FH Vorarlberg
University of Applied Sciences

Risikomanagement im Wandel

Zusammenhang von Großereignissen, Gesetzgebung und Umsetzungsstand in Unternehmen in der DACH Region

Masterarbeit
zur Erlangung des akademischen Grades

Master of Arts

Fachhochschule Vorarlberg
Accounting, Controlling & Finance

Betreut von
Prof. Dr. Ute Vanini

Vorgelegt von
Pia Gräber, B.Sc.

Dornbirn, 04. Juli 2021

Kurzreferat

Risikomanagement im Wandel - Zusammenhang von Großereignissen, Gesetzgebung und Umsetzungsstand in Unternehmen in der DACH Region

Das unternehmerische Risikomanagement hat sich in der Vergangenheit und aktuell insbesondere durch die Coronapandemie stetig weiterentwickelt. In der DACH-Region bestehen neben den jeweiligen lokalen Gesellschaftsrechtsgesetzgebungen, welche sich in Umfang und Inhalt unterscheiden, auch internationale Standards, welche zusammen die Rahmenbedingungen für das Risikomanagement bilden. Teilweise wurden diese Gesetzlichen und sonstigen Anforderungen durch bestimmte Ereignisse eingeführt bzw. überarbeitet. Dies spiegelt sich auch im Umsetzungsstands des unternehmerischen Risikomanagements und dessen System in Organisationen wider. Insbesondere auf den Bilanzskandal des Enron-Konzerns 2002 sowie die Finanzkrise 2008 können Änderungen in der Gesetzgebung zum Risikomanagement zurückgeführt werden, welche von den Unternehmen ebenfalls umgesetzt werden. Aktuell werden die gesetzlichen Anforderungen von allen Unternehmen umgesetzt. In der jüngeren Vergangenheit zeigt sich ein positiver Trend von einem compliance-orientierten zu einem performance-orientierten Risikomanagement. Dies bedeutet, dass immer mehr Unternehmen Risikomanagement auch über die gesetzlichen Anforderungen hinaus betreiben und dies so aktiv zur Unternehmenssteuerung beiträgt.

Abstract

Transformation of Risk Management - Correlation of major incidents, legislation and implementation status in organizations within the DACH region

Enterprise Risk Management has constantly developed throughout the past and especially due to the current corona health crisis. Besides the respective local corporate laws, which differ by scope and content, there are also international Standards within the DACH-region which provide risk management framework. Enactments and changes concerning these legislative and other requirements can partially be traced back to specific events. This is also reflected in the implementation status of enterprise risk management within organizations. Especially the Enron accounting scandal in 2002 and the financial crisis starting 2008 can be named as background for legislation chances and new enactments. These chances are also considered within enterprise risk management. Currently all organizations meet regulatory requirements. In the recent past, a positive trend shifting from compliance-oriented to performance-oriented risk management can be registered in organizations. This means that the number of companies which use risk management also beyond complying with regulatory requirements and therefore actively for corporate management is growing.

Inhaltsverzeichnis

Tabellen- und Abbildungsverzeichnis

Abkürzungsverzeichnis

BilMoG	Bilanzrechtsmodernisierungsgesetz
BilReG	Bilanzrechtsreformgesetz
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CRO	Chief Risk Officer
DACH	Deutschland, Österreich, Schweiz
DCGK	Deutscher Corporate Governance Kodex
EMEA	Europe, Middle East, Africa
ERM	Enterprise Risk Management
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer
IFRS	International Financial Reporting Standards
IKS	Internes Kontrollsystem
KMU	Kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
OR	Obligationenrecht
PCAOB	Public Company Accounting Oversight Board
PS	Prüfungsstandard
RM	Risikomanagement
RMS	Risikomanagementsystem
SOX	Sarbanes-Oxley Act
StaRuG	Stabilisierungs- und Restrukturierungsgesetz
TransPuG	Transparenz- und Publizitätsgesetz
UGB	Unternehmensgesetzbuch
UMAG	Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts
URÄG	Unternehmensrechtänderungsgesetz

1. COVID-19 als Anstoß zum Umdenken im Risikomanagement

Die aktuelle Covid-19 Pandemie stellt Unternehmen in Europa seit Beginn des Jahres 2020 vor zahlreiche neue Herausforderungen. Neben gesundheitlichen Auswirkungen zeigen sich mittlerweile auch die wirtschaftlichen Folgen. Das Wirtschaftswachstum sinkt und auch auf dem Arbeitsmarkt bietet sich nach zahlreichen weltweiten Lockdowns eine neue Situation, sodass die Coronapandemie unter anderem als *„Stresstest“* (Boecker und Zwirner 2020) für die Wirtschaft oder auch als *„Black Swan Ereignis“,* welches allerdings nicht völlig unvorhergesehen aufgetreten ist (Gleißner 2020, S. 101), bezeichnet wird.

Die Wirtschaftsprüfungsgesellschaft Ernst & Young geht hier sogar noch weiter und bezeichnet die aktuelle Krise als *„eine der größten Herausforderungen in der Geschichte der Menschheit“*. (Hölzl 2020)

Insbesondere KMUs spüren die Auswirkungen der Krise besonders, da speziell in diesen Betrieben das Risikomanagement zuvor nur oberflächlich behandelt wurde. Die Coronakrise zeigt KMUs aber auch Großunternehmen und Konzernen, dass durchaus Aufholbedarf in Sachen Risikomanagement besteht. (vgl. Francke 2020)

Die Coronakrise fordert also ohne Zweifel das unternehmerische Risikomanagement und die dafür verantwortlichen Personen in den Organisationen und hat beziehungsweise wird zukünftig ein Umdenken hinsichtlich gesundheitlichen Krisen als Risiko bewirken.
Doch die Coronakrise stellt nicht die erste Herausforderung für Unternehmen in Sachen Risikomanagement dar. Auch in der Vergangenheit ereigneten sich bereits zahlreiche Krisen verschiedenen Ursprungs. Beispielsweise die Finanz- und Weltwirtschaftskrise oder auch Terroranschläge. Aber auch Gesundheitskrisen wie die Schweinegrippe, Ebola oder der SARS Ausbruch zählen dazu. Dies zeigt, dass die derzeitige Pandemie durchaus nicht unvorhersehbar war. Wer hat hier also die Gefahr einer weltweiten Pandemie unterschätzt? Kann dies allein den Unternehmen selbst zugeschrieben werden oder trifft hier auch andere Stakeholder in Sachen Risikomanagement eine nicht wahrgenommene Verantwortung?

Risikomanagement liegt allerdings nicht alleine in den Händen der Unternehmen, auch der Gesetzgeber spielt hierbei eine entscheidende Rolle. Die jeweils lokalen Unternehmens- und Gesellschaftsrechtgesetzgebungen sowie verschiedene teils freiwillig, teils verpflichtend anzuwendende Standards bilden die Rahmenbedingungen für die Umsetzung des unternehmerischen Risikomanagements.

Dies zeigt, dass das Risiko- und Krisenmanagement sowohl von Seiten der Unternehmen als auch seitens der Gesetzgeber beeinflusst werden kann. Im Fall der Coronapandemie

scheint es also, als wäre das Risiko einer Gesundheitskrise von beiden Seiten unterschätzt worden.

Aber die Krise kann auch zu einer Weiterentwicklung des Risikomanagements beitragen und dieses für künftige Herausforderungen besser aufstellen. Es liegt insbesondere in der Hand der Unternehmen, sowohl negative als auch positive Erkenntnisse aus der Krise zu ziehen und sich dahingehend zu entwickeln.

Doch wie haben Gesetzgeber und Risikomanagementsysteme in der Vergangenheit auf Krisen und sonstige Ereignisse reagiert und welche Zusammenhänge lassen sich hier feststellen?

Ziel dieser Arbeit ist es einen Zusammenhang zwischen eingetretenen Ereignissen, gesetzlichen Änderungen und in einem weiteren Schritt auch den Umsetzungsstand zu erkennen. Dieser Zusammenhang bezieht sich sowohl auf die zeitliche Einordnung als auch inhaltliche Aspekte. Zudem soll erörtert werden, in welchen Bereichen sich das Risikomanagement insbesondere entwickelt hat und in welchen Bereichen aufgrund der eingetretenen Ereignisse noch Entwicklungsbedarf für die Zukunft besteht.
Um dies zu erreichen müssen zunächst systematisch relevante Ereignisse definiert werden. Hierbei wird der Beginn des Betrachtungszeitraumes auf das Jahr 2000 festgelegt. Insbesondere zeichnen sich relevante Ereignisse dadurch aus, dass diese mit einer umfassenderen Risikobetrachtung verhindert oder abgemildert hätten werden können. Anschließend werden anhand verschiedener Literatur sowie Gesetzestexten und Standards, Änderungen in ebendiesen herausgearbeitet. Zeitlich erfolgt diese Analyse beginnend mit dem Gesetz zur Kontrolle und Transparenz in Deutschland, welches 1998 in Kraft trat. Ebenso werden Folgen für die Risikomanagementpraxis angegeben. Änderungen und Ereignisse werden als Ergebnis in zeitlichen Zusammenhang gesetzt, um direkte Verbindungen zu erkennen. Einen weiteren Schritt stellt die Analyse verschiedener Studien zur Risikomanagementpraxis in Unternehmen dar. Für diese Analyse werden aus den vorhergehenden Recherchen zu Gesetzesänderungen und Ereignissen, abgeleitete Kriterien herangezogen. Anhand dieser Kriterien wird der Umsetzungsstand des Risikomanagements in Organisationen erarbeitet. Hierbei wird auch auf eventuelle länder- und branchenspezifische Unterschiede eingegangen. Abschließend werden die Ergebnisse aus der Analyse der gesetzlichen und quasi-gesetzlichen Änderungen sowie der jeweilige Umsetzungsstand zusammengeführt, um folgende Fragen zu beantworten.

Welche gesetzlich und quasi-gesetzlich bedingte Weiterentwicklungen des Risikomanagements und von Risikomanagementsystemen in Unternehmen sind seit dem Jahr 2000 feststellbar?

