt. Die *Mission* des Unternehmens bestimmt, welche *strategischen Ziele* gesetzt werden, und diese wiederum bestimmen die angewandten *Strategien* und davon *abgeleiteten Ziele*. Ziele sollen mithilfe von *Kennzahlen* quantifiziert und messbar gemacht werden.

SBR.KON: Kontext, Assets und Ressourcen (nach ISO/IEC 27005, COSO ERM)

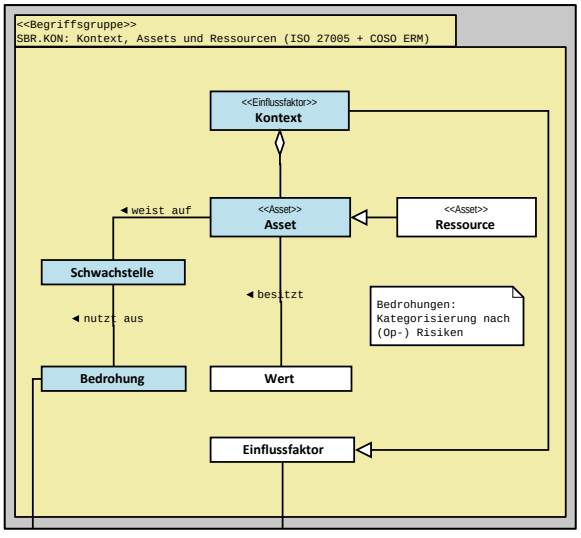

Abbildung 4.14: Begriffsgruppe SBR.KON[88]

[87] Quelle: eigene Darstellung
[88] Quelle: eigene Darstellung

Der *Kontext* eines Unternehmens stellt einen wesentlichen *Einflussfaktor* auf Risiken und Chancen dar: Er enthält sämtliche *Assets*, also Objekte, die für das Unternehmen *Wert* besitzen, wozu beispielsweise auch *Ressourcen* zu zählen sind. Assets können *Schwachstellen* aufweisen, die von *Bedrohungen* ausgenutzt werden können, woraus Risiken entstehen.

SBR.KOE/KOI: Externer und interner Kontext (nach COSO ERM, ISO/IEC 27005)

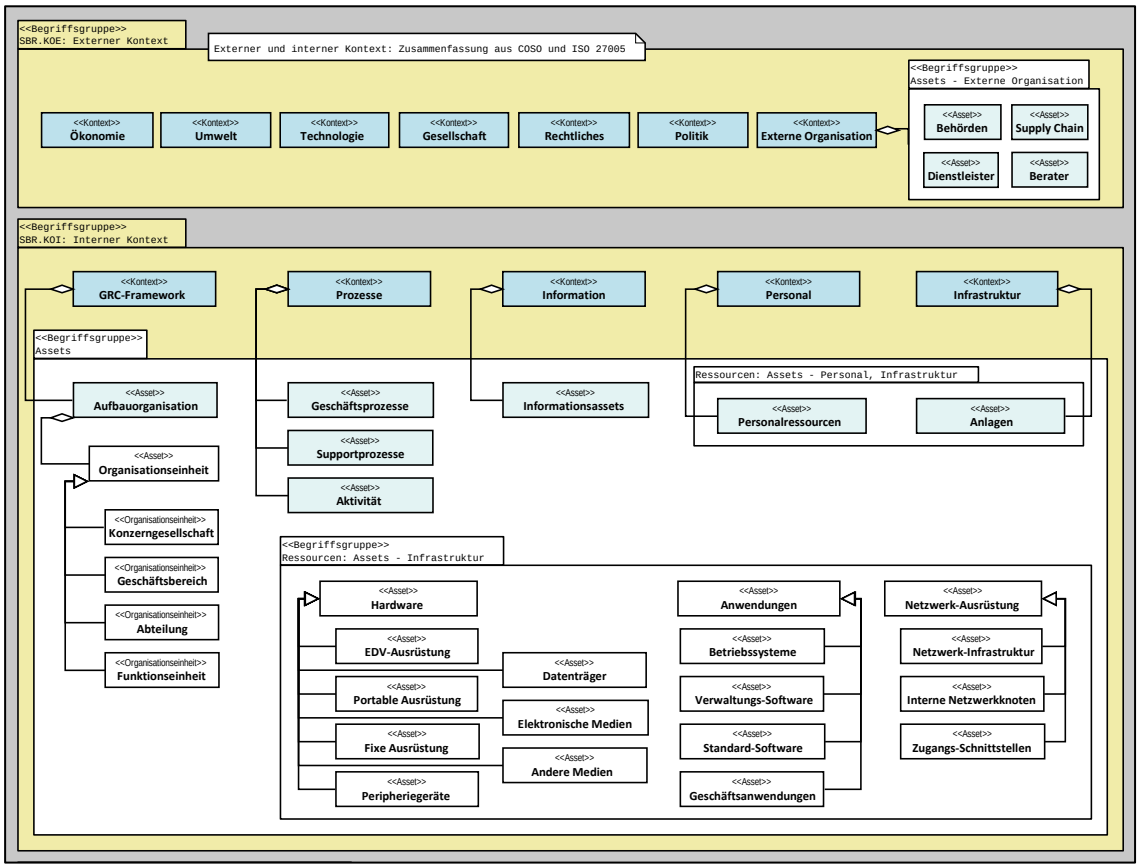

Abbildung 4.15: Begriffsgruppen SBR.KOE, SBR.KOI[89]

Kontext und Assets sind nach verschiedenen Kategorien zu unterteilen, die eine möglichst weitreichende Erfassung der relevanten Einflussfaktoren erlauben.

[89] Quelle: eigene Darstellung

SBR.IKS: Internes Kontrollsystem (nach COSO ERM, Risk IT)

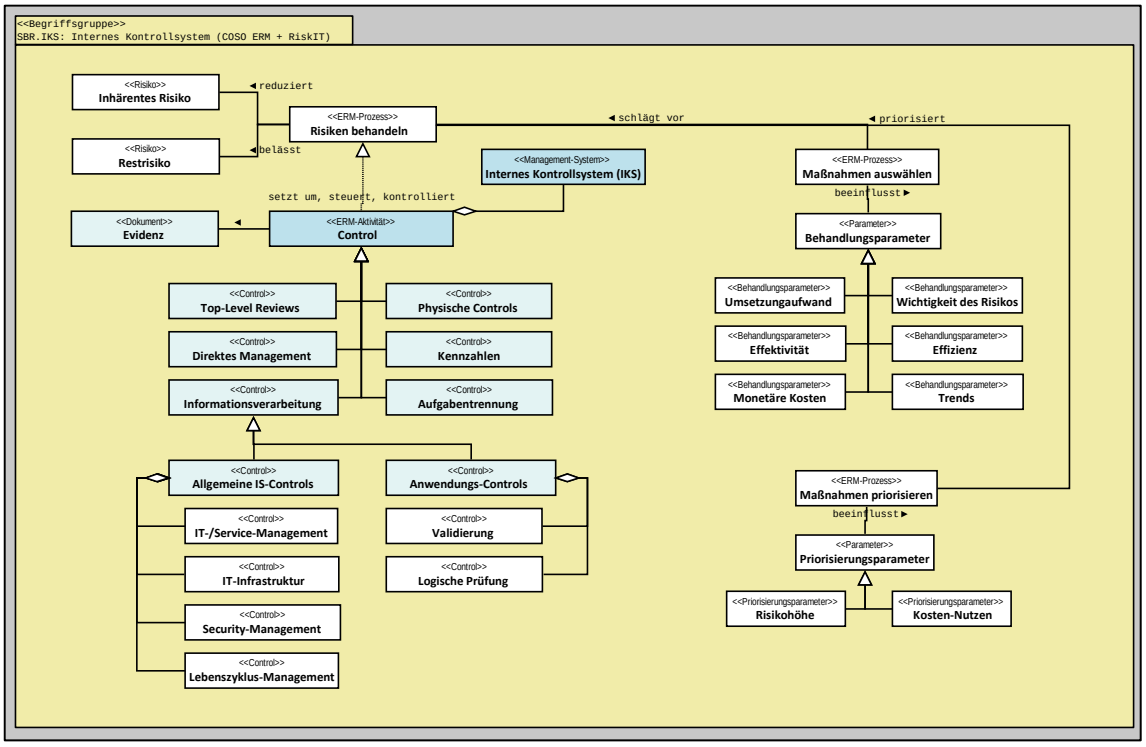

Abbildung 4.16: Begriffsgruppe SBR.IKS[90]

Die *Risikobehandlungsmaßnahmen* eines Unternehmens werden vor ihrem Einsatz zunächst nach einer Reihe von Parametern *ausgewählt* und *priorisiert*. Das *Interne Kontrollsystem (IKS)* enthält sämtliche Steuerungs- und Kontrollaktivitäten (*Controls*), die dazu dienen, die Risikobehandlung *umzusetzen, zu steuern und zu kontrollieren*. Während ihres Betriebs fallen *Evidenzen* an, die deren korrekte Funktion – beispielsweise im Rahmen von internen und externen Audits – im Nachhinein belegen.

[90] Quelle: eigene Darstellung

SBR.RGM: Reifegradmodell (nach Risk IT)

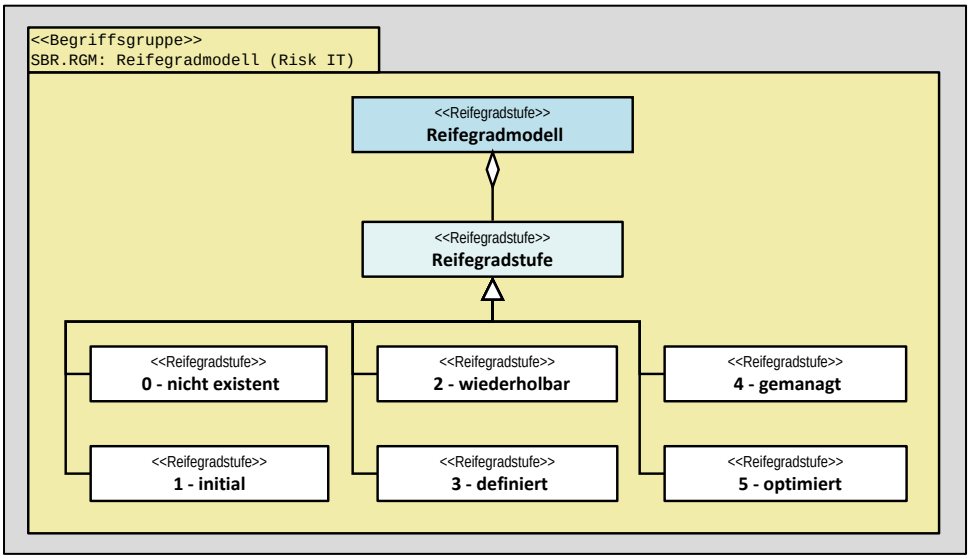

Abbildung 4.17: Begriffsgruppe SBR.RGM[91]

Der Reifegrad von Systemkomponenten wie Prozessen und Prozessgruppen kann mithilfe eines mehrstufigen *Reifegradmodells* bewertet werden, um Verbesserungsmöglichkeiten zu identifizieren und die Weiterentwicklung priorisieren zu können. Die verwendete Systematik wurde aus Risk IT übernommen und ist, ebenso wie das bekannte Modell aus COBIT 4.1, an CMM/CMMI angelehnt (siehe Abschnitt 3.2.12).

FRA: Framework – Informationssicherheits-Managementsystem (ISMS)

Das Framework bildet die organisatorische Basis zum IT-bezogenen Risikomanagement und definiert ein Informationssicherheits-Managementsystem (ISMS). Dieses ist an den bekannten Deming-Kreislauf angelehnt und enthält 13 Prozessgruppen, die nach den Phasen *Plan – Do – Check – Act* sowie einem Bereich für unterstützende Prozesse strukturiert werden.

[91] Quelle: eigene Darstellung

FRA.PLN.VLE: Verantwortung der Leitungsebene festlegen (nach BSI, MaRisk)

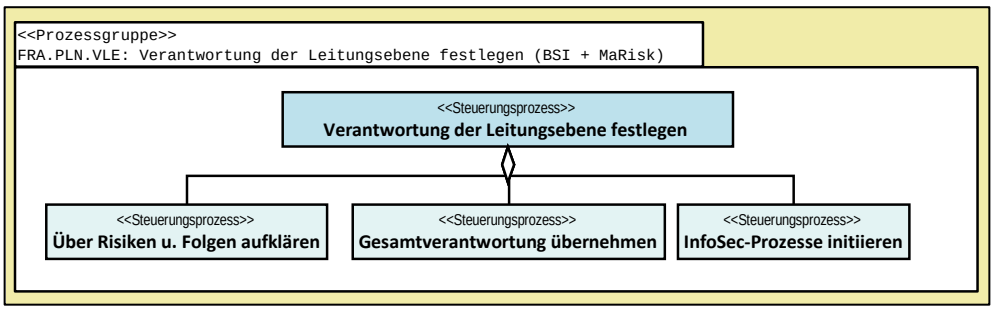

Abbildung 4.18: Prozessgruppe FRA.PLN.VLE (ISMS PLAN)[92]

Im Rahmen der Planungsphase ist zunächst die *Verantwortung der Leitungsebene des Unternehmens festzulegen*. Das Management ist dabei über die *Risiken und Folgen in Bezug auf Informationssicherheit aufzuklären*. Des Weiteren ist es die Aufgabe der Führungsebene, die *Gesamtverantwortung* für das Risikomanagement formell zu übernehmen und die relevanten *Informationssicherheits-Prozesse zu initiieren*.