- Inwieweit können diese gesetzlichen und quasi-gesetzlichen Änderungen auf bestimmte externe Ereignisse zurückgeführt werden?
- Inwieweit werden diese Änderungen von Unternehmen der DACH Region umgesetzt?

Die vorliegende Arbeit gliedert sich in sechs Teile. Nach Erläuterung der Zielsetzung, Methodik sowie Relevanz, findet eine Erörterung des theoretischen Hintergrunds zur historischen Entwicklung sowie möglichen Ausrichtungen des Risikomanagements statt. Im dritten Teil der Arbeit werden Großereignisse definiert und beschrieben. Anschließend folgt im gleichen Teil beginnend mit dem KonTraG in Deutschland, eine Analyse der gesetzlichen Anforderungen und sonstigen Standards zum Risikomanagement sowie deren Änderungen. Hierbei wird auf die wichtigsten internationalen Standards und Gesetze sowie die lokalen Gesetzgebungen und sonstigen Anforderungen zum Risikomanagement in Deutschland, Österreich und der Schweiz eingegangen. Nach Analyse der gesetzlichen und quasi-gesetzlichen Anforderungen folgt in Teil vier eine Metastudie zum Umsetzungsstand in Unternehmen. In Kapitel fünf werden die Erkenntnisse der Großereignisse, Gesetzesänderungen und der Metastudie zusammengeführt, um im abschließenden sechsten Teil einen Ausblick auf die Entwicklung nach der Coronapandemie zu geben.

2. Grundlagen des Risikomanagements

Für den Begriff Risikomanagement existieren zahlreiche Definitionen und Erklärungen, welche sich in den letzten Jahren verändert und weiterentwickelt haben. In den folgenden Unterkapiteln wird zunächst die historische Entwicklung des Risikomanagements dargestellt. Anschließend werden verschiedene Definitionen erläutert, woraufhin auf die gesetzlichen Rahmenbedingungen in der DACH-Region sowie auf die Bedeutung von Risikomanagementsystemen in Unternehmen eingegangen wird. (vgl. Kajüter 2012, S. 16)

2.1 Kennzeichnung & alternative Diskussionen von Risikomanagement

2.1.1 Risikomanagement von der Antike bis zur Gegenwart

Bereits in den altertümlichen Gesellschaften der Römer, Ägypter, Phönizier und Griechen wurden strategische Allianzen zwischen Händlern gegründet, um Gefahren abzuwenden. Alexander der Große kann bereits als Beispiel für ein erstes Risikomanagement im Altertum herangezogen werden. Allerdings existierte der Begriff des „Risikos“ zu dieser Zeit noch nicht, was darauf zurückzuführen ist, dass die genannten Gesellschaften im Glauben lebten, dass die Zukunft durch die Götter bestimmt ist. Nachdem er in einer entscheidenden Schlacht die Perser geschlagen hatte und somit auch Persien an sein Reich angeschlossen hatte, setzte er strategische Schritte, um sein Reich zu sichern und sich auch in den neu eroberten Gebieten Macht und Einfluss zu verschaffen. Er ging Bündnisse ein, forderte von seinen Anhängern Eheschließungen mit persischen Adeligen und übernahm gewisse persische Gepflogenheiten. So zielte er darauf ab, Aufständen und Widerstand in seinen Gebieten vorzubeugen. (vgl. Romeike 2018, S. 4f)

So lässt sich bereits aus den Jahrhunderten vor Christus erkennen, dass gewisse Ereignisse zu präventiven Maßnahmen führen, um neuen Risiken vorzubeugen.

Allerdings existieren auch in altertümlichen arabischen, italienischen sowie spanischen Schriften Erwähnungen risikoähnlicher Begriffe. Beispielsweise wurde der italienische Begriff „risicare“ mit „wagen“ übersetzt, was darauf hindeutet, dass es sich hierbei nicht rein um das Schicksal handelt, sondern um eine aktive Entscheidung. (vgl. Fiege 2006, S. 37)

Der Begriff des Risikos wurde im 14. Jahrhundert in der Seefahrt und dem Seehandel in Italien zum ersten Mal offiziell erwähnt. Es kam hier zu den ersten Versicherungsverträgen, welche den immer mehr wachsenden Seehandel absichern sollten. Auch die Entwicklung des Risikobegriffs bis heute ist eng mit der Entwicklung des Versicherungswesens verknüpft. Ein weiterer Bereich, welcher seit der Antike den Begriff des Risikos prägte ist das

Glückspiel. So heißt es bei Romeike und Hager (2020), das Glückspiel sei „der Inbegriff eines bewusst eingegangenen Risikos“ (S.6). Im Laufe der Jahrhunderte wurde der Begriff des Risikos mathematischer und es erfolgten statistische Bewertungen um diese anschließend durch verschiedene Versicherungen abdecken zu können. Es zeigt sich, dass Unternehmen seit jeher bereits Ansätze zum Umgang mit Risiken suchen. (vgl. Romeike 2018, S. 6–12; Romeike und Hager 2020, S. 6f)

Auch der Ursprung des Begriffes „Risikomanagement“ liegt in der Versicherungsbranche, in jener der USA zunächst unter dem Begriff „Insurance Management“, welcher die versicherbaren Risiken eines Unternehmens beinhaltet. Aufgrund der Zunahme der Risiken sowie deren Komplexität und Kosten, wurde dazu übergegangen, Risiken durch präventives Handeln zu vermeiden, anstatt lediglich Versicherungen abzuschließen, welche nach Eintreten des Risikos die finanzielle Absicherung übernehmen sollten. Hierfür etablierte sich der Begriff des Risikomanagements (Risk Management). Mit der präventiven Betrachtung wurde es auch möglich, nicht versicherbare Risiken zu betrachten und zu bewerten. Zunächst wurden Preis- sowie Wechselkursrisiken miteingeschlossen, worauf auch die Einbeziehung von spekulativen Risiken folgte. (vgl. Paetzmann 2008, S. 42f)

Mit der Weiterentwicklung des Risikomanagements und dessen Bedeutung erhöhte sich auch die Komplexität. Für jedes neu betrachtete Risiko geht auch eine Quantifizierung einher. Hierzu existieren zahlreiche Ansätze, welche jeweils auf die Art des Risikos angepasst sind.

Unterschiedliche Definitionen von Risiko sowie Risikomanagement werden im folgenden Kapitel diskutiert.

2.1.2 Definitionen von Risiko & Risikomanagement verschiedener Standards

Heute sind die Begriffe Risiko und Risikomanagement beispielsweise in einer ISO-Norm definiert. “Koordinierte Aktivität zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken” (ISO 31000:2009) – so wird der Begriff des Risikomanagements in der international gültigen Norm ISO31000 definiert. Der Begriff des Risikos wird in der Norm als „Auswirkung von Unsicherheit auf Ziele“ (ISO 31000:2009) dargestellt. Auch in der Norm ISO9001:2015 wurde das Risikomanagement mit dem Update von 2015 integriert.

Risiko wird als möglich eintretendes Ereignis, welches Auswirkungen auf Unternehmensziele und deren Erreichung hat, definiert. Bei einem solchen Ereignis kann es sich im weiteren Sinne um Entscheidungen, Handlungen oder Unterlassungen handeln, welche die Zielerreichung des Unternehmens gefährden. (vgl. Diederichs 2013, S. 9) Der Begriff des

Risikos ist meist negativ ausgelegt, so werden im Alltag anstelle von Risiko auch die Begriffe Wagnis oder Gefahr verwendet. (vgl. Kajüter 2012, S. 16)

Zudem hängt die Interpretation und Wahrnehmung von Risiko vom subjektiven Empfinden des Betrachters ab, was dazu führen kann, dass bestimmte Risiken unter- bzw. überschätzt werden. (Keitsch 2007) Für ein Unternehmen kann dies bedeuten, dass Ziele verfehlt und unter Umständen auch der Fortbestand des Unternehmens gefährdet wird. Aufgrund dessen werden verschiedene Risiken in der Unternehmenspraxis quantifiziert und gewichtet, um so einer Gefährdung bestmöglich vorzubeugen.

Allgemein kann beim Begriff des Risikos zwischen einem ursachenbezogenen sowie einem wirkungsbezogenen Ansatz unterschieden werden. (vgl. Fiege 2006, S. 38–42)

Der ursachenbezogene Ansatz bezieht das Risiko auf Entscheidungssituationen im Unternehmen und stellt die Ursache des Risikos in den Mittelpunkt. Ein Risiko entsteht nach diesem Ansatz durch unvollkommene Informationen über den Eintritt zukünftiger Ereignisse. Verschiedene Eintrittsszenarien und deren Wahrscheinlichkeiten als Folge einer Entscheidung im Unternehmen unterliegen einer Unsicherheit und können oft nur subjektiv eingeschätzt werden. Dieser Ansatz wurde bedeutend von Frank Knight (1921) geprägt. Vgl. (Backes 2019; Fiege 2006; vgl. Keitsch 2007; Skorna und Nießen 2020)

Aufgrund der unvollständigen Informationslage für die Zukunft wird die Risikodefinition um einen wirkungsbezogenen Ansatz ergänzt. Hierbei stehen die Auswirkungen im Vordergrund, wobei teilweise alle Auswirkungen und teilweise lediglich negative Auswirkungen betrachtet werden. So beschreibt Backes (2019) das Risiko in diesem Ansatz als Abweichung des Ergebnisses einer Entscheidung von einem Prognosewert. (vgl. Backes 2019; Diederichs 2013; vgl. Fiege 2006; Skorna und Nießen 2020)

Im Prüfungsstandard 340 des Instituts der Wirtschaftsprüfer werden ebenfalls Definitionen der Begriffe Risiko, Risikomanagement sowie Risikomanagementsystem angeführt. Die Betrachtung liegt in diesem Standard auf den negativen Auswirkungen. Demnach sind Risiken „*Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen Zielabweichung führen können*“. Das Risikomanagement wird als strukturierter Umgang mit diesen negativen Zielabweichungen beschrieben. Abschließend stellt ein Risikomanagementsystem die Gesamtheit aller Maßnahmen dar, welche das Risikomanagement sicherstellen. (IDW EPS 340 n.F. Tz 8)

Weiter wird Risikomanagement als unternehmensweiter Prozess, welcher alle organisatorischen Maßnahmen zur Erkennung und Umgang mit Risiko umfasst, beschrieben. Dieser Prozess ist in die Unternehmensführung eingegliedert und bedarf spezieller Methoden um

diesen systematisch umzusetzen. Das Risikomanagement wird in Teilprozesse untergliedert:

- Risikoidentifikation
- Quantifizierung
- Aggregation
- Überwachung und Bewältigung.