FRA.PLN.STR: Strategieplanung durchführen (nach MaRisk, COSO ERM)

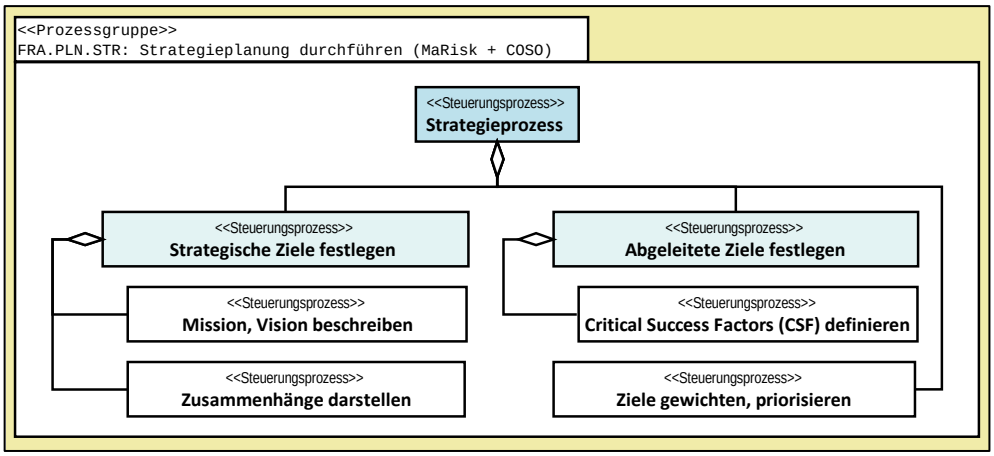

Abbildung 4.19: Prozessgruppe FRA.PLN.STR[93]

Der *Strategieprozess* enthält die *Definition strategischer* und *abgeleiteter Ziele*. Besonderer Wert ist auf die Definition von kritischen Erfolgsfaktoren mit hoher Priorität (*Critical Success Factors, CSF*) sowie die Auflösung von Zielkonflikten zu legen.

[92] Quelle: eigene Darstellung
[93] Quelle: eigene Darstellung

FRA.PLN.ORG/GLE: Organisationsstruktur festlegen (nach BSI, Risk IT), Grundsatz und Leitlinien definieren (nach MaRisk, ISO/IEC 27001)

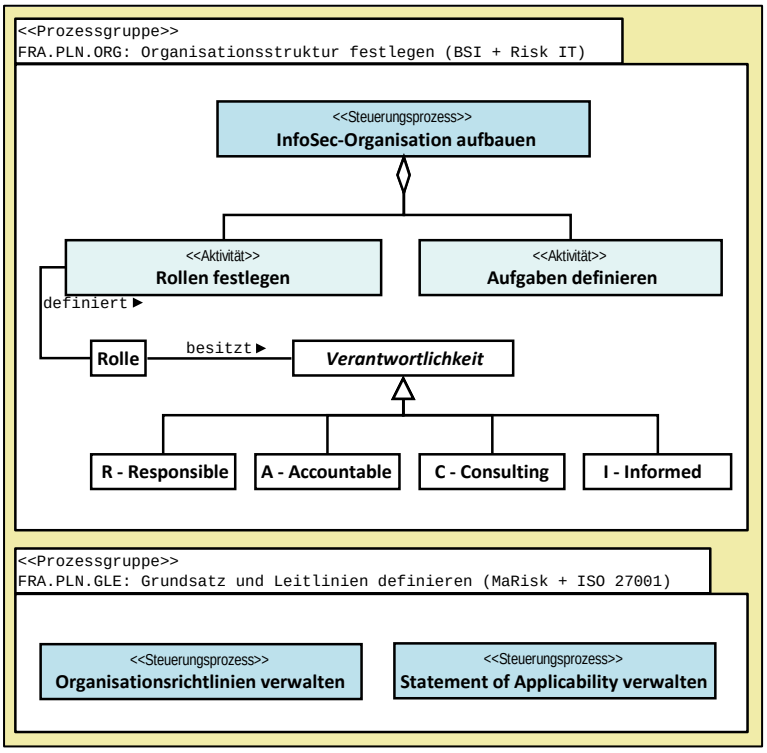

Abbildung 4.20: Prozessgruppen FRA.PLN.ORG, FRA.PLN.GLE[94]

Neben den Prozessen, deren Aufbau unter dem Strukturierungspunkt *PRO* beschrieben wird, stellen auch *Rollen und Verantwortlichkeiten* einen wesentlichen Bestandteil der Informationssicherheits- und Risikomanagement-Organisation dar. Zuständigkeiten können beispielsweise nach dem *RACI-Modell* aus Risk IT definiert werden, das einer Rolle eine beliebige Kombination aus vier möglichen Typen an Verantwortlichkeiten zuweist: *Responsible* (ausführend), *Accountable* (verantwortlich), *Consulting* (beratend tätig) und *Informed* (wird informiert).

Die entsprechenden Richt- und Leitlinien (Policies) sowie die Definition des Anwendungsbereichs (*Statement of Applicability*) sind ebenso aufzusetzen, zu verwalten und zu verteilen.

[94] Quelle: eigene Darstellung

FRA.PLN.ALU: Auslagerungen verwalten (nach MaRisk, IDW PS 951)

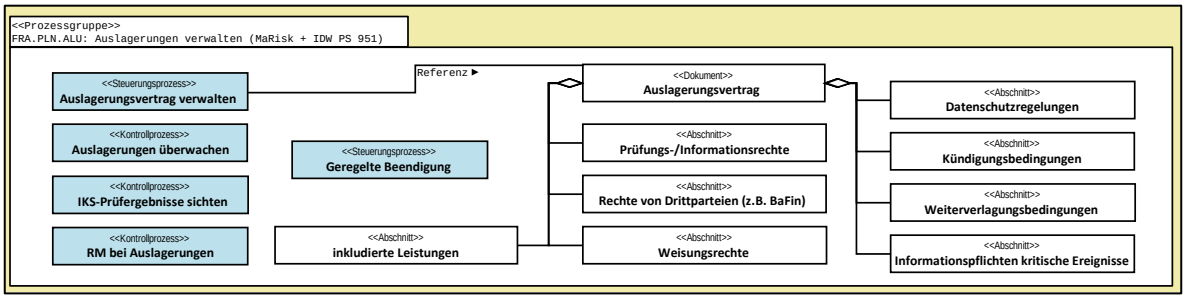

Abbildung 4.21: Prozessgruppe FRA.PLN.ALU[95]

Die *Verwaltung von* Auslagerungen umfasst sowohl die *Pflege des zugehörigen Vertrages* als auch die *kontinuierliche Überwachung des Systembetriebs*, die *Sichtung von Prüfergebnissen des IKS* des Dienstleisters und die *Steuerung und Kontrolle entsprechender Risiken*. Einen weiteren wesentlichen Punkt stellt die *geregelte Beendigung von Outsourcing-Verhältnissen* im Sinne der reibungslosen Fortführung der Geschäftstätigkeit (*Business Continuity*) dar.

FRA.DO.BET: ISMS betreiben (nach MaRisk)

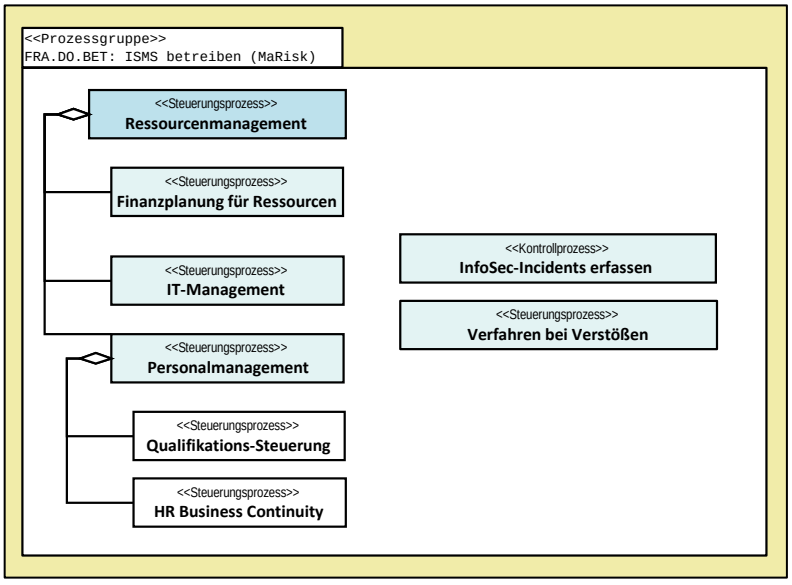

Abbildung 4.22: Prozessgruppe FRA.DO.BET[96]

Der *Betrieb des ISMS* ist vor allem durch die *Planung und Bereitstellung der notwendigen Ressourcen* geprägt. Zudem sind *Sicherheitsvorfälle zu behandeln* (Incident Management) und *Verfahren bei Verstößen* gegen Richtlinien durchzuführen.

[95] Quelle: eigene Darstellung
[96] Quelle: eigene Darstellung

FRA.CHK.AUD: Interne Audits (nach MaRisk, ISO/IEC 27001, COSO ERM)

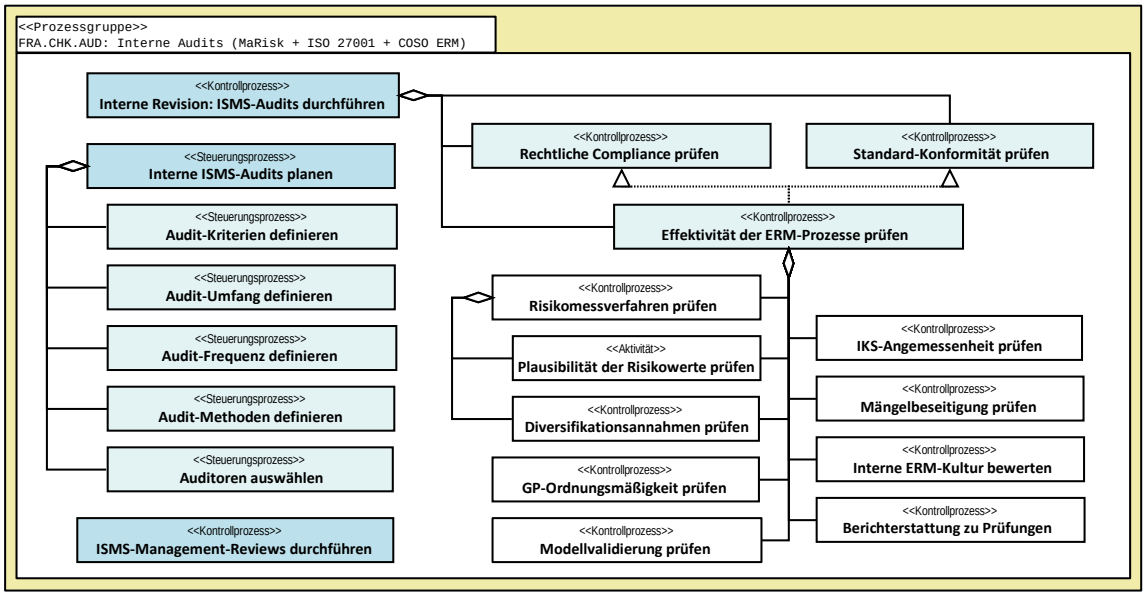

Abbildung 4.23: Prozessgruppe FRA.CHK.AUD[97]

Im Rahmen der *Check*-Phase des Deming-Kreislaufs ist das Informationssicherheits-Managementsystem zunächst regelmäßigen bzw. anlassbezogen Prüfungen zu unterziehen. Diese umfassen einerseits *interne Audits* durch die Abteilung der internen Revision, wobei die *rechtliche Compliance* des Risikomanagements, dessen *Konformität zu verwendeten Standards* sowie die *Effektivität deren Prozesse* geprüft wird. Andererseits hat das Management des Unternehmens regelmäßig eine davon unabhängige Prüfung der Risikomanagement-Systeme durchzuführen (*Management-Reviews*).

FRA.CHK.KON: Kontinuierliche Überwachung (nach ISO/IEC 27001, MaRisk)

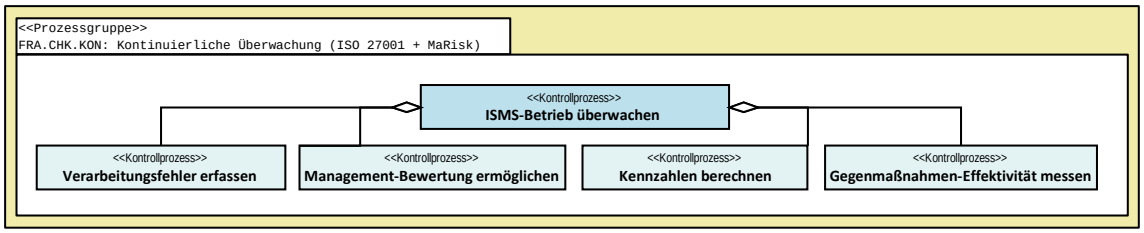

Abbildung 4.24: Prozessgruppe FRA.CHK.KON[98]

Als zweite Säule der internen Qualitätssicherung des Risikomanagement-Systems dient dessen *kontinuierliche Überwachung*, die die *Erfassung von Verarbeitungsfehlern* ebenso mit einschließt wie die *Berechnung von Kennzahlen* und die darauf aufbauende *Messung der Effektivität getroffener Verbesserungs- bzw. Gegenmaßnahmen* bei

[97] Quelle: eigene Darstellung
[98] Quelle: eigene Darstellung

entdeckten Mängeln. Die Informationen sind zudem derart aufzubereiten, dass eine effektive und effiziente *Bewertung des Systems durch die Management-Ebene* möglich ist.

FRA.ACT.VER: Verbesserung des ISMS (nach ISO/IEC 27001, Basel II)

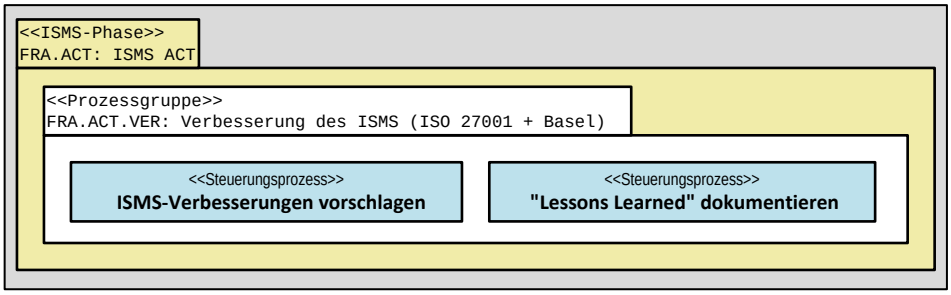

Abbildung 4.25: Prozessgruppe FRA.ACT.VER[99]

In der *Act*-Phase werden auf Basis der zuvor aggregierten Kennzahlen *Verbesserungsmöglichkeiten identifiziert*, konkrete *Verbesserungsmaßnahmen vorgeschlagen* sowie die *Lektionen dokumentiert*, die im aktuellen Durchlauf des Deming-Zyklus gelernt wurden. Diese Informationen bilden die Grundlage für die anschließende Plan-Phase des nächsten Durchlaufs im kontinuierlichen Verbesserungsprozess des Risikomanagement-Frameworks.

FRA.SUP.KOM: Kommunikation und Berichterstattung durchführen (nach ISO/IEC 27005, MaRisk, COSO ERM)

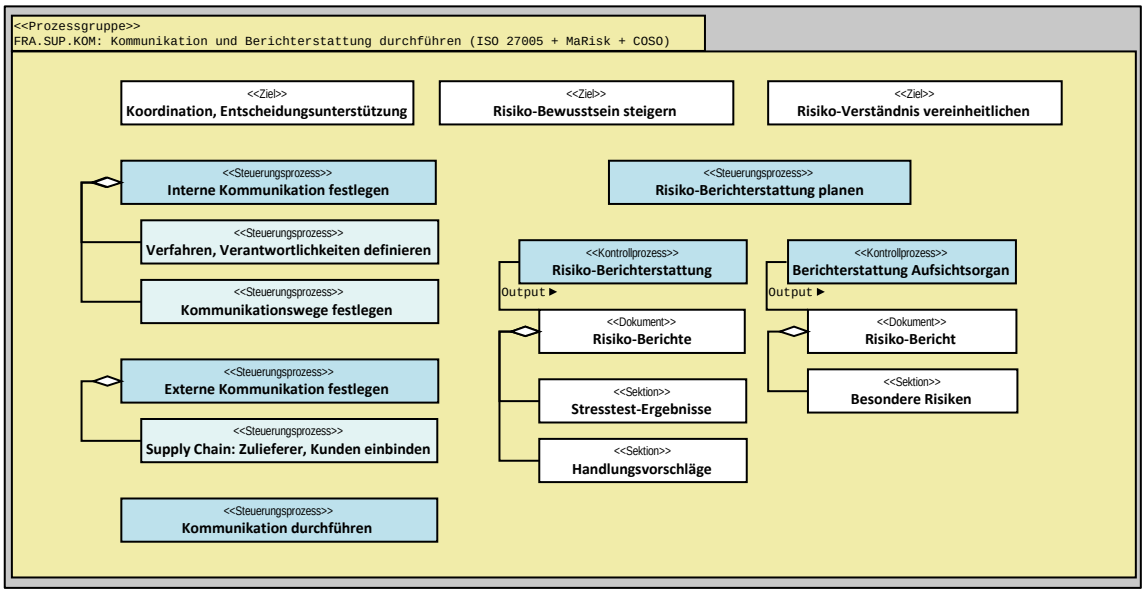

Abbildung 4.26: Prozessgruppe FRA.SUP.KOM[100]

[99] Quelle: eigene Darstellung

Kommunikation und Berichterstattung bilden einen wesentlichen Erfolgsfaktor über den gesamten Lebenszyklus von ISMS und Risikomanagement-Prozessen hinweg und wurden daher in den Kreis der drei unterstützenden Prozessgruppen aufgenommen. Dabei sind die *externe und interne Kommunikation* in Bezug auf *Verfahren, Verantwortlichkeiten und Kommunikationswege festzulegen* und die zugehörigen *Systeme zu betreiben*, um relevante Informationen zeitnah einholen, verarbeiten und verbreiten zu können.

Die *Berichterstattung* zum Thema Risikomanagement sollte die *Ergebnisse durchgeführter Stresstests* und *mögliche Handlungsvorschläge* enthalten, um beispielsweise als Basis für Management-Reviews dienen zu können. Die entsprechenden Informationen sollten in höher aggregierter Form auch den *Aufsichtsorganen* aktiv kommuniziert werden.

FRA.SUP.DOK: Dokumentation (nach ISO/IEC 27001, COSO ERM, MaRisk)

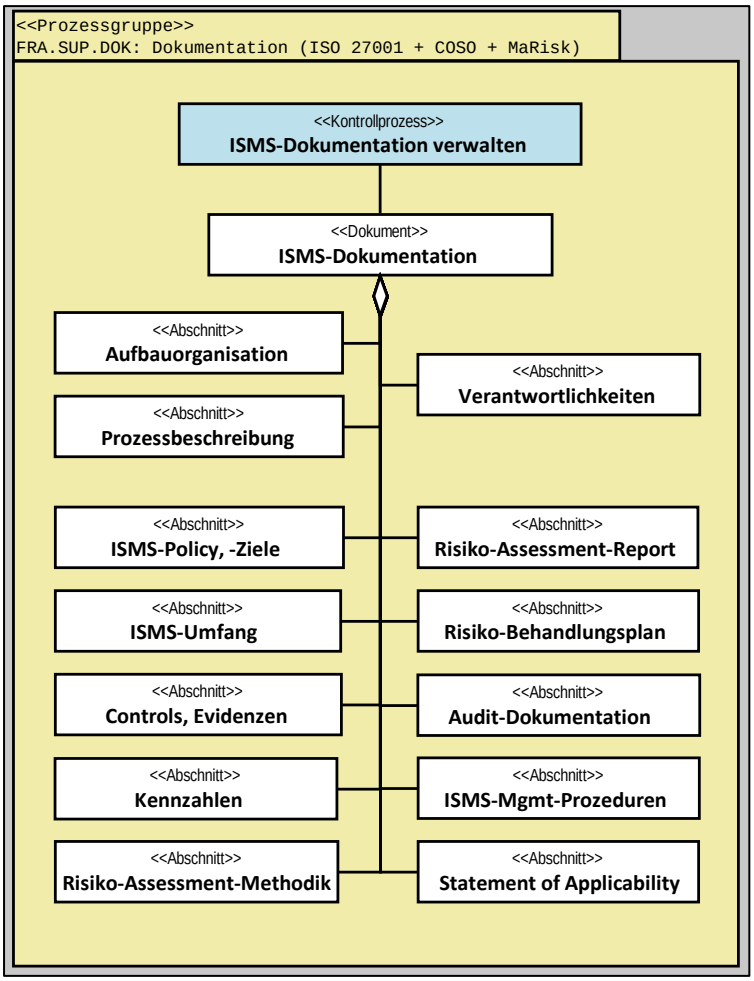

Abbildung 4.27: Prozessgruppe FRA.SUP.DOK[101]

[100] Quelle: eigene Darstellung
[101] Quelle: eigene Darstellung

Im Rahmen der *Dokumentation* sind sämtliche Informationen zum ISMS sowie den Risikomanagement-Prozessen für alle Interessensgruppen überblicksmäßig und detailliert festzuhalten. Dabei ist die *Aufbau- und Ablauforganisation* des Risikomanagements ebenso zu beschreiben wie *relevante Policies*, der *Aufbau der Kennzahlensysteme*, *Risikoassessment-Methoden* und *Risiko-Behandlungspläne*. Des Weiteren sind aktuelle und historische Daten aus dem laufenden Betrieb, wie *Evidenzen*, *Risiko-Berichte* oder *Audit-Ergebnisse*, in Roh- und aggregierter Form mit einzubeziehen.

FRA.SUP.INF: Informations- und Dokumentenmanagement (nach ISO/IEC 27001, BSI)

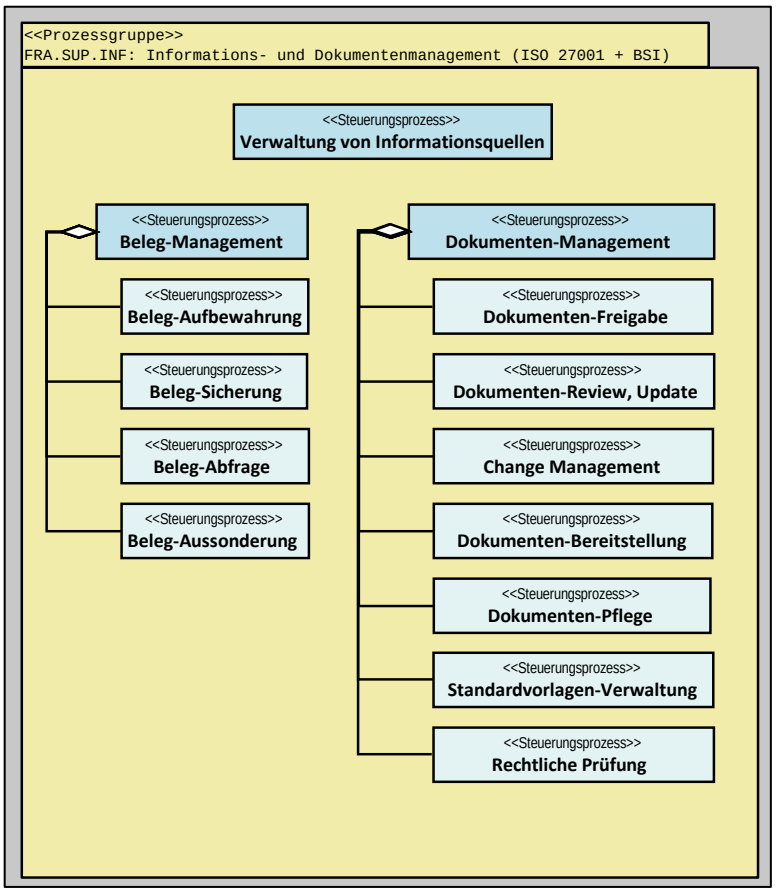

Abbildung 4.28: Prozessgruppe FRA.SUP.INF[102]

Um relevante Informationen für das ISMS und die Risikomanagement-Prozesse angemessen verwalten zu können, ist ein System zur *Verwaltung von Belegen* (Evidenzen) und *Dokumenten* einzusetzen, das deren Pflege über den gesamten Lebenszyklus hinweg sicherstellt. Außerdem sind die internen und externen *Informationsquellen sorgsam auszuwählen*, sodass die relevanten Informationskriterien im notwendigen Maße eingehalten werden können.

[102] Quelle: eigene Darstellung

PRO: Risikomanagement-Prozesse

Die Prozesse zum IT-bezogenen Risikomanagement enthalten die zentralen Abläufe aus den Bereichen der Kontextdefinition und des Risikoassessments, sowie der Evaluierung, Behandlung und Überwachung von Risiken.

PRO.KON: Kontext, Umfang und Abgrenzung definieren (nach ISO/IEC 27005)

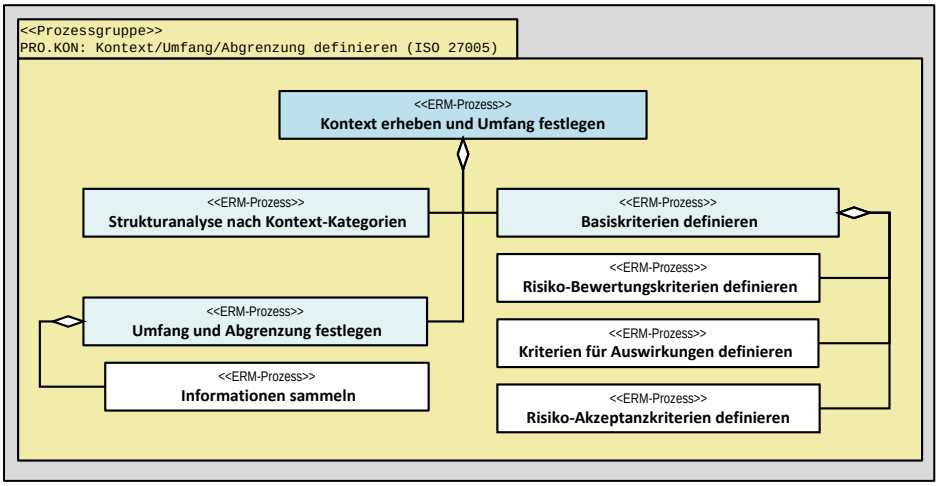

Abbildung 4.29: Prozessgruppe PRO.KON[103]

Im Rahmen der *Kontextdefinition* ist zunächst eine umfassende *Strukturanalyse* nach den ausgewählten Kontext-Kategorien (SBR.KOE, SBR.KOI) durchzuführen und in einem adäquaten Modell festzuhalten. Anhand dieses Modells ist abzugrenzen, welchen *Umfang* das Risikomanagement-System abdecken soll. Zudem sind diverse *Basiskriterien* festzulegen, die in den folgenden Schritten verwendet werden, wie jene für *Risikobewertung* und *Auswirkungen* (bspw. eine drei- oder fünfstufige qualitative Skala nach den Informationskriterien aus SBR.INF) oder Schwellenwerte zur *Risikoakzeptanz*.

PRO.AST.IDE: Risiken identifizieren und abschätzen (nach ISO/IEC 27005, BSI)

Die *Identifikation und Abschätzung von Risiken* bildet den Startpunkt zum *Risikoassessment*. Dabei sind vorab sämtliche relevanten *Assets* innerhalb des gewählten Umfangs sowie deren Beziehungen untereinander zu *identifizieren*, sowie in Bezug auf ihren Schutzbedarf zu *bewerten*. Hierfür sind entsprechende *Kategorien* zu bilden (bspw. eine vier- oder fünfstufige qualitative Skala von *niedrig* bis *sehr hoch*), die auch zur Gruppierung von Assets in klar abgegrenzte *Sicherheitszonen* herangezogen werden können.