(vgl. Gleißner und Klein 2017, S. 23; Stampfer 2019, S. 25f; vgl. Vanini 2012, S. 19)

Ebenfalls kann Risikomanagement als Umgang mit Risiken im Unternehmen definiert werden. Risiken sind oft branchenabhängig, manche Faktoren sind auch branchenübergreifend gleich, wobei allerdings die Priorisierung abweichen kann. (vgl. Kajüter 2012, S. 19f)

Kajüter (2012) unterteilt das Risikomanagement in Unternehmen in drei Teilbereiche:

- Risikofrüherkennungssystem
- Risikobewältigungssystem
- Internes Überwachungssystem

Die genannte Unterteilung bildet das sogenannte Risikomanagementsystem, welches in Konzernen angewendet wird. Dies beinhaltet sämtliche Maßnahmen in einem Unternehmen, welche zum Management von Chancen und Risiken eingesetzt werden. Beispielsweise können dies organisatorische, technische, personelle oder Prozess-Ressourcen sein, welche im Unternehmen für das Risikomanagement eingesetzt werden. Zudem zählen Risikostrategie und Risikopolitik eines Unternehmens zum System. Dieses System soll die Existenz und Zielerreichung des Unternehmens sichern. (vgl. Institut für Interne Revision Österreich 2014, S. 21f)

2.2 Risikomanagementsysteme als Steuerungsinstrument

Das Risikomanagement, für welches die Verantwortlichkeit oft im Top-Management liegt, ist in Unternehmen eng mit der strategischen Ausrichtung und Unternehmensführung verbunden. Für die Umsetzung eines systematischen Risikomanagements benötigt es zudem eine Risikostrategie, ein Risikocontrolling sowie ein Risikoreporting.
Die Risikostrategie eines Unternehmens muss folgende Informationen beinhalten:

- Arten von Risiken
- Risikobereitschaft, Risikoeinstellung und Risikotragfähigkeit des Unternehmens
- Risikoursprung
- Zeitliche Einordnung der Risiken

Wie hoch die Risikobereitschaft eines Unternehmens ist, hängt von verschiedenen Faktoren ab. Einerseits stellt die Unternehmensform und Eigentümerstruktur eine wichtige Variable dar, da unter anderem die persönliche Risikoeinstellung der Unternehmensleitung bzw. der Eigentümer die Risikostrategie beeinflusst. Neben der eher subjektiven persönlichen Risikoeinstellung sind auch Unternehmenskennzahlen wie Cashflows und Liquidität von großer Bedeutung. (vgl. Brauweiler 2019; Rohlfs und Mahnke 2020; vgl. Romeike 2018)

Im Zuge der Implementierung eines Risikomanagementsystems im Unternehmen müssen zunächst alle potentiellen vergangenen, aktuellen und zukünftigen Risiken identifiziert werden. Für jedes identifizierte Risiko, welches Relevanz für das vorliegende Unternehmen besitzt, muss ein Vorgehen festgelegt werden. Das muss unter anderem die jeweils relevanten KPIs und Kennzahlen, die Berichterstattung, die Steuerung sowie die Verantwortlichkeiten enthalten. Insbesondere müssen Frühwarnindikatoren sowie Szenarien zur Risikovermeidung bzw. Risikominimierung festgelegt werden. Um den Fortbestand des Unternehmens nachhaltig zu sichern, müssen Risikomanagement, -controlling und -berichterstattung durch geeignete Strukturen sichergestellt werden. Die Implementierung eines Risikomanagementsystems ist in verschiedenen Gesetzen gefordert, wie beispielsweise in § 91 des deutsche Aktiengesetzes oder im deutschen sowie österreichischen Corporate Governance Codex.[1] (vgl. Brauweiler 2019; Diederichs 2013; vgl. Romeike 2018)

Einen weiteren Vorteil eines implementierten Risikomanagementsystems stellt der Einfluss auf Bonitätsprüfungen und Rankings dar. Für die Stakeholder (Investoren, Kreditgeber etc.) des Unternehmens am Kapitalmarkt bedeutet ein RMS die Reduktion der Ausfallwahrscheinlichkeit, da hierdurch relevante Risiken frühzeitig erkannt und gesteuert werden. (vgl. Kajüter 2012, S. 2)

Im Folgenden wird der Risikomanagementprozess im Unternehmen anhand zweier Abbildungen dargestellt, welche sich verschiedener Visualisierungen bedienen. Abbildung 1 zeigt den Prozess unter Berücksichtigung eines Inputs sowie Outputs.

[1] Weitere gesetzliche Vorgaben und Anforderungen werden in Kapitel 3.2 analysiert.

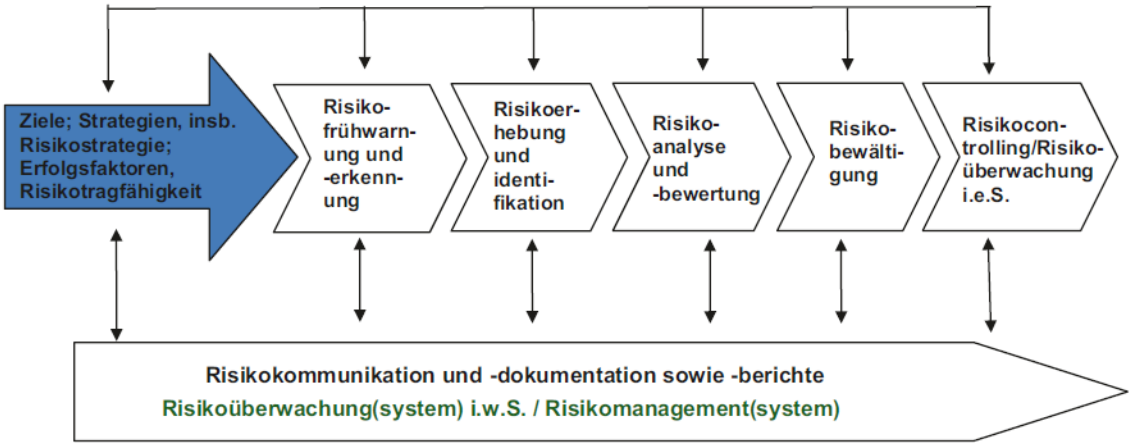

Abbildung 1: Prozess des Risikomanagements im Unternehmen
Quelle: Brauweiler 2019, S. 8

Abbildung 2 verdeutlicht den Zusammenhang des Risikomanagements und des hierfür benötigten PDCA-Zyklus, welcher auch durch den IDW Prüfungsstandard 340 vorgeschrieben wird.

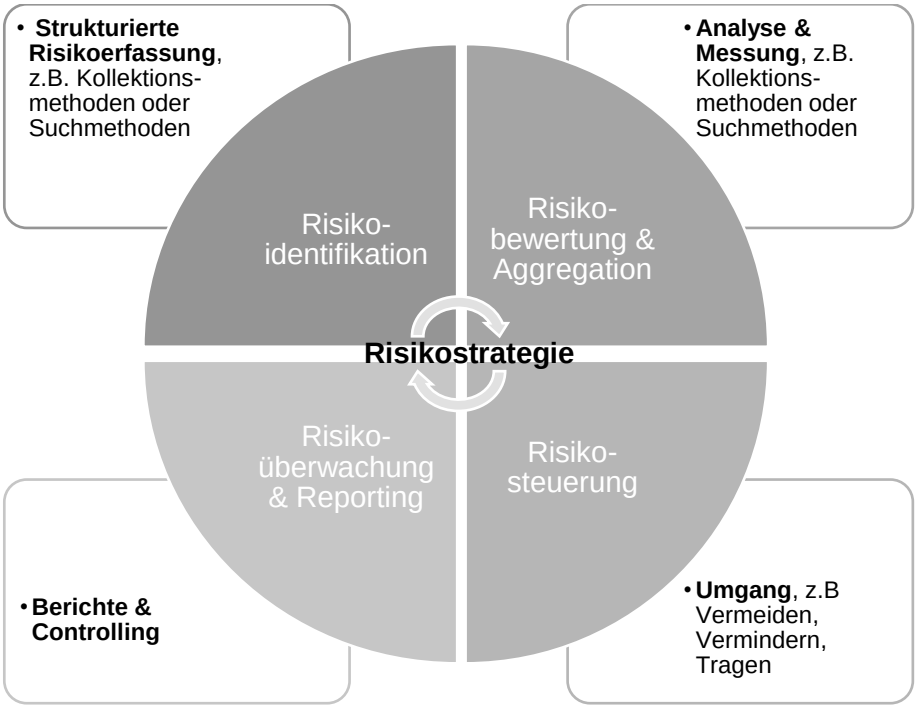

Abbildung 2: PDCA Zyklus des Risikomanagements im Unternehmen
Quelle: Eigene Darstellung nach IDW EPS 340 n.F.; Romeike 2018, S. 38