[103] Quelle: eigene Darstellung

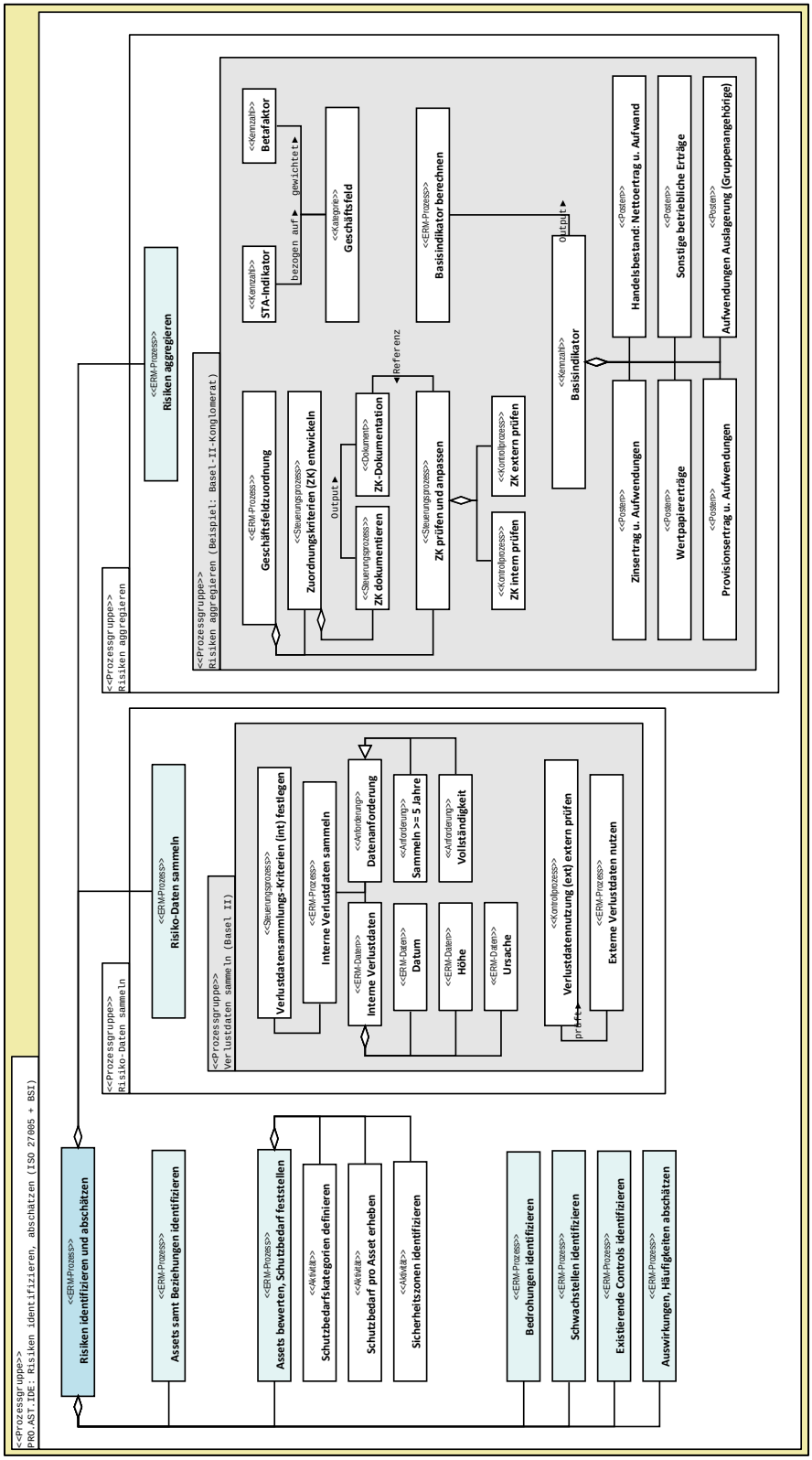

Abbildung 4.30: Prozessgruppe PRO.AST.IDE[104]

[104] Quelle: eigene Darstellung

Im nächsten Schritt werden relevante Bedrohungen identifiziert sowie jene Schwachstellen an den Assets erhoben, durch deren Ausnutzen diese Bedrohungen in der Lage sind, Risiken hervorzurufen. Da in den meisten Fällen im Unternehmen bereits Maßnahmen bestehen, um zumindest einen Teil dieser Risiken zu handhaben, werden diese im Hinblick auf eine reibungslose Integration des Risikomanagements mit bestehenden Ansätzen nun ebenfalls erhoben, und anschließend jene Häufigkeiten und mögliche Schweregrade der Auswirkungen geschätzt, die mit und ohne die existierenden Behandlungsmaßnahmen gelten (somit wird auch bereits die Effektivität der bestehenden Maßnahmen geschätzt bzw. erhoben).

Werden quantitative Daten für Schätzungen in Bezug auf Risiken verwendet, so sind die internen und externen Anforderungen an deren Qualität zu erheben und deren Einhaltung sicherzustellen, was im bestehenden Modell anhand des Beispiels von Basel II dargestellt wird. Hierbei ist zu beachten, dass in der Praxis qualitative Schätzungen in vielen Fällen zur Entwicklung einer effektiven Risikobehandlung bereits ausreichen, und die Verwendung von zu feingranularen Skalen die Gefahr birgt, eine in Wahrheit nicht vorhandene Messgenauigkeit zu suggerieren.

Bei der Verwendung von Wahrscheinlichkeitsverteilungen zur Abschätzung von Häufigkeiten sollten auch sogenannte *Long-Tail Risiken* beachtet werden – also Ereignisse, die zwar sehr selten eintreten, dann jedoch katastrophale Auswirkungen haben, wie etwa Erdbeben in wenig gefährdeten Gebieten oder schwere nukleare Unfälle (siehe bspw. [2, S. 166]).

Des Weiteren kann es notwendig sein, die Eigenschaften von Risiken nach bestimmten Kriterien zu aggregieren, wofür neuerlich auch externe Anforderungen gelten können, wie es das bestehende Modell wiederum anhand der Indikatorberechnung nach Basel II exemplarisch darstellt. Bei der Festlegung interner Richtlinien sollte ein pragmatischer Ansatz gewählt werden, um den Aggregationsmechanismus unmittelbar an die für die Kommunikation und Berichterstattung (FRA.SUP.KOM) notwendigen Granularitätsstufen anzupassen.

In jedem Fall ist darauf zu achten, dass im Rahmen des gewählten Umfangs sämtliche relevanten Risiken in die Aggregation aufgenommen werden, während Doppelzählungen zugleich zu vermeiden sind, da sowohl fehlende als auch mehrfach gezählte Risikodaten die jeweiligen Gesamtergebnisse massiv verfälschen und damit zu inadäquaten Lösungen zur Risikobehandlung führen können.

Eine Reihe von detaillierteren Beispielen für Risikobewertung und Aggregation findet sich unter anderem im informativen Anhang E der ISO/IEC 27005 [18, S. 47ff.], während die internationale Norm ISO/IEC 31010 verschiedene Methoden zum Risikoassessment beschreibt. [68]

PRO.AST.EVA/STR: Risiken evaluieren (nach ISO/IEC 27005, Risk IT, MaRisk), Stresstests (nach MaRisk)

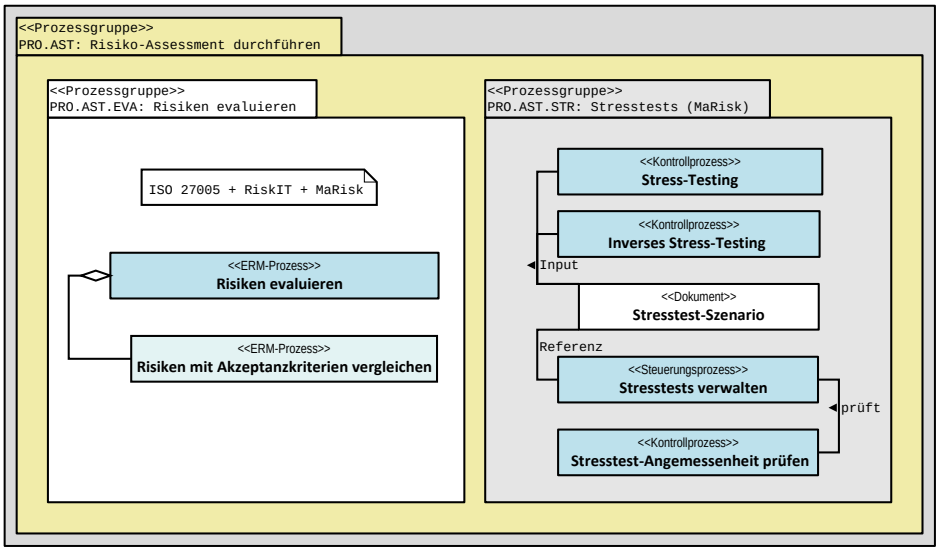

Abbildung 4.31: Prozessgruppen PRO.AST.EVA, PRO.AST.STR[105]

Die an die Identifikation und Abschätzung anschließende Evaluierung von Risiken hat zum Ziel, die Notwendigkeit einer expliziten Risikobehandlung festzustellen, indem die *Risikohöhen mit den zuvor festgelegten Akzeptanzkriterien verglichen* werden. Ein mögliches Mittel für die Abschätzung und Evaluierung von Risiken stellen szenariobasierte *Stresstests* dar, wie sie unter anderem in der MaRisk [27, S. AT4.3.3] und dem Standard Risk IT beschrieben werden [17, S. 24ff.], [38, S. 51ff.].

PRO.BEH/AKZ: Risiken behandeln (nach ISO/IEC 27001, ISO/IEC 27005, Basel II, COSO ERM), Restrisiken akzeptieren (nach ISO/IEC 27005)

Zur *Risikobehandlung* stehen Maßnahmen aus vier grundlegenden Kategorien zur Verfügung, die in praktisch allen untersuchten Quellkomponenten beschrieben werden und in der Lage sind, Einfluss auf Bedrohungen, Schwachstellen oder die Höhe möglicher Schadensauswirkungen zu nehmen:

Die *Minderung* von Risiken durch Abschwächung ihrer Auswirkungen oder Verringerung ihrer Häufigkeit (bspw. die Einführung von Feuerlöschanlagen oder der Bau mit feuerfesten Materialien), die *Übernahme* von Risiken ohne aktive Behandlung, die *Vermeidung* von Risiken (bspw. durch die Aufgabe von bestimmten Märkten) oder die *Verlagerung* von Risiken (im Allgemeinen über Versicherungen). Werden Risiken ohne Behandlung übernommen, sollte dies formal festgehalten und die Risikosituation in weiterer Folge nicht ignoriert, sondern genau beobachtet werden, um bei Bedarf zusätzliche Maßnahmen treffen zu können.

[105] Quelle: eigene Darstellung

Die verschiedenen Behandlungsoptionen sind – beispielsweise anhand der in Abbildung 4.32 dargestellten Kriterien – zu *bewerten*, *auszuwählen* und nach deren Dringlichkeit zu *priorisieren*, wonach ein *Risiko-Behandlungsplan erstellt* und *umgesetzt* wird.

Da die Behandlung von Risiken in der Praxis im Allgemeinen einen Kompromiss aus Effektivität und Wirtschaftlichkeit (Kosteneffizienz) darstellt, verbleiben auch nach dieser Behandlung *Restrisiken* (vgl. auch SBR.IKS), die seitens der Management-Ebene *formal akzeptiert* werden sollten (PRO.AKZ).

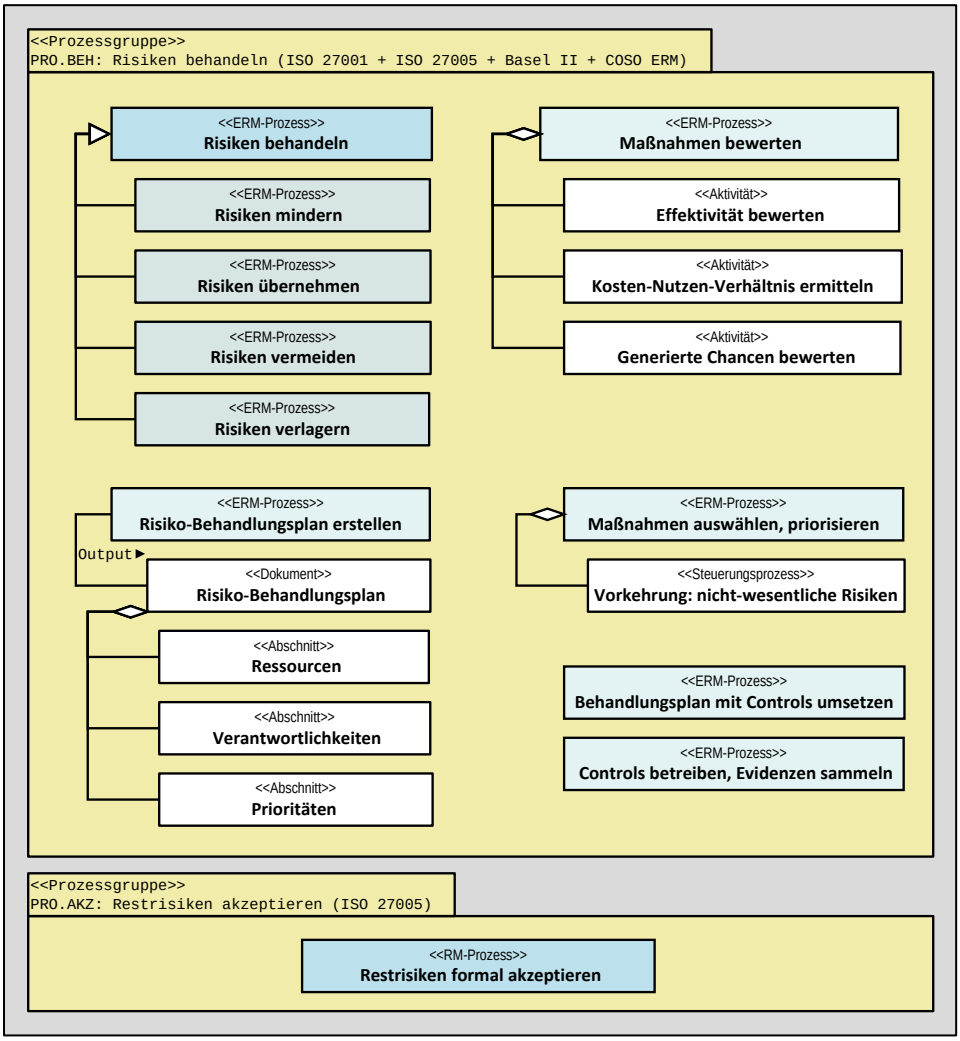

Abbildung 4.32: Prozessgruppen PRO.BEH, PRO.AKZ[106]

[106] Quelle: eigene Darstellung

PRO.MON: Risiken überwachen (nach ISO/IEC 27001, MaRisk, Risk IT)

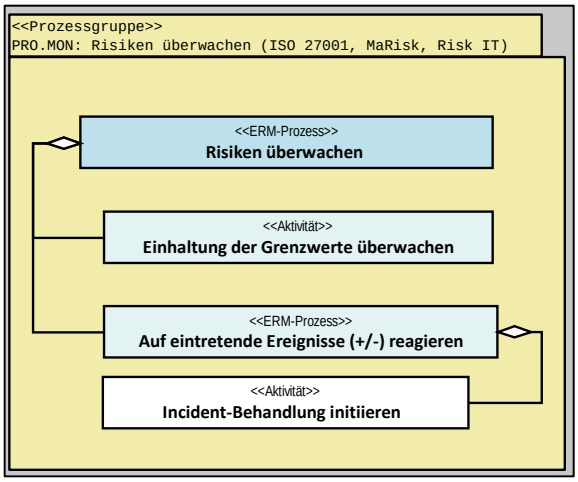

Abbildung 4.33: Prozessgruppe PRO.MON[107]

Wurde das Risikoassessment durchgeführt, die Risikobehandlung geplant und die entsprechenden Implementierungsprojekte erfolgreich umgesetzt, verbleibt die *kontinuierliche Überwachung* der Risikosituation als primäre Aufgabe bis zum Beginn des nächsten Prozessdurchlaufs. Dabei ist die *Einhaltung der definierten Grenzwerte für Risiken sicherzustellen* und bei Bedarf *auf Ereignisse zu reagieren*, wie es im Rahmen des Risikobehandlungsplans vorgesehen wurde. Werden diese Grenzwerte wiederholt überschritten, deutet dies zunächst auf eine unzureichende Risikobehandlung hin, worauf ein neuer Prozessdurchlauf (beginnend mit PRO.KON) angestoßen werden sollte.

Lassen sich die bestehenden Probleme durch diese Vorgehensweise nicht lösen, ist eine Eskalation zur Überwachungs- bzw. Verbesserungsphase des Risikomanagement-Frameworks (FRA.CHK, FRA.ACT) vorzunehmen, da in diesem Fall eine Anpassung der Risikomanagement-Prozesse selbst oder auch des Frameworks vonnöten sein könnte.

[107] Quelle: eigene Darstellung

4.2.3 Vereinheitlichtes Prozessmodell

Im vorherigen Abschnitt wurden Struktur und Inhalt des harmonisierten Integrationsmodells anhand einer statischen, hierarchiegebundenen Betrachtung diskutiert. Da dynamisch ablaufende Prozesse einen wesentlichen Teil des Integrationsmodells bilden, liegt es zudem nahe, die zuvor beschriebenen Konzepte in ein Prozessmodell überzuführen, das im Folgenden vorgestellt wird.

Vereinheitlichtes Prozessmodell – vereinfachte Darstellung

Abbildung 4.34 zeigt das im Rahmen der vorliegenden Arbeit erstellte Prozessmodell in überblicksmäßiger Form. Dabei bildet das Framework (FRA), das ein Informationssicherheits-Managementsystem definiert, den Rahmen für den Aufbau und den Betrieb eines unternehmensweit einheitlichen, integrierten Risikomanagement-Systems, und stellt über den aus vier Phasen bestehenden Deming-Kreislauf einen kontinuierlichen Verbesserungsprozess bereit.

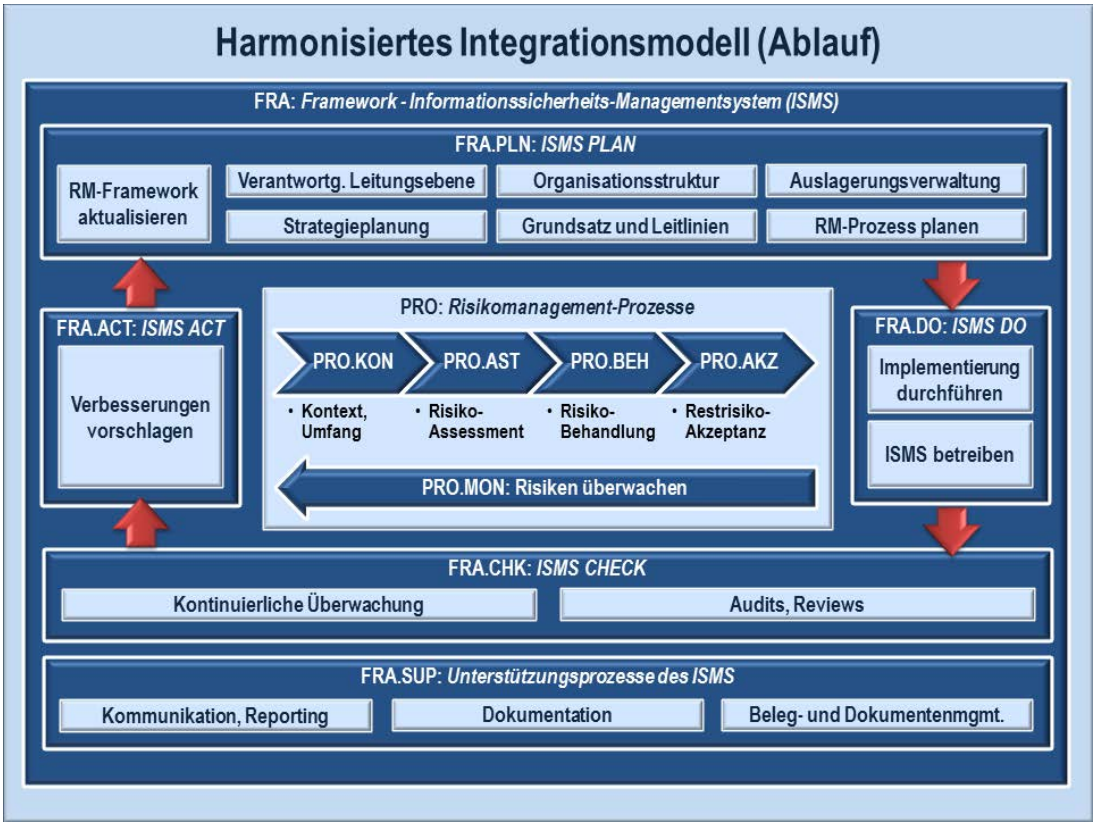

Abbildung 4.34: Harmonisiertes Integrationsmodell (Ablauf, vereinfacht)[108]

Der in der Plan-Phase des Frameworks (FRA.PLN) erarbeitete und im vorigen Abschnitt detailliert beschriebene Risikomanagement-Prozess (PRO) wird als zentrale Komponente in der Mitte der Grafik dargestellt, während die Unterstützungsprozesse im unteren Teil gezeigt werden.

[108] Quelle: eigene Darstellung

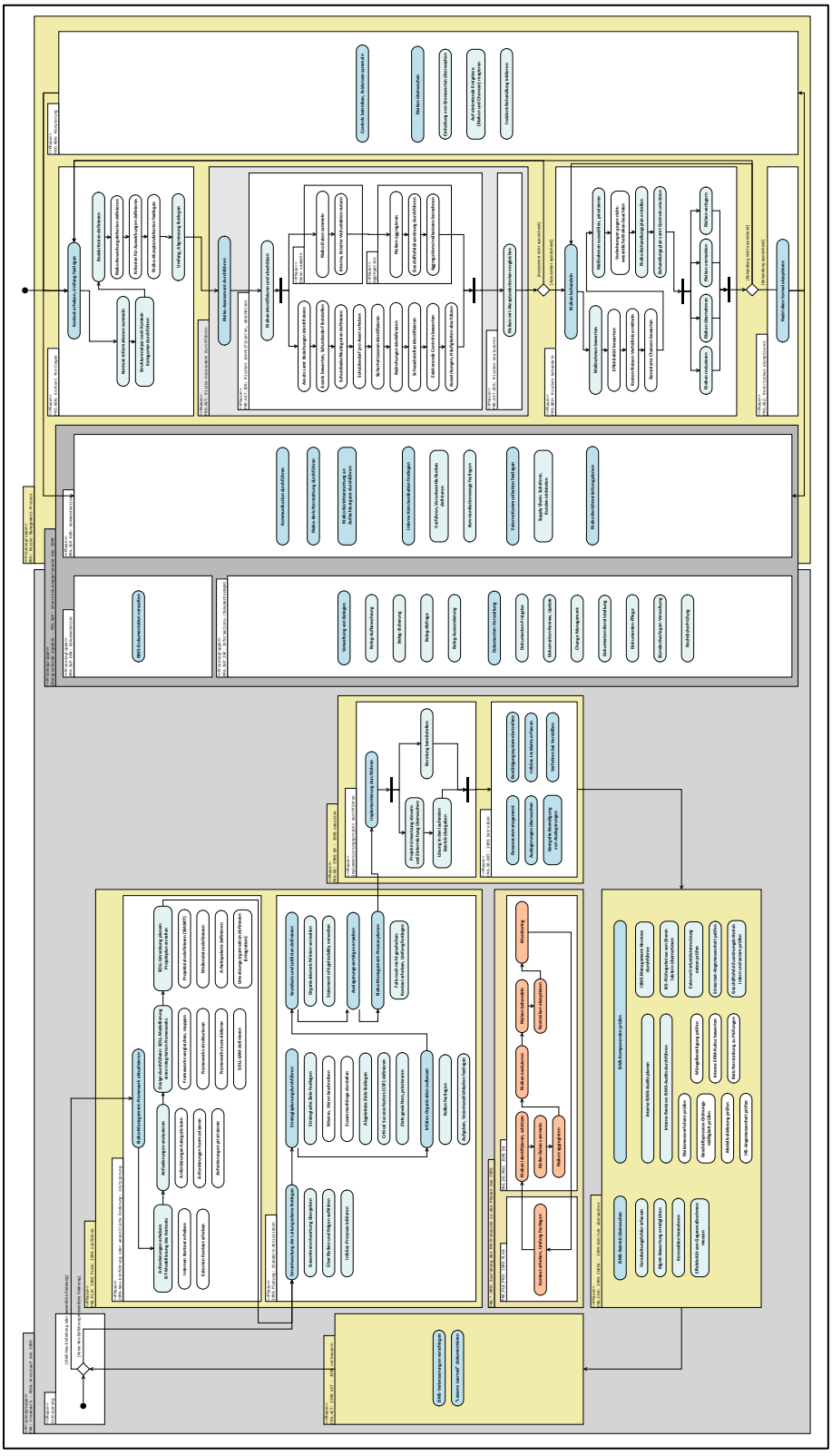

Abbildung 4.35: Harmonisiertes Integrationsmodell (Ablauf, vollständig)[109]

[109] Quelle: eigene Darstellung

Vereinheitlichtes Prozessmodell – vollständige Darstellung

Eine detaillierte Darstellung des harmonisierten Prozessmodells mit entsprechendem Kontrollfluss ist in Abbildung 4.35 enthalten, die syntaktisch an den Modelltyp *Aktivitätsdiagramm* der Unified Modeling Language angelehnt ist.[110]

In der Initiierungsphase ist zunächst festzustellen, ob eine Neu-Einführung oder wesentliche Änderung am Framework vorzunehmen ist. Wenn dies der Fall ist, wird der obere Teil der FRA.PLN-Phase durchlaufen, der zudem die Verbindung des Ablaufmodells mit der für die vorliegende Arbeit angewandten Vorgehensweise zeigt: Diese findet sich als Aktivität mit der Bezeichnung *Design durchführen: SOLL-Modellierung eines Integrierten Frameworks* unter dem Punkt *Risikomanagement-Framework aktualisieren*.

Wurde das Framework soeben oder bereits in einem früheren Phasendurchlauf entwickelt und bedarf keiner weiteren Anpassung, werden die Standard-Aktivitäten der Plan-Phase (FRA.PLN) abgearbeitet. In jedem Fall werden sämtliche Änderungen anschließend im Rahmen eines Implementierungsprojekts umgesetzt und das ISMS betrieben (FRA.DO).

Treten in der nun folgenden Check-Phase (FRA.CHK) wesentliche Mängel auf, oder ist eine zuvor festgelegte Zeitspanne abgelaufen, werden die durch Überwachung und Prüfung identifizierten Verbesserungspotenziale in der Act-Phase (FRA.ACT) zusammengefasst und konkrete Verbesserungsmaßnahmen vorgeschlagen, die als Grundlage für die Planungsphase eines weiteren Durchlaufs des Deming-Zyklus dienen. Hierdurch werden Framework und Risikomanagement-Prozesse auf iterativ-inkrementelle Art und Weise kontinuierlich aktualisiert und verbessert.

Sobald das Framework in den laufenden Betrieb übernommen wird, kann zudem das Risikoassessment (PRO.AST.*) beginnen und somit der Risikomanagement-Prozess anlaufen, der durch das Framework verwaltet wird.

[110] Da sich viele Teilprozesse nicht in eine direkte Reihenfolgebeziehung bringen lassen, fehlen in der Abbildung Teile des Kontrollflusses. Es handelt sich daher um kein formal/methodisch korrektes UML-Diagramm.

Kapitel 5: Evaluierung und kritische Betrachtung

Im Zuge der Evaluierung findet zunächst eine kritische Würdigung der vorliegenden Arbeit aus dem wissenschaftstheoretischen Blickwinkel statt, wonach die Erfüllung der zuvor gestellten Anforderungen diskutiert wird.