Im Zuge der Risikoidentifikation müssen alle Risiken und Szenarien erfasst werden. Rohlfs und Mahnke beschreiben Risikoidentifikation als „*die Suche und Bestimmung aller Einzelrisiken sowie das Bilden von Risikogruppen bzw. -kategorien".* Dies bedeutet, dass ähnliche Risiken zu Clustern zusammengefasst werden sollten, um dem Unternehmen einen besseren und strukturierten Überblick über die Risikolage und damit einhergehend auch über die Chancen zu ermöglichen. Im Rahmen der Risikoidentifizierung müssen alle Informationen, welche zur Bewertung, Analyse und Einordnung der einzelnen Risiken nötig sind, gesammelt werden. Es existieren verschiedene Methoden für die Risikoidentifikation, welche in Kollektionsmethoden und Suchmethoden unterteilt werden können. Mit Kollektionsmethoden (z.B. SWOT-Analyse, Checklisten) können insbesondere bereits bekannte Risiken identifiziert werden, welche beispielsweise in einer vergangenen durchgeführten Risikoidentifikation bereits behandelt wurden. Um neue und unbekannte Risiken zu identifizieren, werden vorrangig Suchmethoden verwendet. Es werden analytische Suchmethoden, welche ihren Ursprung im Qualitätsmanagement haben, von Kreativitätsmethoden unterschieden. Analytische Suchmethoden basieren auf strukturierten Daten, welche mit verschiedenen Verfahren ausgewertet werden können, um somit potentielle zukünftige Risiken zu identifizieren. Kreativitätsmethoden, welche unter anderem die Methode des Brainstormings beinhalten, sollen vor allem zu neuen Denkansätzen und Perspektiven führen und somit unbekannte Risikopotentiale aufzeigen. In der Praxis ist von essentieller Bedeutung, dass verschiedene Methoden zur Risikoidentifizierung verwendet werden, um die Risikosituation und Bedrohung eines Unternehmens möglichst umfassend abzubilden. Die beschriebenen Methoden können ebenfalls zur Risikobewertung herangezogen werden. Dies ermöglicht die gleichzeitige Identifikation und Bewertung. Allerdings unterscheiden sich die Outputs dieser beiden Phasen. Während nach der Risikoidentifzierung lediglich eine strukturierte Auflistung der erkannten Risiken vorliegt, werden diese im Zuge der Bewertung und Aggregation bereits nach Eintrittswahrscheinlichkeit und Schadenspotential gegliedert. Bekannte Methoden zur Bewertung stellen sogenannte Risk-Maps oder Risikoportfolios dar, welche auch das Ergebnis der Risikoidentifizierung sowie -bewertung darstellen. Hierbei werden Risiken bezüglich ihrer Eintrittswahrscheinlichkeit sowie ihres Schadenspotentials bewertet. (vgl. IDW EPS 340 n.F.; Rohlfs und Mahnke 2020; vgl. Romeike 2018; Romeike und Hager 2020)

In der darauffolgenden Phase zur Risikosteuerung muss entschieden werden, wie mit den zuvor identifizierten und bewerteten Risiken verfahren wird, um den Fortbestand des Unternehmens sicherzustellen und positiv zu beeinflussen. Hierbei existieren verschiedenen Möglichkeiten zum Umgang mit Risiken, welche betrachtet werden müssen.

- Risikovermeidung
- Risikoreduktion
- Risikotransfer
- Risikoteilung
- Tragung von Risiko

Durch eine Aufteilung der Risiken in die oben genannten Kategorien zur Steuerung soll ein ausgewogenes Verhältnis zwischen Chancen und Risiken eingerichtet werden und so zum Unternehmenserfolg beitragen. Die Risikosteuerung ist eng mit der Risikostrategie des Unternehmens verknüpft. So wird beispielsweise der Anteil an abgesicherten Risiken in einem risikoavers ausgerichteten Unternehmen höher sein als in einem Unternehmen mit hoher Risikobereitschaft. (vgl. IDW EPS 340 n.F.; Romeike 2018)

Abschließend wird durch die Risikoberichterstattung und die dadurch erfolgende Risikoüberwachung sichergestellt, dass Abweichungen oder Schwachstellen frühzeitig identifiziert werden können. Durch ein strukturiertes Risikoreporting wird zudem der Informationsfluss zwischen den Stakeholdern des Unternehmens sichergestellt. Durch die stetige Berichterstattung werden gegebenenfalls neue Risiken identifiziert, wodurch der Prozess erneut beginnt.

2.3 Compliance-orientiertes Risikomanagement

Im Jahr 2004 veröffentlichte der Zusammenschluss COSO ein übergreifendes Rahmenkonzept für das Risikomanagement im Unternehmen, auch als Enterprise Risk Management (ERM) bezeichnet. Zuvor existierten zahlreiche verschiedene Konzepte und Standards unterschiedlicher Institutionen wie Wirtschaftsprüfungsgesellschaften, Unternehmensberatungen und aus der Wirtschaftswissenschaft. Gemäß COSO Standard trägt das Risikomanagement zur Erreichung der Unternehmensziele bei und soll gleichzeitig überraschende Wendungen, welche das Unternehmen und dessen Ziele gefährden, vermeiden beziehungsweise abmildern. Für das Risikomanagement im Unternehmen bestehen unterschiedliche Ansätze. Zum einen kann das ERM lediglich insofern ausgestaltet sein, dass gesetzliche Anforderungen erfüllt werden (Compliance). Zum anderen kann das Risikomanagementsystem wie bereits in Kapitel 2.2 beschrieben, zur aktiven Steuerung und Überwachung des Unternehmens herangezogen werden (Performance). ERM kann innerhalb dieser beiden Ausprägungen zudem nach Verankerung im Unternehmen gegliedert werden. Folgende Abbildung zeigt die unterschiedlichen Einteilungen des ERM. Die horizontale Achse gibt die Ausprägung an, während die vertikale Achse die Verankerung innerhalb der Organisation eines Unternehmens wiederspiegelt. (vgl. Tekathen 2015)

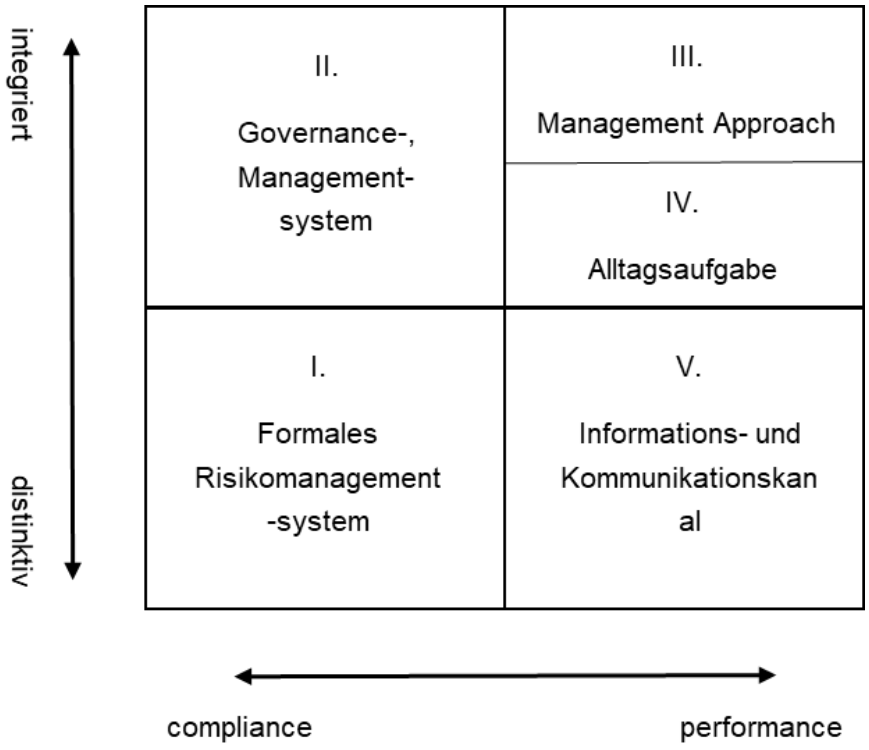

Abbildung 3: Einordnungen ERM
Quelle: Eigene Darstellung nach Tekathen 2015

Compliance Orientiertes Risikomanagement lässt sich demnach in ein rein formales Risikomanagementsystem sowie ein Governance- beziehungsweise Managementsystem unterteilen.

I. Formales Risikomanagementsystem

Unter dieser Einordnung wird die Identifizierung, Beschreibung und Bewertung von Risiken sowie eine Aufzählung der jeweiligen Gegenmaßnahmen verstanden. Vorranging dient ein hier eingeordnetes ERM-System dazu, den Vorgaben zu Berichterstattung gerecht zu werden und somit einen Compliance-Nachweis zu schaffen. Zudem soll auch eine Auditierbarkeit des Unternehmens geschaffen werden. Allerdings müssen auch in dieser ersten Ausprägung die Risiken innerhalb der Unternehmensstruktur, wie beispielsweise einem Konzern, aggregiert und vernetzt werden. Das ERM darf nicht lediglich lokal ausgerichtet werden, sondern muss alle Risiken innerhalb einer Organisation enthalten. Gleichzeitig können neben diesem umfassenden ERM lokale spezifische Risikomanagementsysteme bestehen (z.B. Finanzrisikomanagement). Diese sind mit dem organisationsweiten ERM verknüpft, operieren allerdings lokal. Das ERM erfüllt hier in erster Linie eine Dokumentationsfunktion. (vgl. Tekathen 2015)

II. Governance- bzw. Managementsystem

In der Einordnung als Governancesystem soll ERM neben der reinen Dokumentationsfunktion auch dazu beitragen, die Risiken zu vermeiden beziehungsweise abzumildern. ERM bildet hier einen organisationsweiten Ordnungsrahmen zur Führung und Kontrolle eines Unternehmens. Das Risikomanagement wird neben anderen Systemen wie unter anderem dem Qualitätsmanagementsystem in die Organisation integriert und soll im Rahmen eines PDCA-Zyklus zur Optimierung innerhalb der Organisation beitragen. Durch die Einführung von Managementsystemen in unterschiedlichen Bereichen der Organisation, welche Abläufe standardisieren und gesetz- und regelkonformes Agieren der unterschiedlichen Parteien im Unternehmen sicherstellen, können Risiken abgeschwächt werden und somit ein effektives ERM geschaffen werden. (vgl. Tekathen 2015)

3. Entwicklungen der gesetzlichen Anforderungen in Zusammenhang mit eingetretenen Ereignissen

In den folgenden Unterkapiteln werden zunächst die betrachteten Großereignisse definiert und analysiert. Anschließend wird detailliert auf die Gesetzesänderungen in der DACH Region eingegangen sowie weitere relevante Risikomanagementstandards definiert und analysiert. In einem weiteren Unterkapitel wird auf die derzeitige Covid-19 Krise und die damit einhergehenden bereits erfolgten gesetzlichen Änderungen sowie einem Ausblick für die Zukunft eingegangen. Abschließend erfolgt eine kritische Diskussion der Ereignisse sowie der Gesetzeslage und deren Änderungen.