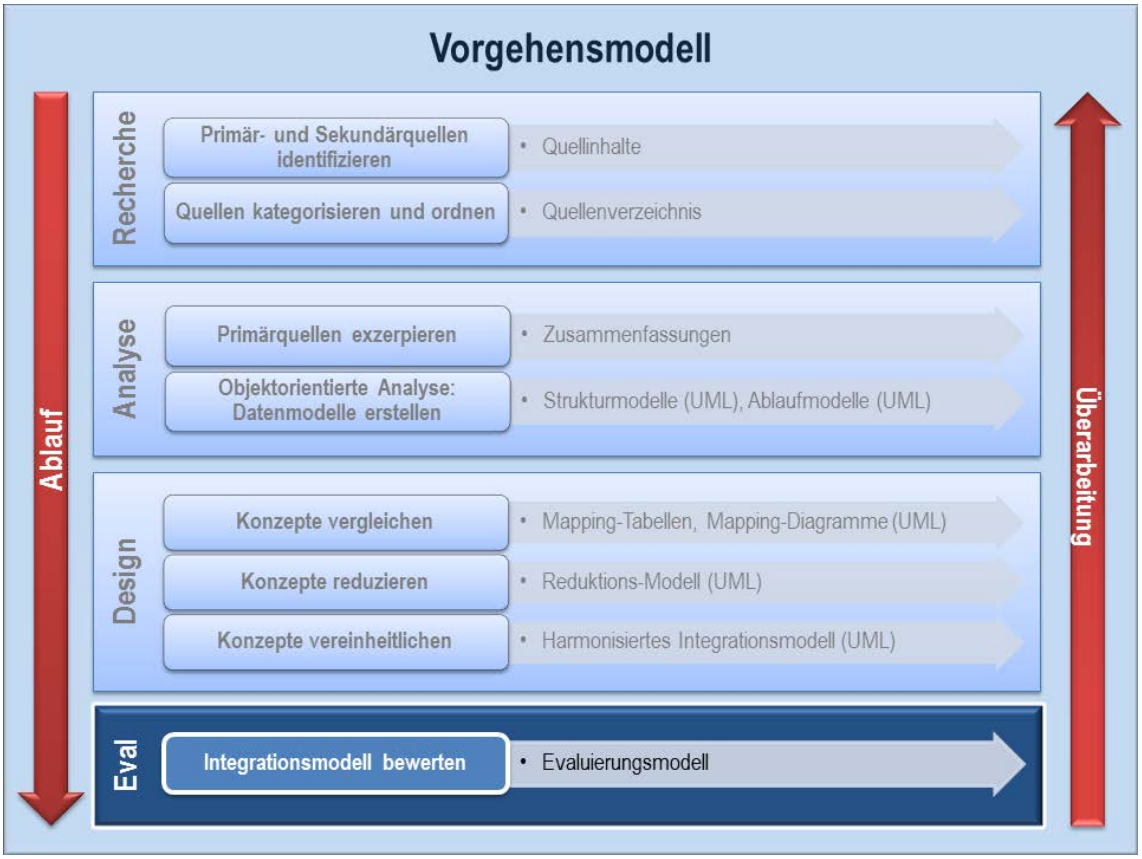

Abbildung 5.1: Vorgehensmodell: Evaluierungsphase[111]

5.1 Wissenschaftstheoretischer Kontext

Wie in Abschnitt 1.3 gezeigt, stellt eine Modellbildung eine verkürzende, pragmatische Abbildung eines Originals dar, also eine vereinfachte Darstellung von Zusammenhängen, die einem klar definierten Zweck dient, sowie zu einer bestimmten Zeit für einen bestimmten Benutzerkreis erstellt wurde. [28]

Aus dieser Tatsache ergibt sich zwangsweise der Verlust von Details im Vergleich zum Original, da nur für den Modellierungszweck wesentliche Zusammenhänge in das

[111] Quelle: eigene Darstellung

Modell übernommen werden. [28] Dies besitzt für die vorliegende Arbeit zunächst insofern Bedeutung, als nicht ausgeschlossen werden kann, dass von relevanten Details abstrahiert wird, die der Leser der Arbeit zu deren Verständnis benötigen würde, die für den Autor aufgrund der eingehenden Beschäftigung mit dem behandelten Themenkomplex jedoch klar erscheinen.

Diese Problematik verschärft sich im konkreten Fall aufgrund der Tatsache, dass durch die Verwendung von Good-Practice-Frameworks und Standards ebenfalls Modelle als gegebene Axiome dienen, die selbst das Ergebnis ähnlicher Abstraktionsprozesse darstellen. Im Rahmen der vorliegenden Arbeit wurde versucht, dieser Problematik durch die Anwendung einer möglichst vollständig dokumentierten und transparenten Vorgehensweise zu begegnen, und so direkten Zugang zu den verwendeten Abschnitten aus den Quellkomponenten zu schaffen, um es dem Leser zu ermöglichen, bei Bedarf Informationen auf feineren Granularitätsstufen einholen zu können.

Des Weiteren unterliegt jede Modellierung inhärent der sogenannten Induktionsproblematik, also der Tatsache, dass – nach David Hume [29] bzw. Sir Karl Popper [30] – Schlüsse aus einer beobachteten Stichprobe auf eine Grundgesamtheit (hier: die Grundgesamtheit der IT- und Unternehmensprozesse) niemals endgültig verifiziert, dafür jedoch prinzipiell anhand eines einzigen Gegenbeispiels umso leichter falsifiziert werden können.

Ein derartiger Falsifikationsversuch fand für die vorliegende Arbeit im Rahmen eines Peer-Reviews mit einem Experten aus dem Bereich des IT-Risikomanagements[112] statt, bei dem Verbesserungen an Details diskutiert und in die vorliegenden Ergebnisse eingearbeitet wurden. Eine Falsifikation konnte nicht erbracht werden, was im Sinne des kritischen Rationalismus als eine Verifikation in einer ersten Iteration zu betrachten ist.

Diese Verifikation des Integrationsmodells kann durch den Einsatz im Rahmen von Praxisprojekten weitergeführt werden, wobei bei Bedarf durch die zyklische Natur des Frameworks dessen Komponenten angepasst werden können.

[112] DDr. Alexander Hampel ist zur Zeit der Verfassung dieser Arbeit seit mehr als sechs Jahren auf dem Gebiet des IT-Risikomanagements tätig und stand für ein Peer-Review im Umfang von insgesamt zwölf Arbeitsstunden zur Verfügung.

5.2 Erfüllung spezifischer Anforderungen und Mehrwert der Arbeit

In Abschnitt 1.1.3 wurde die Notwendigkeit aufgezeigt, eine klar definierte, über das gesamte Unternehmen hinweg einheitlich strukturierte Vorgehensweise zu entwickeln, die von der Geschäftsebene getrieben ist und Auslagerungen bzw. interorganisationale Geschäftsprozesse berücksichtigt. Diese sollte sämtliche relevanten Rahmenwerke, Standards und Regelungen identifizieren, integrieren und aufeinander abstimmen, und somit ein effektives und wirtschaftliches Risikomanagement zu schaffen.

Die vorliegende Arbeit ging dabei der Frage nach, inwieweit eine derartige Harmonisierung möglich sei und fokussierte dabei auf den Einsatz und die Auslagerung von Diensten der Informationstechnologie (IT-Risikomanagement).

Darauf aufbauend wurde eine Reihe von Anforderungen an das Integrationsmodell gestellt, deren Erfüllung nun zur Diskussion steht:

- Das Modell sollte als idealtypischer Risikomanagement-Ansatz geeignet sein, der Konzepte aus verschiedenen Quellkomponenten vereinheitlicht und einen großen Umfang besitzt.

- Das vorgestellte IT-Risikomanagementsystem sollte mit den bestehenden Ansätzen des betrieblichen Risikomanagements (Enterprise Risk Management, ERM) integrierbar sein und Veränderungen in seinen Quellkomponenten ohne unverhältnismäßig hohen Aufwand integrieren können.

- Die Quellkomponenten sollten zur Nachverfolgbarkeit im Sinne der Transparenz und möglicher Zertifizierungen durchgängig identifizierbar bleiben.

- Outsourcing sollte umfassend betrachtet werden, da Auslagerungen in der Praxis eine enorme Verbreitung erfahren haben.

5.2.1 Eignung als idealtypischer Risikomanagement-Ansatz

Um die inhaltliche Eignung als idealtypischer Risikomanagement-Ansatz zu beurteilen, wurden die Inhalte des harmonisierten Integrationsmodells in die aus Abschnitt 4.1.1 bekannte Tabelle zur Zusammenfassung des Mappings der Quellkomponenten übernommen (Tabelle 5.1). Hierbei zeigt sich, dass das für diese Arbeit erstellte Integrationsmodell mit 47 Punkten tatsächlich einen weitaus höheren Abdeckungsgrad aufweist als sämtliche einzelnen Quellkomponenten.

Evaluierung des harmonisierten Gesamtmodells

		Komponente												
#	Strukturierungspunkt	Gesamtmodell	Basel II	SolvV	KWG	MaRisk	ISO 27001	ISO 27005	ISO 31000	BSI Standards	COSO ERM	Risk IT	SOX & ISACA	*Summe*
A	Begriffe													
A.1	Risiken	2	1	1	1	1	1	2	2	2	2	2	0	15
A.2	Ereignisse	1	0	0	0	0	1	1	1	1	2	2	0	8
A.3	Gefährdungen, Bedrohungen, Schwachstellen	1	1	1	0	0	1	2	1	2	0	1	0	9
A.4	Assets und Wert	2	0	0	0	0	2	2	1	2	0	2	0	9
A.5	Informationssicherheit	2	0	0	0	1	2	0	0	2	1	1	0	7
A.6	ERM-Struktur	2	0	0	0	0	0	0	0	0	2	2	0	4
A.7	Kontroll- und Steuerungsmaßnahmen	2	1	1	1	1	1	1	1	1	1	2	1	12
A.8	Kontext	2	1	1	0	0	0	2	1	0	0	0	0	5
A.9	Risikomanagement-Prinzipien, Zielsetzungen	0	0	0	0	0	0	0	2	0	0	1	0	3
A.10	Reifegrade	2	0	0	0	0	0	0	0	0	0	2	0	2
B	Management-System													
B.1	Systemdefinition	2	1	1	1	2	1	0	1	2	2	2	2	15
B.2	Ressourcenmanagement	1	1	1	1	2	1	1	1	1	0	1	0	10
B.3	Kommunikation und Berichterstattung	2	1	1	1	2	0	1	1	1	1	1	1	11
B.4	Notfallmananagement	0	0	0	1	1	0	0	0	2	0	0	0	4
B.5	Risikomanagement bei neuen Produkten/Märkten	0	0	0	0	2	0	0	0	0	0	0	0	2
B.6	Auslagerungen	2	0	0	1	2	0	0	0	0	0	0	0	3
B.7	Verantwortung und Leitungsebene	1	1	1	1	1	1	0	1	1	1	1	1	10
B.8	Strategieplanung	2	1	1	1	2	1	1	1	1	2	2	1	14
B.9	Organisationsstruktur	2	0	1	0	2	0	2	1	2	2	1	0	11
B.10	Kontext, Umfang und Abgrenzung	2	0	0	0	0	0	2	1	2	0	1	0	6
B.11	Dokumentation	2	1	1	0	2	2	0	1	1	1	0	1	10
B.12	Grundsatz und Leitlinien	2	1	1	0	2	2	0	1	1	1	1	1	11
B.13	Informations- und Dokumentenmanagement	2	0	0	0	1	2	1	1	1	0	0	0	6
B.14	Einführung des Management-Systems	1	0	0	0	0	0	0	1	2	1	1	1	6
B.15	Überwachung, Prüfung und Optimierung	2	1	1	1	2	2	1	1	2	2	1	1	15
C	Risiko-Management-Kreislauf													
C.1	Prozessdefinition	2	1	1	1	1	2	2	1	1	2	2	1	15
C.2	Risiko-Assessment	2	1	1	1	1	1	2	1	1	2	2	1	14
C.3	Risiko-Überwachung	2	1	1	1	1	2	1	1	1	1	1	0	11
C.4	Risiko-Behandlung	2	1	1	1	1	1	2	1	1	1	2	1	13
	Summe (Gesamtmodell)	47												
	Summe (Quellkomponenten)		16	17	14	30	26	26	25	33	27	34	13	

Legende	
0	nicht vorhanden
1	geringe Detaillierung
2	hohe Detaillierung

Tabelle 5.1: Evaluierung des harmonisierten Integrationsmodells[113]

[113] Quelle: eigene Darstellung

5.2.2 Integration mit bestehenden ERM-Ansätzen und Flexibilität bei Veränderungen der Quellkomponenten

Diese Anforderungen werden durch das entworfene Integrationsmodell auf mehreren Ebenen unterstützt:

- Der Aufbau des Integrationsmodells orientiert sich am weit verbreiteten Informationssicherheits-Managementsystem (ISMS) aus der internationalen Norm ISO/IEC 27001 und berücksichtigt die Inhalte weiterer praxisrelevanter Frameworks wie COSO ERM. Dies erleichtert einerseits die Integration, wenn ähnlich strukturierte Ansätze verwendet werden; andererseits erlaubt der zyklische Ansatz eine wiederholte Überarbeitung bei Änderungen an den Quellkomponenten.

- Im Rahmen der Entwurfsphase des Frameworks (FRA.PLN) wird unter anderem der interne Kontext im Unternehmen erhoben, zu dem auch bestehende ERM-Systeme zu zählen sind. Über die anschließende Anforderungsanalyse und die Designphase können eine Zusammenführung mit diesen Ansätzen erreicht sowie veränderte Quellkomponenten eingearbeitet werden.

5.2.3 Identifikationsmöglichkeit der Quellkomponenten

Auf diese wurde beim Entwurf des Integrationsmodells durchgängig großes Augenmerk gelegt, wobei in der Phase des Mappings sowie der Reduktion durch das Konzept der *Integrationspakete* eine direkte Zuordnung zu den jeweiligen Quellkomponenten sichergestellt wurde. Da im Verlauf des finalen Harmonisierungsschritts die Quellkonzepte stark vereinheitlicht werden mussten, um ein homogenes Gesamtmodell erstellen zu können, wurde die Nachverfolgbarkeit ab diesem Punkt zwar eingeschränkt, sie bleibt jedoch durchgängig vorhanden.

Im Integrationsmodell wird daher für jede Begriffsgruppe angegeben, aus welchen Quell-Frameworks sie gebildet wurde. Für eine detaillierte Zuordnung ist im Reduktionsmodell sowie den Mapping-Tabellen nachzuschlagen, die auch auf die jeweilig verwendeten Kapitel der Quellkomponenten verweisen.

Das damit erreichte Niveau an Transparenz stellt vor allem im wissenschaftlichen Sinne einen wesentlichen Vorteil der vorliegenden Arbeit im Vergleich zu bestehenden Literaturquellen dar.

5.2.4 Betrachtung von Outsourcing

Trotz der in Kapitel 1.2.4 gezeigten enormen Wichtigkeit von Outsourcing im praktischen IT-Betrieb werden Auslagerungen lediglich im Rahmen des Basel-II-Konglomerats überblicksmäßig behandelt; der zugehörige Abschnitt der MaRisk [27, S. AT9] bildet praktisch die alleinige Basis für die Prozessgruppe *Auslagerungen verwalten* (FRA.PLN.ALU), spezifiziert jedoch zum Großteil lediglich Anforderungen an die Gestaltung des Auslagerungsvertrags.[114]

Für eine detailliertere Betrachtung von Outsourcing sei auf die Inhalte der *IT Infrastructure Library* (*ITIL*) sowie das Dokument *Outsourcing in Financial Services* des Baseler Komitees für Bankenaufsicht verwiesen, das neun *Guiding Principles* zu diesem Thema definiert. [69]

[114] Der IDS PS 951 wird in der zugehörigen Prozessgruppe zwar erwähnt, steuert aber lediglich das Element *IKS-Prüfergebnisse sichten* zum Gesamtmodell bei und besitzt damit im Vergleich zu MaRisk AT9 geringe Relevanz

Kapitel 6: Zusammenfassung und Schlussfolgerung

Dieses finale Kapitel fasst die zuvor präsentierten Inhalte zusammen, zieht die notwendigen Schlüsse und wirft zusätzliche Fragestellungen auf, deren Erörterung Teile weiterführender Forschung bilden können.

6.1 Zusammenfassung

Die vorliegende Arbeit stellte ein Integrationsmodell zur Harmonisierung des Risikomanagements für den Einsatz und das Outsourcing von Informationstechnologie vor. Dabei wurden im Rahmen einer umfassenden Recherche zunächst jene Primärquellen identifiziert, die als Quellkomponenten für das zu erstellende Modell dienen sollten. Nach deren textueller Zusammenfassung erfolgte eine objektorientierte Analyse der Quellkomponenten auf struktureller und inhaltlicher Ebene, die durch die Erstellung von 14 Strukturmodellen mit rund 3.300 Entitäten sowie einer Reihe von Ablaufmodellen in der Syntax der Unified Modeling Language (UML) verwirklicht wurde.

In der anschließenden Design-Phase wurden die zuvor ermittelten Konzepte anhand eines Mapping-Modells gegenübergestellt und im Hinblick auf ihre Eignung zur weiteren Integration bewertet. Mittels Bildung von *Integrationspaketen* aus den gewählten Konzepten konnte die Nachverfolgbarkeit sichergestellt werden.

Durch die Reduktion und Zusammenfassung dieser Pakete wurde im nächsten Schritt ein harmonisiertes Integrationsmodell erarbeitet, welches Begriffs- und Prozessgruppen als UML-Klassen- und Aktivitätsdiagramme definiert, um ein unternehmensweit einheitliches und effektives Risikomanagement-System für den Einsatz und die Auslagerung von Diensten der Informationstechnologie über dessen gesamten Lebenszyklus hinweg betreiben zu können.

Neben einer Evaluierung des Integrationsmodells im Hinblick auf die Erfüllung der geltenden Anforderungen fand letztendlich eine Validierung im Rahmen eines Peer-Reviews statt, bei dem ein Falsifikationsversuch im Sinne des kritischen Rationalismus durchgeführt wurde.

6.2 Schlussfolgerungen

Während der Erstellung der vorliegenden Arbeit wurde offensichtlich, dass die gestellte Forschungsfrage eindeutig dahingehend beantwortet werden kann, dass die geforderte Harmonisierung zu weiten Teilen möglich ist und – wie in Abschnitt 5.2 gezeigt wurde – ein Integrationsmodell schafft, das über den Umfang aller einzelnen Quellkomponenten hinausgeht, hohe Flexibilität besitzt und für die eingeflossenen Komponenten die Nachverfolgbarkeit in akzeptabler Art und Weise gewährleistet.

Allerdings ist mit einer derartigen Integration ein hoher Aufwand verbunden, der sowohl mit steigendem Detaillierungsgrad als auch mit der Zahl der Quellkomponenten deutlich überlinear – und beispielsweise im Falle eines vollständigen Mappings „von jeder zu jeder Komponente“ in der Designphase sogar quadratisch – wächst.

So wurden im Rahmen der objektorientierten Analyse für die vorliegende Arbeit vom Autor in einem Zeitraum von rund sechs Monaten über 3.300 UML-Klassen in 14 Klassendiagrammen erstellt, im Mapping-Modell zu den Risikomanagement-Standards rund 240 Konzepte miteinander verglichen und für die Abstimmung der IT Governance Frameworks eine knapp 1.000 Zeilen große Vergleichstabelle erstellt.

Dieser beträchtliche Aufwand könnte Teil einer Erklärung für die Tatsache sein, dass zurzeit nur eine geringe Zahl vergleichbarer Werke zum Thema IT-Risikomanagement existiert (siehe Abschnitt 1.4).

6.3 Weiterführende Fragestellungen

Trotz des großen Umfangs des harmonisierten Integrationsmodells existiert eine Reihe an Themenbereichen, deren Behandlung zwar wünschenswert wäre, im Rahmen dieser Masterarbeit jedoch nicht realisiert werden konnte:

- Wie bereits erwähnt, sollte **Outsourcing** aufgrund dessen enormer Bedeutung in der Praxis eingehender behandelt werden. Die vorliegende Arbeit verweist dazu lediglich auf die MaRisk sowie das Dokument *Outsourcing in Financial Services* des Baseler Komitees für Bankenaufsicht. [69]

- Das Thema **Notfallmanagement** wurde aus dem Kreis der Quellkomponenten lediglich vom BSI-Standard 100-4 abgedeckt. Dieser wurde zwar analysiert, jedoch nicht in das Integrationsmodell übernommen, da zum Thema Business Continuity Management weitere Normen und Standards existieren, die bei einer fundierten Modellbildung gemeinsam betrachtet werden sollten. Dazu zählen beispielsweise die internationale Norm *ISO/IEC 27031* [70] oder der britische Standard *BS 25999*. [71] Da dieser Themenkreis unmittelbar an jenen des Risikomanagements angrenzt, wäre dessen Behandlung sinnvoll.

- Einige der Quellkomponenten definieren beispielhafte **Rollenmodelle** zum Thema IT-Risikomanagement, deren Harmonisierung zwar nicht in die vorliegende Arbeit aufgenommen wurde, für eine ganzheitliche Betrachtung jedoch als weitere Hilfestellung dienen könnte.

- Ein ähnlich wertvolles Hilfsmittel könnten beispielhafte Vorschläge für die **Dokumentation** des Risikomanagement-Systems darstellen.

- Während die **Nachverfolgbarkeit** der Quellkomponenten bis zur Phase der Reduktion angemessen sichergestellt werden konnte, könnte diese bei der abschließenden Harmonisierung durch den Einsatz entsprechender softwaregestützter Werkzeuge beispielsweise dahingehend weiter verbessert werden, dass – auch über Modellgrenzen hinweg – explizite Referenzen auf die einzelnen Bausteine gesetzt werden, die eine Visualisierung von Abhängigkeiten sowie eine Navigation auf Abhängigkeitspfaden durch die Modelle erlauben.

Im Sinne der Vollständigkeit könnte eine detaillierte Bearbeitung dieser Punkte zum Gegenstand weiterführender Forschungstätigkeit werden.

Literaturverzeichnis

[1] O. Grimm, „Basel III: Nie wieder Bankenkrach in Europa,“ 20 Juli 2011. [Online]. Available: http://diepresse.com/home/wirtschaft/international/679667/Basel-III_Nie-wieder-Bankenkrach-in-Europa. [Zugriff am 16 Jänner 2012].

[2] Baseler Ausschuss für Bankenaufsicht, Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen - Überarbeitete Rahmenvereinbarung, Basel, 2004.

[3] derStandard.at, „Globalisierung als Goldgrube für IT-Dienstleister,“ 26 September 2007. [Online]. Available: http://derstandard.at/3040332. [Zugriff am 16 Jänner 2012].

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

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

[6] C. Linsley, „Auditing, Risk Management and a Post Sarbanes-Oxley World,“ *Review of Business*, S. 21 - 25, Fall 2003.

[7] J. A. Hall und S. L. Liedtka, „The Sarbanes-Oxley Act: Implications for Large-Scale IT Outsourcing,“ *Communications of the ACM,* S. 95 - 100, März 2007.

[8] Congress of the United States of America, An Act To protect investors by improving the accuracy and reliability of corporate disclosures made persuant to the securities laws, and for other purposes (Sarbanes-Oxley Act of 2002), Washington, D.C, USA, 2002.

[9] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management - Integrated Framework, Jersey City, NJ, USA, 2004.

[10] derStandard.at, „Die Schützer des Internets werden zum Angriffsziel,“ 5 August 2011. [Online]. Available: http://derstandard.at/1311802791050/Hacker-Die-Schuetzer-des-Internets-werden-zum-Angriffsziel. [Zugriff am 16 Jänner 2012].

[11] DiePresse.com, „Sony-Hack: Daten unverschlüsselt, erste mögliche Betrugsopfer,“ 28 April 2011. [Online]. Available: http://diepresse.com/home/techscience/hightech/konsolen/653743/SonyHack_Da

ten-unverschluesselt-erste-Betrugsopfer. [Zugriff am 16 Jänner 2012].

[12] C. Briseño, „Atomkatastrophe Fukushima: Japan verschwieg Risiken der radioaktiven Wolke," Spiegel Online, 9 August 2011. [Online]. Available: http://www.spiegel.de/wissenschaft/technik/0,1518,779126,00.html. [Zugriff am 16 Jänner 2012].

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-4 - Notfallmanagement, Bonn, 2008.

[14] ISO/IEC, ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements, Genf, 2005.

[15] ISO/IEC, ISO/IEC 31000:2009 - Risk management - Principles and guidelines, Genf, 2009.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-3 - Risikoanalyse auf der Basis von IT-Grundschutz, Bonn, 2008.

[17] ISACA, The Risk IT Framework - Principles, Process Details, Management Guidelines, Maturity Models, Rolling Meadows, IL, USA, 2009.

[18] ISO/IEC, ISO/IEC 27005:2008 - Information technology - Security techniques - Infomation security risk management, Genf, 2008.

[19] ISO/IEC, ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management, Genf, 2005.

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Internet-Sicherheit - Glossar/Begriffe," 2011. [Online]. Available: https://www.bsi.bund.de/DE/Themen/InternetSicherheit/GlossarBegriffe/GlossarBegriffe_node.html. [Zugriff am 6 Dezember 2011].

[21] IT Governance Institute (ITGI), COBIT 4.0 - Control Objectives, Management Guidelines, Maturity Models - Deutsche Ausgabe, Rolling Meadows, IL, USA, 2005.

[22] ISACA, COBIT 5: The Framework - Exposure Draft, Rolling Meadows, IL, USA, 2011.

[23] S. Leimeister, IT Outsourcing Governance, Wiesbaden: Gabler Verlag, 2010.

[24] IT Governance Institute (ITGI), Global Status Report on the Governance of Enterprise IT (GEIT) - 2011, Rolling Meadows, IL, USA, 2011.

[25] Technology Partners International (TPI) - Information Services Group, „The TPI Index - Global Sourcing Market Data and Insights - Third Quarter 2011," 2011. [Online]. Available: http://www.tpi.net/pdf/getfile.asp?file=index/3Q11-TPI-

Index.pdf. [Zugriff am 12 Dezember 2011].

[26] B. Kaib, Outsourcing in Banken, Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler, 2008.

[27] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 11/2010 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk, Bonn/Frankfurt am Main, 2010.

[28] H. Stachowiak, Allgemeine Modelltheorie, Springer-Verlag: Wien u.a., 1973.

[29] D. Hume, A Treatise of Human Nature: Being an Attempt to introduce the experimental Method of Reasoning into Moral Subjects, 1740.

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

[31] Die Österreichische Bibliothekenverbund und Service GmbH (OBVSG), „OBV Suche," 2011. [Online]. Available: http://search.obvsg.at/primo_library/libweb/action/search.do. [Zugriff am 7 Dezember 2011].

[32] K.-R. Müller, IT-Sicherheit mit System, Wiesbaden: Friedr. Vieweg & Sohn Verlag, 2008.

[33] European Network and Information Security Agency (ENISA), „Risk Management," 2011. [Online]. Available: http://www.enisa.europa.eu/act/rm. [Zugriff am 29 November 2011].

[34] European Network and Information Security Agency (ENISA), „Inventory of Risk Management / Risk Assessment Methods," 2011. [Online]. Available: http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-methods. [Zugriff am 29 November 2011].

[35] International Register of ISMS Certificates, „Regsiter Search," November 2011. [Online]. Available: http://www.iso27001certificates.com/Register%20Search.htm. [Zugriff am 13 Dezember 2011].

[36] IT Governance Institute (ITGI) und Office of Government Commerce (OGC), Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit - A Management Briefing from ITGI and OGC, Rolling Meadows, IL, USA (u.a.), 2008.

[37] COSO, „COSO - Home," 2011. [Online]. Available: http://www.coso.org/. [Zugriff am 13 Dezember 2011].

[38] ISACA, The Risk IT Practitioner Guide, Rolling Meadows, IL, USA, 2009.

[39] The Economist, „One Basel leads to another," 18 Mai 2006. [Online]. Available: http://www.economist.com/node/6908488. [Zugriff am 14 Dezember 2011].

[40] Bundesrepublik Deutschland, Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das zuletzt durch Artikel 2 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1126) geändert worden ist (KWG), Berlin, 2011.

[41] Bundesrepublik Deutschland, Solvabilitätsverordnung vom 14. Dezember 2006 (BGBl. I S. 2926), die zuletzt durch Artikel 1 der Verordnung vom 5. Oktober 2010 (BGBl. I S. 1330) geändert worden ist (SolvV), Berlin, 2010.

[42] Bundesministerium der Finanzen der Republik Deutschland, „Glossar - Basel III," 2011. [Online]. Available: http://www.bundesfinanzministerium.de/nn_39814/DE/BMF__Startseite/Service/Glossar/B/022__Basel__III.html. [Zugriff am 14 Dezember 2011].

[43] Frankfurter Allgemeine Zeitung, „Basel III: EU legt Entwurf zu Aufsichtsregeln für Banken vor," 7 Juli 2011. [Online]. Available: http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/basel-iii-eu-legt-entwurf-zu-aufsichtsregeln-fuer-banken-vor-11107067.html. [Zugriff am 14 Dezember 2011].

[44] IT Governance Institute (ITGI), IT Control Objectives for Sarbanes-Oxley - The Importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting, Rolling Meadows, IL, USA, 2004.