3.1 Identifikation und Analyse von relevanten Ereignissen seit 2000

In der Vergangenheit hatten diverse Ereignisse wie die Dotcom-Blase, der Terroranschlag in New York am 11. September 2001, die Finanzkrise 2008/09 oder die Schuldenkrise um Griechenland 2010, Auswirkungen auf die Gesetzgebung in verschiedenen Bereichen. Durch den Eintritt dieser Ereignisse wurden Unternehmen vor neue Herausforderungen gestellt und es wurden neue Risiken, Schwächen und Stärken aufgezeigt. Die Auswahl der Ereignisse erfolgte aufgrund internationaler Bekanntheit, Bezug zu Risikomanagement sowie der Schwere der Auswirkungen und Folgen. Zudem wurden neben internationalen Ereignissen auch lokale Fälle aus der DACH-Region gewählt. Einige Ereignisse beziehungsweise die Ermittlungen dazu dauern nach wie vor an, sodass hier nur ein derzeitiger Ausblick auf die Auswirkungen gegeben werden kann.

Zunächst werden die ausgewählten Ereignisse unter Angabe von Ursache und Wirkung in chronologischer Reihenfolge beschrieben. Anschließend werden die daraus gewonnenen Erkenntnisse und Ergebnisse in einer Übersichtstabelle zusammengefasst.

Dotcom Blase 2000

Diese Spekulationsblase, welche Internetunternehmen betraf, platzte im Jahr 2000 in den USA. In den 1990er Jahren stiegen die Börsenwerte von Internetunternehmen stark und stetig an. Die Werte konnten durch die bis dorthin traditionellen Bewertungsverfahren nicht mehr erklärt werden. Um diese Unsicherheit zu beheben, wurden neue Verfahren zur Bewertung entwickelt, welche die hohen Bewertungen erklären sollten. Viele der Internetunternehmen in den USA verzeichneten in den späten 1990er Jahren hohes Umsatzwachstum, jedoch kaum Gewinne. Da sich die Internetunternehmen mit neuartigen Technologien zur Kommunikation und Information allerdings in einer noch neuen, sich schnell entwickelnden Phase befanden, brachten die fehlenden Gewinne keine Abwertung mit sich. Es wurde

davon ausgegangen, dass mit diesen neuen Technologien das Wirtschaftswachstum dauerhaft steigen würde. Im Jahr 2000 stoppte diese Entwicklung, da erkannt wurde, dass die zuvor erwarteten Gewinne nicht eintreten würden und die Unternehmen somit überbewertet waren und die Spekulationsblase platzte. Es folgte eine Rezession an den Börsen und die Anzahl an Internetunternehmen nahm stark ab. Die Dotcom Blase führte dazu, dass die zuvor neu eingeführten Bewertungsverfahren überdacht wurden und für Internetunternehmen zwar die Bedeutung der verschiedenen ökonomischen Einflussfaktoren angepasst wurden, jedoch nicht die grundsätzliche wirtschaftliche Bewertung. In den folgenden Jahren gewannen die verbleibenden Unternehmen wieder an Wert und es folgten Unternehmensübernahmen, bei welchen die Rahmenbedingungen und Bewertungen dem Niveau vor dem Platzen der Dotcom Blase entsprachen (beispielsweise Übernahmen Youtube durch Google). (vgl. Fox 2010; Holtemöller 2010)

Anschlag World Trade Center 2001

Am 11. September 2001 wurde das World Trade Center in der amerikanischen Metropole New York von zwei Flugzeugen getroffen. Dieser Terroranschlag wurde zum Wendepunkt in verschiedenen Bereichen. Einerseits wurden Sicherheitsvorkehrungen sowohl in der Reisebranche als auch bei Versicherungen und Banken erheblich verschärft, was zu höheren Kosten in den betroffenen Unternehmen führte. An der amerikanischen Börse sanken die Kurse und die Zahl der Arbeitslosen stieg. Da die mittel- und langfristigen wirtschaftlichen Folgen dieses Anschlages nicht abgeschätzt werden konnten, sank auch die Zahl an Investitionen in Unternehmen und Anleger hielten aufgrund der Unsicherheit Kapital zurück. Aufgrund des Anschlags fand eine neue Priorisierung verschiedener Risiken statt. Das Risiko eines Terroranschlags und dessen Auswirkungen auf die finanzielle Situation von Unternehmen war zuvor niedrig priorisiert. (vgl. Klein 2007)

Bilanzskandal Enron 2001 (I)

Der Energiekonzern Enron wurde 1985 gegründet und besaß innerhalb der USA das größte Netzwerk von Gas-Pipelines. Bis zum Jahr 2001 weitete Enron seine Tätigkeit aus und betrieb neben den Pipelines außerdem Kraftwerke (Wasser, Strom) sowie Breitband Internet. Zudem handelte Enron an verschiedenen Börsen mit diesen Produkten. Im Jahr 2001 musste der Konzern nach einem der größten Bilanzskandale der USA Insolvenz anmelden. Nach Veröffentlichung der Bilanzzahlen des 3. Quartals 2001 mit einem ausgewiesenen Verlust von über 600 Millionen Dollar und einer Eigenkapitalreduzierung von 1,2 Milliarden Dollar aufgrund von Beteiligungsverträgen, beginnt die US Börsenausficht SEC eine Untersuchung des Unternehmens. Schließlich stellte sich heraus, dass der Energiekonzern die

Umsätze und Gewinne in den Vorjahren zu hoch ausgewiesen hatte. Es wurden nichtexistierende Umsätze in den Bilanzen angegeben. Im Dezember 2001 meldete Enron Konkurs an. Nach Bekanntwerden der Bilanzfälschungen sank der Aktienwert des Unternehmens auf wenige Cent pro Aktie. Zudem wurde bekannt, dass das Management des Konzerns seine eigenen Aktienanteile zuvor zum Höchstpreis veräußert hatte und vor Konkursanmeldung Abfindungen in Millionenhöhe ausbezahlt wurden. Die Wirtschaftsprüfungsgesellschaft Arthur Andersen, welche die Bilanzen des Konzerns prüfte, war ebenfalls in den Skandal verwickelt. Dokumente und Dateien mit Hinweisen auf die Bilanzfälschungen wurden von Mitarbeitern der Arthur Andersen vernichtet. Die Wirtschaftsprüfungsgesellschaft wurde in einem Verfahren zu diesem Fall wegen Behinderung der Justiz zu einer Geldstrafe ($ 500.000,-) verurteilt. (vgl. Eckhaus und Sheaffer 2018; Frentz 2003; vgl. Healy und Palepu 2003)

Der Enron Skandal war der Auslöser zur Einführung des Sarbanes-Oxley Acts, welcher eine Verschärfung der Bilanzierungsgesetze insbesondere Offenlegungspflichten und Kontrollsysteme für ein verbessertes Risikomanagement, vorschrieb. Der Sarbanes-Oxley Act wird in Kapitel 3.2.1 detaillierter beschrieben.

Konkurs Swissair 2002(CH)

Der Konkurs der Schweizer Fluglinie Swissair im Jahr 2002 stellt einen der größten Unternehmenskonkurse des Landes dar. Die Fluglinie galt in den Jahren zuvor als finanziell stabiles Unternehmen und wurde diesbezüglich als „fliegende Bank“ bezeichnet. (Kolmar 2017) Unter anderem durch den Terroranschlag des 11. Septembers und dem damit einhergehenden Rückgang des weltweiten Flugverkehrs wurde die Fluglinie innerhalb weniger Wochen zahlungsunfähig und hatte Schulden in Höhe von 15 Millionen Schweizer Franken auszuweisen. Aufgrund von Unstimmigkeiten mit den beiden Großbanken UBS und Credit Suisse, welche sich zusammen mit der Schweizer Bundesregierung und der Führungsetage der Swissair einen Rettungsplan ausarbeiteten, musste der gesamte Flugbetrieb vorübergehend für einige Tage eingestellt werden. Durch einen Notkredit konnte ein eingeschränkter Flugbetrieb wiederaufgenommen werden, was auch die Erreichbarkeit der Schweiz als Wirtschaftsstandort sichern sollte. Zudem wurde hierdurch die Basis für die heutige Schweizer Fluggesellschaft Swiss geschaffen. Im April 2002 ging die Swissair sowie die Muttergesellschaft SAirGroup in Konkurs sowie Liquidation. (vgl. Kiani-Kreß 2001)

Immobilienblase USA (I) & Finanzkrise (I)

Die weltweite Finanzkrise hat ihren Ursprung in den USA. Hier wurden durch die Regierung die Finanzmärkte dereguliert, zudem wurde nach dem Anschlag auf das World Trade Center und den daraus resultierenden Rückgang an den Börsen und in der gesamten Wirtschaft

mehr Geld gedruckt. Durch niedrige Zinsen wurden Kredite für die gesamte Bevölkerung zugänglich und attraktiv. Hierdurch wurde auch der Immobilienmarkt für den Großteil der Bevölkerung zugänglich, was zu einer hohen Anzahl an Spekulationsgeschäften in dieser Branche führte. Durch das sprunghafte Ansteigen der Geschäfte auf dem Immobilienmarkt kam es ähnlich der Dotcom-Blase zu einer Immobilienblase, welche 2007 platzte und worin die folgende Finanzkrise resultierte. Durch die unzureichende Regulierung der amerikanischen Finanzmärkte kam es zudem zu falschen Ratings und Kreditbewertungen verschiedener Banken und Agenturen. Zudem wurden Kredite über Schattenbanken abgewickelt, um die Bankenaufsicht zu umgehen. So schienen diese Kredite nicht in der Bilanz des Kreditinstitutes auf und hatten somit auch keine Sicherung durch zusätzliches Eigenkapital zur Folge. Durch die Chance der damit beinahe unbegrenzten Möglichkeiten zur Kreditvergabe, verringerte sich auch die Prüfung der Kreditwürdigkeit der Kreditnehmer. Durch das Platzen der Immobilienblase verschlechterte sich die Lage der Banken, worauf Kreditausfälle folgten. Den Höhepunkt stellt laut Literatur die Insolvenz der New Yorker Investmentbank Lehman-Brothers im September 2008 dar. (vgl. Quiring et al. 2013, S. 10) Als Folge der Finanzkrise wurden Banken verstaatlicht und die Risikoabsicherung bei Banken durch Eigenkapital stieg. Risikoprävention und Absicherung erhielten sowohl auf Seiten der Banken als auch der Anleger wieder einen hohen Stellenwert. (vgl. Geiß und Köhler 2013; Quiring et al. 2013)

Auf die zuvor beschriebene Finanzkrise in Amerika folgte auch in Europa eine Bankenkrise und in deren Folge die sogenannte Euro-Krise in Griechenland. Auch europäische Banken stellten für den amerikanischen Kapitalmarkt Kreditgeber dar. Durch die Finanzkrise wurden diese Kredite abgewertet. Zu dieser Zeit galten für Banken in verschiedenen Ländern unterschiedliche Regelungen zur Kreditvergabe und Berichterstattung. Zudem waren die Länder unterschiedlich stark mit dem amerikanischen Kapitalmarkt verknüpft, wodurch die Krise einen größeren Einfluss auf bestimmte Staaten nahm. (vgl. Dijsselbloem 2019)

Schuldenkrise Griechenland (I)

Griechenland wies bereits vor der Bankenkrise in Europa einen hohen Verschuldungsgrad auf. Beispielsweise betrug die Staatsverschuldung bereits in 2004 112%. Zudem erhöhten sich die Löhne von griechische Angestellten in den Jahren vor 2010 um bis zu 80%. Die übrigen Mitglieder der europäischen Union forderten Griechenland zu Sparmaßnahmen auf, um die Staatsverschuldung zu verringern. Die Kreditwürdigkeit Griechenlands sank drastisch. Zudem konnten geplante Sparmaßnahmen von der griechischen Regierung nicht umgesetzt werden. Im Mai des Jahres 2010 einigten sich die übrigen Euroländer unter Beteiligung des Internationalen Währungsfonds auf Hilfskredite, welche mit strengen Maßnahmen verbunden waren. Da diese Maßnahmen keine Entspannung auf den internationalen

Finanzmärkten bewirkten, wurde ein Notfallfonds (Europäische Finanzstabilisierungsfazilität) eingerichtet. (vgl. Agridopoulos und Papagiannopoulos 2016; Dijsselbloem 2019)

Olympus Bilanzskandal (I)

Auch der japanische Konzern Olympus verschleierte, ähnlich dem Fall Enron, über mehrere Jahre Verluste und somit Schulden in seiner Bilanz. Diese Verluste wurden insbesondere als Beraterkosten bei Übernahmegeschäften verbucht und ausgewiesen. Nach Bekanntwerden folgte eine Abwertung des Aktienwertes. Zudem wurde Olympus der Verweis aus der japanischen Börse angedroht, falls erneut Unstimmigkeiten der Bilanzwerte auftreten würden. (vgl. Manager Magazin 2011; WELT 2011)

Konkurs Steinhoff (D)

Das Unternehmen Steinhoff wurde ursprünglich in Deutschland gegründet und durch verschiedene Umstrukturierungen 1998 als Steinhoff International Holdings Ltd an der südafrikanischen Börse in Johannesburg gelistet. Bis 2017 folgten diverse Unternehmensübernahmen sowie Verlagerung der Listung der südafrikanischen Steinhoff Gesellschaft an die Frankfurter Börse. Neben dieser Gesellschaft existierten noch diverse Tochtergesellschaften, unter anderem in Europa und in den Vereinigten Staaten. Ende 2017 wurden, mitunter durch Verweigerung des Testats durch die Wirtschaftsprüfungsgesellschaft Deloitte, Unregelmäßigkeiten in der Steinhoff-Bilanz bekannt. Der Vorstandsvorsitzende verschwand nach Eingestehen der Unregelmäßigkeiten, was mehrere Wechsel im Management innerhalb eines Monats nach sich zog. Zu Beginn 2018 wurden von der deutschen Finanzdienstleistungsaufsicht sowie einer deutschen Staatsanwaltschaft Untersuchungsverfahren gegen den Steinhoff-Konzern eingeleitet, welches einen Prozess nach sich zog. Der Aktienwert fiel an der Börse um über 90% und Steinhoff wies in den Jahren 2017 sowie 2018 hohe Verluste aus (2017: € 6 Milliarden; 2018: € 1,2 Milliarden). (vgl. Mehring 2019; Reuters 2020)

Brexit (I)

Nach diversen Abstimmungen, Verhandlungen und Verschiebungen vollzog Großbritannien im Januar 2020 den Ausstieg aus der europäischen Union. Der sogenannte Brexit brachte zahlreiche außenwirtschaftliche, finanzielle sowie rechtliche Folgen mit sich. Unter anderem beinhaltet dies, dass Tätigkeiten an den Finanzmärkten der EU-Mitgliedsstaaten für Unternehmen und sonstige Teilnehmer aus dem vereinigten Königreich strengeren Regulierungen unterliegen. (vgl. Löbig und Wendt 2019)

Die mit dem Brexit einhergehende Unsicherheit bezüglich der Möglichkeiten und Rahmenbedingungen für geschäftliche Beziehungen nach dem Ablauf der Übergangsfrist, besteht

nach wie vor. Nach Bekanntgabe des Referendums zum Austritt aus der EU fielen die Kurse an der Londoner Börse. Auch das Wirtschaftswachstum Großbritanniens stagniert seitdem, wohingegen die übrigen Industrienationen ein hohes Wirtschaftswachstum aufweisen.[2]

Bilanzskandal Wirecard (D)

Der Bilanzskandal des Konzerns Wirecard, welcher an der deutschen Börse im DAX gelistet war, wurde im Jahr 2020 bekannt. Bei Prüfung der zu veröffentlichenden Bilanz für das Jahr 2019 konnte die Prüfungsgesellschaft Ernst & Young kein Testat erteilen. Die Wirtschaftsprüfungsgesellschaft verwies auf die Vorlage von „*unrichtige Saldenbestätigungen zu Täuschungszwecken".* Konkret handelte es sich hierbei um Guthaben von € 1,9 Milliarden auf Treuhandkonten bei asiatischen Banken. Diese Banken stritten Geschäftsbeziehungen mit Wirecard ab, woraufhin bekannt wurde, dass ausgestellte Bankbestätigungen gefälscht waren und der Betrag auf diesen Treuhandkonten nicht existent ist. Am 25. Juni 2020 stellte Wirecard nach Verhaftung des Vorstandsvorsitzenden den Insolvenzantrag. Der Bilanzskandal stellte neben dem Unternehmen auch den Ruf des Wirtschaftsprüfers Ernst & Young sowie den deutschen Aufsichtsbehörden in Frage. Auch im Fall der Wirecard AG werden Parallelen zum Fall Enron gezogen. (vgl. FINANCE 2021; Knoll 2020; vgl. Rinker 2020; Schäfer 2020)

Bereits zuvor wurde in einem unabhängigen Prüfbericht von KPMG auf das Fehlen des vorgeschriebenen internen Kontrollsystems hingewiesen:

> *„Ein für die Geschäftsaktivitäten der Wirecard AG übliches Internes Kontrollsystem war in den Sachverhalten, die den Vorwürfen zugrunde lagen, nicht eingerichtet. So hat KPMG Schwächen in den Bereichen Forderungsmanagement und Mahnwesen, Vertragsmanagement und -kontrolle sowie in der Berichterstattung identifiziert. Diese wurden ebenfalls von EY Audit im Rahmen der Jahresabschlussprüfung 2018 angemerkt." (Rinker 2020)*

Commerzialbank Mattersburg (AT)

Ein weiterer Bilanzskandal im Jahr 2020 ereignete sich in Österreich bei der im Burgenland ansässigen Commerzialbank Mattersburg. Im Juli 2020 wurden der Bank von der österreichischen Finanzmarktaufsichtsbehörde FMA aufgrund des Verdachtes auf weitreichende Bilanzfälschung jegliche weiteren Geschäfte untersagt. Ebenso wurde eine Anzeige gegen die Commerzialbank wegen Untreue sowie Bilanzfälschung eingebracht. Ähnlich dem Fall Wirecard schienen in der Bilanz der Commerzialbank Mattersburg zahlreiche Konten mit Guthaben bei anderen österreichischen Banken auf, welche nicht existierten und durch gefälschte Bankbestätigungen belegt worden waren. Zudem wurden Einnahmen aus Zinsen

[2] Bezug auf Situation vor Ausbruch der weltweiten Corona Pandemie.

von Schein-Privatkrediten verbucht. Diese Kredite wurden lediglich zum Zwecke des Ausweises der fiktiven Zinseinnahmen angelegt. Es handelte sich hierbei um circa 50% des ausgewiesenen Vermögens. Die Ermittlungen zu diesem Bilanzskandal dauern noch an und richten sich neben dem Tatbestand der Bilanzfälschung auch an die Kontrollfunktion des Aufsichtsrates sowie das Bankenprüfungsunternehmen, welches mit der Prüfung der Commerzialbank beauftragt war. Anleger erhielten die Möglichkeit, über die sogenannte Einlagensicherung Teile ihres Vermögens zurückzufordern. Da die Einlagensicherung allerdings bei € 100.000 pro Kunde gedeckelt ist, verloren Großanleger die Mehrheit ihrer Einlagen. (vgl. Kraemer und Wessel 2021)

Covid-19 Pandemie (ab 2020)

Die Covid-19 Pandemie wird aufgrund der derzeit volatilen Veränderungen und somit unsicheren Auswirkungen in Kapitel 3.3 gesondert behandelt.