[45] Bundesamt für Sicherheit in der Informationstechnik (BSI), „IT-Grundschutz," 2011. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html. [Zugriff am 29 November 2011].

[46] ZDNet, „IT-Business - Analysen & Kommentare - BSI-Grundschutz: zu komplex, zu aufwändig, zu deutsch," 11 Jänner 2010. [Online]. Available: http://www.zdnet.de/magazin/41525300/bsi-grundschutz-zu-komplex-zu-aufwaendig-zu-deutsch.htm. [Zugriff am 14 Dezember 2011].

[47] ISACA, COBIT 5: Process Reference Guide - Exposure Draft, Rolling Meadows, IL, USA, 2011.

[48] ISACA, COBIT 5 Design Paper - Exposure Draft, Rolling Meadows, IL, USA, 2010.

[49] Office of Government Commerce (OGC), Service Design (ITIL V3), London:

TSO (The Stationery Office), 2007.

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

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

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

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

[54] W. Johannsen und M. Goeken, Referenzmodelle für IT Governance - Strategische Effektivität und Effizienz mit COBIT, ITIL & Co, Heidelberg: dpunkt, 2007.

[55] ISO/IEC, ISO/IEC 20000 - Information technology - Service management, Genf, 2005 - 2011.

[56] Siemens Enterprise, „Overview - How CRAMM works," 2011. [Online]. Available: http://www.cramm.com/overview/howitworks.htm. [Zugriff am 15 Dezember 2011].

[57] Software Engineering Institute (SEI) - Carnegie Mellon University, „CMMI Overview," 2011. [Online]. Available: http://www.sei.cmu.edu/cmmi/. [Zugriff am 30 November 2011].

[58] Borland, „Qualität von Anfang an – nur durchgängiges Qualitätsmanagement garantiert Projekterfolg und Kostenkontrolle," 2011. [Online]. Available: http://www.borland.com/de/customers/informs/16_dez_05/qualitaetsmanagement.html. [Zugriff am 15 Dezember 2011].

[59] ISO/IEC, ISO/IEC 15504: Information technology - Process assessment (Parts 1 - 10), Genf, 2003 - 2011.

[60] Congress of the United States of America, Health Insurance Portability and Accountability Act of 1996, Washington, D.C., USA, 1996.

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

[62] Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW), IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen

ausgelagerte Funktionen (IDW PS 951), Düsseldorf, 2007.

[63] ISO/IEC, ISO/IEC 16085:2006 - Systems and software engineering - Life cycle processes - Risk management, Genf, 2006.

[64] National Institute of Standards and Technology (NIST), Special Publication 800-30: Risk Management Guide for Information Technology Systems (NIST SP 800-30), Gaithersburg, MD, USA (u.a.), 2002.

[65] Organisation for Economic Co-Operation and Development (OECD), OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, Paris (u.a.), 2002.

[66] CERT, Software Engineering Institute (SEI), Carnegie Mellon University, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Pittsburgh, PA, USA, 2008.

[67] PCI Security Standards Council, LLC, Payment Card Industry (PCI) Datensicherheitsstandard (DSS) - Anforderungen und Sicherheitsbeurteilungsverfahren - Version 2.0, Wakefield, MA, USA, 2010.

[68] ISO/IEC, ISO/IEC 31010:2009 - Risk management - Risk assessment techniques, Genf, 2009.

[69] Basel Committee on Banking Supervision, Outsourcing in Financial Services, Basel: Bank for International Settlements, 2005.

[70] ISO/IEC, ISO/IEC 27031:2011 - Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity, Genf, 2011.

[71] British Standards Institution (BSI), BS 25999 - Business continuity management, London, 2006 - 2007.

[72] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS), Bonn, 2008.

[73] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise, Bonn, 2008.

[74] J. McCumber und L. Kelly, Assessing and Managing Security Risk in IT Systems: A Structured Methodology, Boca Raton, FL, USA: Auerbach Publications, 2004.

Abbildungsverzeichnis

Abbildung 1.1: Begriffe rund um Risikomanagement und deren Beziehungen 5
Abbildung 1.2: Kernbereiche der IT Governance 10
Abbildung 1.3: Verbreitung von IT-Outsourcing nach ITGI 12
Abbildung 1.4: Ausgelagerte Aktivitäten nach ITGI 12
Abbildung 1.5: Vergleich von Outsourcing-Verträgen 13
Abbildung 1.6: Sicherheitspyramide IV nach Klaus-Rainer Müller 16
Abbildung 2.1: Vorgehensmodell zur Erstellung der vorliegenden Arbeit 19
Abbildung 3.1: Vorgehensmodell: Analysephase 21
Abbildung 3.2: Gesamtmodell zur ISO/IEC 27005 – Überblick 23
Abbildung 3.3: (1) IT-Risikomanagement nach ISO/IEC 27005 23
Abbildung 3.4: (2) IT-Risikomanagement nach ISO/IEC 27005 24
Abbildung 3.5: (3) IT-Risikomanagement nach ISO/IEC 27005 25
Abbildung 3.6: (4) IT-Risikomanagement nach ISO/IEC 27005 26
Abbildung 3.7: Inhalt und Struktur der ISO/IEC 27001 (grobe Übersicht) 31
Abbildung 3.8: Inhalt und Struktur der ISO/IEC 27002 (grobe Übersicht) 33
Abbildung 3.9: Inhalt und Struktur der ISO/IEC 27005 (grobe Übersicht) 34
Abbildung 3.10: Der Risikomanagement-Prozess nach ISO/IEC 27005 36
Abbildung 3.11: Inhalt und Struktur der ISO 31000 (grobe Übersicht) 38
Abbildung 3.12: Risikomanagement-Framework und -Prozess nach ISO 31000 39
Abbildung 3.13: Inhalt und Struktur von COSO ERM (grobe Übersicht) 41
Abbildung 3.14: Inhalt und Struktur von Risk IT (grobe Übersicht) 43
Abbildung 3.15: Inhalt und Struktur des Basel-II-Konglomerats (grobe Übersicht) 46
Abbildung 3.16: Inhalt und Struktur des SOX (grobe Übersicht) 48
Abbildung 3.17: Inhalt und Struktur der BSI-Dokumente (grobe Übersicht) 49
Abbildung 3.18: IT-Sicherheitsprozess nach BSI und IT-Grundschutz 51
Abbildung 3.19: Inhalt und Struktur von COBIT 4.1 (grobe Übersicht) 53
Abbildung 3.20: Ziele und Metriken nach COBIT 4.1 – IT follows business 53
Abbildung 3.21: Inhalt und Struktur von COBIT 5 (grobe Übersicht) 54
Abbildung 3.22: Der Service-Lebenszyklus nach ITIL V3 56

Abbildung 3.23: Inhalt und Struktur der ITIL V3 (grobe Übersicht) 56
Abbildung 3.24: Aufbau von CRAMM 5 58
Abbildung 3.25: Reifegradmodell nach CMMI 59
Abbildung 3.26: Kurzvergleich der betrachteten Ansätze: Auswertung.....67
Abbildung 3.27: Zeitreihe der betrachteten Ansätze.....68
Abbildung 4.1: Vorgehensmodell: Designphase.....69
Abbildung 4.2: Tabellarisches Mapping der Quellkomponenten (Ausschnitt).....72
Abbildung 4.3: Mapping-Diagramm mit allen Integrationspaketen 73
Abbildung 4.4: Mapping-Diagramm zu Risiken und Ereignissen (Ausschnitt) 74
Abbildung 4.5: Reduktionsmodell: Integrationspakete zum Risikobegriff 76
Abbildung 4.6: Reduktionsmodell 77
Abbildung 4.7: Harmonisiertes Integrationsmodell (stark vereinfachte Darstellung) 79
Abbildung 4.8: Harmonisiertes Integrationsmodell (vereinfachte Darstellung).....80
Abbildung 4.9: Harmonisiertes Integrationsmodell (vollständige Darstellung).....81
Abbildung 4.10: Begriffsgruppe SBR.WSR 82
Abbildung 4.11: Begriffsgruppe SBR.ERI 83
Abbildung 4.12: Begriffsgruppe SBR.INF 84
Abbildung 4.13: Begriffsgruppe SBR.UST 85
Abbildung 4.14: Begriffsgruppe SBR.KON 85
Abbildung 4.15: Begriffsgruppen SBR.KOE, SBR.KOI 86
Abbildung 4.16: Begriffsgruppe SBR.IKS 87
Abbildung 4.17: Begriffsgruppe SBR.RGM.....88
Abbildung 4.18: Prozessgruppe FRA.PLN.VLE (ISMS PLAN).....89
Abbildung 4.19: Prozessgruppe FRA.PLN.STR.....89
Abbildung 4.20: Prozessgruppen FRA.PLN.ORG, FRA.PLN.GLE 90
Abbildung 4.21: Prozessgruppe FRA.PLN.ALU.....91
Abbildung 4.22: Prozessgruppe FRA.DO.BET 91
Abbildung 4.23: Prozessgruppe FRA.CHK.AUD 92
Abbildung 4.24: Prozessgruppe FRA.CHK.KON 92
Abbildung 4.25: Prozessgruppe FRA.ACT.VER.....93
Abbildung 4.26: Prozessgruppe FRA.SUP.KOM.....93
Abbildung 4.27: Prozessgruppe FRA.SUP.DOK.....94
Abbildung 4.28: Prozessgruppe FRA.SUP.INF.....95

Abbildung 4.29: Prozessgruppe PRO.KON 96
Abbildung 4.30: Prozessgruppe PRO.AST.IDE 97
Abbildung 4.31: Prozessgruppen PRO.AST.EVA, PRO.AST.STR 99
Abbildung 4.32: Prozessgruppen PRO.BEH, PRO.AKZ 100
Abbildung 4.33: Prozessgruppe PRO.MON 101
Abbildung 4.34: Harmonisiertes Integrationsmodell (Ablauf, vereinfacht) 102
Abbildung 4.35: Harmonisiertes Integrationsmodell (Ablauf, vollständig) 103
Abbildung 5.1: Vorgehensmodell: Evaluierungsphase 105

Tabellenverzeichnis

Tabelle 1.1: Beispiele für Schwachstellen, Bedrohungen und Risiken 7
Tabelle 3.1: Attribute für die Kurzbeschreibungen der verwendeten Ansätze 29
Tabelle 3.2: Kurzbeschreibung der ISO/IEC 27001 30
Tabelle 3.3: Kurzbeschreibung ISO/IEC 27002 32
Tabelle 3.4: Kurzbeschreibung der ISO/IEC 27005 34
Tabelle 3.5: Kurzbeschreibung der ISO 31000 37
Tabelle 3.6: Kurzbeschreibung von COSO ERM 40
Tabelle 3.7: Kurzbeschreibung von Risk IT 42
Tabelle 3.8: Kurzbeschreibung des Basel-II-Konglomerats 45
Tabelle 3.9: Kurzbeschreibung des Sarbanes-Oxley Act of 2002 47
Tabelle 3.10: Kurzbeschreibung der BSI-Standards und IT-Grundschutzkataloge 49
Tabelle 3.11: Kurzbeschreibung von COBIT 4.1 52
Tabelle 3.12: Kurzbeschreibung der ITIL V3 55
Tabelle 3.13: Kurzbeschreibung von CRAMM 58
Tabelle 3.14: Kurzbeschreibung von CMM/CMMI 59
Tabelle 3.15: Kurzbeschreibung ISO/IEC 15504 60
Tabelle 3.16: Kurzbeschreibung des HIPAA 61
Tabelle 3.17: Kurzbeschreibung SAS 70 61
Tabelle 3.18: Kurzbeschreibung des IDW PS 951 62
Tabelle 3.19: Kurzbeschreibung der ISO/IEC 16085 63
Tabelle 3.20: Kurzbeschreibung der NIST SP 800-30 63
Tabelle 3.21: Kurzbeschreibung der OECD Guidelines 64
Tabelle 3.22: Kurzbeschreibung von OCTAVE 65
Tabelle 3.23: Kurzbeschreibung von PCI DSS 65
Tabelle 3.24: Kurzvergleich der betrachteten Ansätze 66
Tabelle 4.1: Zusammenfassung des Mappings der Komponenten. 75
Tabelle 5.1: Evaluierung des harmonisierten Integrationsmodells 108

Anhang A: Abstract

A.1 English

This paper presents an integration model to harmonize heterogenous risk management approaches used in IT operations and outsourcing. Having defined the working context, motivation and research question, this paper introduces necessary terms and concepts and distinguishes its core topic from related work. As a first step, the relevant risk management approaches are being described in detail, and their contents and structure are being explored using an object-oriented data-modeling approach.
During the design phase, the identified concepts are being compared, evaluated and finally transformed into an integrated UML-based class and activity model containing the necessary groups of terms, definitions and processes. The integration model is validated using an attempt to falsify it in terms of critical rationalism. The paper is concluded by a summary and the deduction of implications as well as questions for further research.

A.2 Deutsch

Die vorliegende Arbeit stellt ein Integrationsmodell zur Harmonisierung des Risikomanagements für den Einsatz und das Outsourcing von Informationstechnologie vor. Nach der einführenden Darlegung von Kontext, Motivation und Forschungsfrage werden wesentliche Begriffsdefinitionen vorgenommen sowie die Arbeit von bestehenden Werken abgegrenzt. In einem ersten Schritt erfolgt eine umfassende Darstellung der verwendeten Ansätze, die im Rahmen einer objektorientierten Analyse auf inhaltlicher und struktureller Ebene betrachtet werden.
In der anschließenden Design-Phase werden die zuvor ermittelten Konzepte gegenübergestellt und bewertet, sowie im finalen Schritt ein Integrationsmodell erarbeitet, welches Begriffs- und Prozessgruppen als UML-Klassen- und Aktivitätsdiagramme definiert. Es findet eine Validierung des Integrationsmodells durch einen Falsifikationsversuch im Sinne des kritischen Rationalismus statt. Eine Zusammenfassung, Schlussfolgerungen und weiterführende Fragestellungen runden die Arbeit ab.

Anhang B: Lebenslauf

Christian Sieberer

Geboren am: 9. Dezember 1986

Geboren in: Steyr, Oberösterreich

Ausbildung

Bachelorstudium Wirtschaftsinformatik	2006 – 2010
Masterstudium Wirtschaftsinformatik	2010 – 2012