Jahr	Ereignis	Lokalisierung	Ursachen	Compliance & Governance Probleme	Folgen/Auswirkungen
2000	Platzen der Dotcom Blase	International	Überbewertung von Unternehmen, da erwartete Gewinne nicht eintrafen	Ausbleibende Gewinne führten nicht zur Abwertung von Unternehmen, zu hohe vorausgesagte Gewinne	Überarbeitung der Bewertungsverfahren Rezession an Börsen, Anzahl Internet Unternehmen nahm ab
2001	Anschlag 9/11 World Trade Center	International	Sicherheitslücken	Sicherheitslücken Terrorismus nicht als potenzielles Risiko priorisiert	Erhöhung Sicherheitsstandards im Flugverkehr und Versicherungsbranche, sinkende Reisebereitschaft, sinkende Kurse an amerikanischer Börse
2001	Bilanzskandal Enron	International	Bilanzfälschung	Unzureichende Offenlegungs- sowie Kontrollpflichten, WP Gesellschaften nicht unabhängig, Korruption	Ausweitung Berichtspflichten bezüglich Risikomanagement Sarbanes-Oxley Act
2002	Konkurs Swissair	Schweiz	sinkendes Reiseverhalten nach 9/11, Unstimmigkeiten mit Banken	Unzureichende Betrachtung von Risiken und deren Auswirkungen	Erweiterung Berichtspflichten bezüglich Risiken Priorisierung Terrorismus als Risiko
2007	Immobilienblase USA	International	Spekulationsgeschäfte, niedrige Kreditzinsen	Deregulierung der US-Börsen, falsche Rating-/Kreditbewertungen Unzureichende Risikoabsicherung	Risikoabsicherung durch Eigenkapital, Bankenverstaatlichung Maßnahmen zur Risikoprävention
2007/2008	Finanzkrise	International			
2010	Schuldenkrise Griechenland	International	Hohe Staatsverschuldung, Bankenkrise Europa	Keine einheitliche europäische Regelung zu Staatsverschuldung	Internationale Betrachtung von Risiken Auswirkungen/Risiken anderer Krisen und Risikoaggregation
2011	Olympus Bilanzskandal	International	Bilanzfälschung	Unzureichende Prüfung	Erweiterung/Konkretisierung/Verschärfung Prüfungspflichten
2017	Konkurs Steinhoff	Deutschland	Bilanzfälschung	komplexes Konzerngefüge, unzureichende Transparenz in Bilanzen	Erweiterung Transparenz in Konzernbilanzen
2018-2020	Brexit	International	Referendum	n/a	strengere Regulierungen am britischen Finanzmarkt, Unsicherheit zu Geschäften mit GB, stagnierendes Wirtschaftswachstum in GB
Ab 2020	Corona Pandemie	International		Pandemie als Risiko nicht betrachtet	Aufnahme von pandemischen Risiken in Risikomanagement
2020	Bilanzskandal Wirecard	Deutschland	Bilanzfälschung	unzureichende Prüfung in Vorjahren, Korruption	Erweiterung Prüfungspflichten Prüfung der deutschen Aufsichtsbehörden
2020	Commerzialbank Mattersburg	Österreich	Bilanzfälschung	Aufsichtsrat nicht unabhängig Unzureichende Prüfung der Bilanzen	Revision Regelung Einlagensicherung Erweiterung Prüfungspflichten

Abbildung 4: Ereignisse und deren Auslöser und Auswirkungen

3.2 Gesetzliche und sonstige Anforderungen an Risikomanagement und deren Veränderung

In der vorliegenden Masterarbeit werden, neben international gültigen Standards, als Basis die lokalen Gesetze der DACH-Region analysiert, welche Aktiengesellschaften sowie GmbHs betreffen. Hierbei handelt es sich in erster Linie um das Handelsgesetzbuch und Aktiengesetz für Deutschland, das Unternehmensgesetzbuch für Österreich sowie das Schweizer Obligationenrecht. Es werden jeweils die Gesetze sowie deren Änderungen untersucht. Zudem werden in der vorliegenden Arbeit die Regulatorien, welche spezifisch für den Finanz- und Versicherungsbereich gelten, aufgrund des Umfangs ausgeschlossen. Eine gesammelte Aufstellung der relevanten Gesetzesänderungen sowie deren Inhalt und Begründungen befindet sich im Anhang dieser Arbeit (A2-digital).

Für das Risikomanagement von Unternehmen existieren zahlreiche Gesetze sowie quasigesetzliche Anforderungen. Neben der jeweils nationalen Gesetzgebung bestehen auch internationale Standards, welche sich allerdings in Umfang und Tiefe der genannten Anforderungen an das Risikomanagement unterscheiden. Die gesetzlichen Rahmenbedingungen für das Risikomanagement haben sich über die vergangenen Jahre verändert. Die folgenden Abbildungen zeigen die Rahmenbedingungen jeweils in den Jahren 2006 sowie 2020.

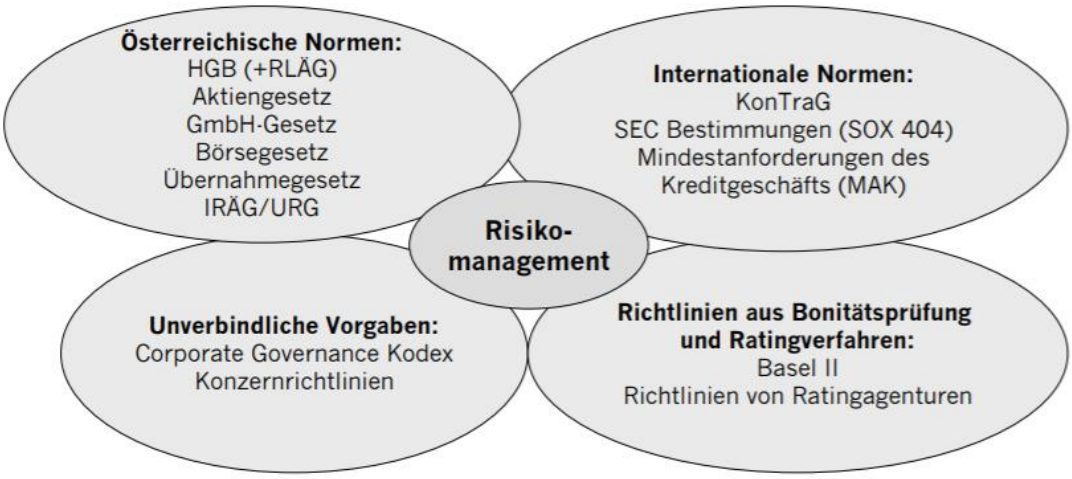

Abbildung 5: Rahmenbedingungen für das Risikomanagement im Unternehmen 2006
Quelle: Denk et al. 2006, S. 11

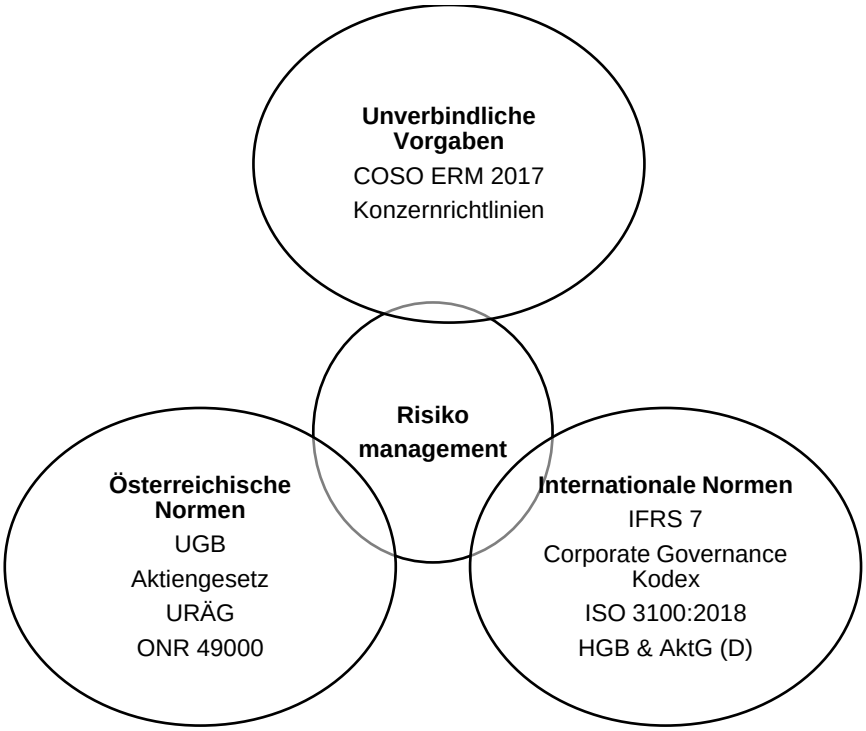

Abbildung 6: Aktuelle Rahmenbedingungen für das Risikomanagement
Quelle: Eigene Abbildung nach 3GRC 2018, S. 22–29; Institut für Interne Revision Österreich 2014, S. 22–29

Die beiden Abbildungen verdeutlichen, dass sich in der Vergangenheit unverbindliche Vorgaben zu verbindlichen Normen entwickelt haben.

3.2.1 Internationale Gesetzgebung und Standards

Im Bereich der internationalen Standards und Gesetze wird in dieser Arbeit auf den Sarbanes-Oxley Act als Grundlage für viele lokale Gesetzgebungen, den Enterprise Risk Management Standard des COSO Komitees sowie die Norm ISO 31000 eingegangen.

Sarbanes-Oxley Act (2002)

Im Jahr 2002 wurde in den Vereinigten Staaten von Amerika der sogenannte Sarbanes-Oxley Act verabschiedet, welcher als ein sehr weitreichendes Gesetz zum Risikomanagement gilt. Nach zahlreichen Bilanzskandalen sowie Bilanzbetrug in den vorhergehenden Jahren soll der Sarbanes-Oxley Act das Vertrauen von Anlegern zurückgewinnen und zu stärken. Ziel des SOX ist es, Bilanzmanipulationen und die damit einhergehenden Folgen zu verhindern. Es handelt sich um eine Erweiterung und Spezifizierung der bis dorthin geltenden Corporate Governance Regeln und beinhaltet eine Verschärfung der Offenlegungspflichten, Informationsvorschriften, Kontrollsysteme und strafrechtliche Konsequenzen bei Nichtbeachtung. (vgl. Biel 2005; Nicklisch 2007)

Der SOX gilt für alle an der amerikanischen Börse gelisteten Gesellschaften, unabhängig deren Firmensitz. Dies bedeutet, dass sowohl amerikanische als auch ausländische Unternehmen, welche an einer US-Börse gelistet sind (auch Zweitnotierung), die Vorgaben umzusetzen haben. Weiter erstreckt sich der Geltungsbereich auf alle Wirtschaftsprüfer, welche Prüfungsdienstleistungen für die zuvor genannten Unternehmen durchführen. Dies gilt auch für alle Wirtschaftsprüfer, welche Tochtergesellschaften von in den USA gelisteten amerikanischen Unternehmen prüfen, unabhängig davon, ob sich diese Tochtergesellschaften in den USA befinden. (vgl. Von der Crone und Roth 2003)

Unter anderem beinhaltet der SOX folgende Vorgaben (vgl. Hart 2009; Von der Crone und Roth 2003):

- Quartalsberichte und sonstige Abschlussberichte von US-Publikumsgesellschaften sind jeweils von CEO als auch von CFO des Unternehmens zu unterzeichnen und somit zu beglaubigen. Sollten hier fahrlässig falsche oder unvollständige Informationen bestätigt werden, sind strafrechtliche Konsequenzen möglich.
- Kürzere Fristen für Veröffentlichung von Quartals- und Jahresberichten
- Die Mehrheit der Aufsichtsratsmitglieder muss unabhängig sein
- Der zu bildende Prüfungsausschuss muss unabhängig sein, wobei mindestens ein Finanzexperte erforderlich ist
- Prüfer dürfen nicht zugleich Unternehmensberater desselben Unternehmens sein
- Außerbilanzielle Vorgänge müssen in der Bilanz, unter Angabe von kurz- und langfristigen Auswirkungen und vertraglichen Verpflichtungen, detailliert aufgeführt werden
- Einführung eines zentralen Aufsichtsorgans für in den USA börsennotierte Gesellschaften und deren Prüfungsgesellschaften (*PCAOB*) zur Umsetzung der Regelungen

Der SOX erhielt zunächst umfangreiche Kritik von den betroffenen Unternehmen, da diese weitreichenden Maßnahmen auch eine erhebliche interne Kostensteigerung mit sich brachten. Allerdings führen die strengeren Regeln zu niedrigeren Kapitalkosten sowie einer größeren Investitionsbereitschaft bei möglichen Investoren. (vgl. Coates, IV 2007)

Der Sarbanes-Oxley Act bildet die Basis für zahlreiche europäische Gesetzgebungen. Allgemein wurde allerdings durch die Europäische Gemeinschaft als Gesetzgeber sowie die einzelnen nationalen Gesetzgebungen versucht, jeweils individuelle Regelungen zu erlassen und kein europäisches Imitat des Sarbanes-Oxley Act zu entwickeln.

COSO-ERM Framework (2004/2017)

Der COSO Standard wurde zunächst in 2004 veröffentlicht. Dieser ursprüngliche Standard stellte das Risikomanagement als Würfel dar. In der überarbeiteten Version aus 2017 wurde das Würfel-Modell durch ein Prozessmodel erneuert.

Im COSO Standard werden neben allgemeinen Begriffen auch das unternehmensweite Risikomanagement, Zielkategorien und deren Erreichung, Komponenten des Risikomanagements sowie Funktionsfähigkeit, Einschränkungen, Verantwortlichkeiten und Berichterstattung erläutert.

Das Würfel-Modell aus 2004 basiert darauf, dass Beziehungen zwischen den Zielen eines Unternehmens und den verschiedenen Komponenten des Risikomanagements im Unternehmen, existieren. Laut dieser Annahme geben die Komponenten wieder, was zum Erreichen der Unternehmensziele nötig ist. Diese Beziehungen sind im Würfel-Modell dreidimensional dargestellt. Im Würfel sind vier Zielkategorien, acht Komponenten sowie vier Einheiten einer Organisation dargestellt. (vgl. COSO 2004)

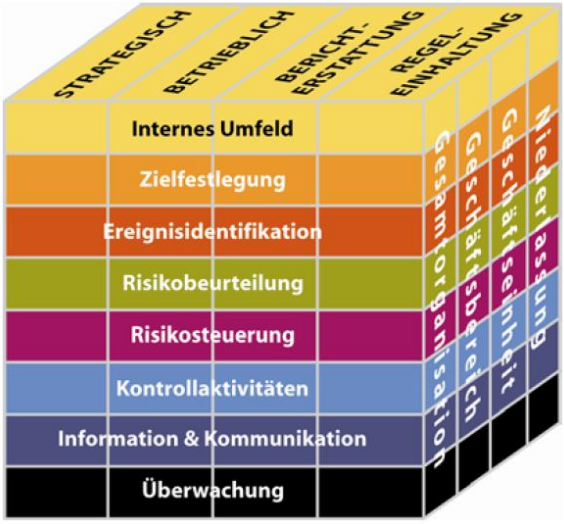

Abbildung 7: COSO ERM Würfel Modell 2004
Quelle: COSO 2004, S.5

In der Neufassung aus 2017 wurde ein dreistufiges Prozessmodell eingeführt. Durch die drei Stufen „1. Mission, Vision and Core Values“, „2. Strategy and Business Objectives” und “3. Enhanced Performance” werden insbesondere eine umfassendere Beziehung zwischen diesen Komponenten sowie die Unternehmenskultur (Stufe 1) stärker in den Vordergrund gestellt. In das Dreistufen-Modell werden die Komponenten und Prinzipien eingefügt. Anders als im ursprünglichen Würfel-Modell wird hier in lediglich fünf Komponenten unterteilt. Diese Komponenten werden durch insgesamt 20 Prinzipien ergänzt. Diese Unterteilung

entspricht jener aus dem Rahmenwerk *COSO-IKS 2013*. Abbildung 8 zeigt das überarbeitete Modell unter Angabe der Komponenten und Prinzipien. (vgl. COSO 2017)

Abbildung 8: COSO ERM Prozessmodell 2017
Quelle: COSO 2017, S.6f

ISO 31000 (2009/2018)

Im Jahr 2009 wurde die ISO 310000 eingeführt, welche 2018 überabeitet wurde. Diese Norm gliedert sich neben der Angabe des Anwendungsbereichs in folgende Bereiche:

- Begriffe und Definitionen
- Grundsätze des Risikomanagements
- Beschreibung Risikomanagementsystem
- Beschreibung Risikomanagementprozess

Die ISO 31000 bildet eine Grundlage für das Risikomanagement, dessen Anwendung je nach Branche bzw. Anwendungsbereich angepasst werden muss. (Weis 2012)

Damit ein Risikomanagement effektiv wirkt, muss dies laut ISO 31000 *„integriert, strukturiert, umfassend, maßgeschneidert, einbeziehend und dynamisch“* sein. Ebenso müssen menschliche Faktoren berücksichtigt werden und alle erreichbaren Informationen herange-

zogen werden. Das Risikomanagement muss außerdem kontinuierlich analysiert und verbessert werden. Die Norm definiert zudem Bestandteile des Risikomanagementsystems sowie des dazugehörigen Prozesses, welcher bereits ähnlich in Kapitel 2.2 beschrieben wurde. Abbildung 9 zeigt die Bestandteile des Risikomanagementsystems sowie des Risikomanagementprozesses laut ISO 31000.

Abbildung 9: Bestandteile von RMS & Risikomanagementprozess
Quelle: Eigene Abbildung nach ISO 31000

Die Neuerungen der Version aus dem Jahr 2018 lassen sich wie folgt zusammenfassen (Tranchard 2018):

- Überprüfung der Grundsätze
- Risikomanagement als Aufgabe des Top-Managements im Unternehmen
- Risikomanagement als iterativer Prozess
- Risikomanagement als offenes Systemmodel mit externem Feedback, um einem breiteren Kontext und Bedürfnissen gerecht zu werden

3.2.2 Deutsche Gesetzgebung und Standards

Die Grundlage des deutschen Unternehmensrechts bildet das HGB. Im HGB wurde das Risikomanagement 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verankert, welches bereits vor dem beschriebenen Sarbanes-Oxley Act erlassen wurde. Bis zur Gegenwart erfolgten regelmäßige Änderungen verschiedener Paragraphen des HGB sowie der verschiedenen Gesellschaftsrechte wie Aktiengesetz und GmbH-Gesetz, welche das Risikomanagement betreffen, die im Folgenden chronologisch erläutert werden. Hierbei wird lediglich auf die Änderungen, welche das Risikomanagement betreffen, eingegangen.

Gesetz zur Kontrolle und Transparenz (1998)

Das KonTraG bildet die Basis zur Verankerung des Risikomanagements in der deutschen Gesetzgebung. Die Begründung dieses Artikelgesetzes zur Änderung des HGB und weiterführender Gesetzgebung wird in der Literatur unter anderem mit den Unternehmenskonkursen verschiedener Deutscher Konzerne in den 1990er Jahren (u.a. Balsam AG, Metallgesellschaft AG, Klöckner-Humboldt-Deutz AG, Dr. Jürgen Schneider AG) begründet. Die Risikomanagement-relevanten Änderungen lassen sich in die Aufgaben der Gesellschaftsorgane, die Pflicht zur Berichterstattung sowie die Prüfung der Berichterstattung unterteilen. Allgemein wird durch das KonTraG die Pflicht für ein Überwachungssystem für Risiken und damit einhergehende Berichtspflichten und Prüfungspflichten vorgeschrieben. Eine Vorgabe zu Form, Umfang oder Inhalt wird allerdings nicht gegeben.

In § 92 Abs. 2 AktG wird die Pflicht des Vorstandes festgeschrieben, ein Überwachungssystem einzurichten, um Risiken, welche das Unternehmen gefährden, frühzeitig zu erkennen.

> *Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.* (§ 92 Abs. 2 AktG)

Durch § 111 Abs. 2 Satz 3 AktG wird die Zuständigkeit für die Erteilung des Prüfauftrages des Jahresabschlusses bzw. Konzernabschlusses dem Aufsichtsrat übertragen. Zuvor war hierfür der Vorstand verantwortlich.

Durch die beiden Änderungen zu § 289 HGB sowie § 315 HGB wird der (Konzern-) Lagebericht um den Aspekt der Chancen und Risiken erweitert.

Durch § 289 Abs. 1 HGB soll sichergestellt werden, dass der Aufsichtsrat umfassend über die Lage des Unternehmens und dessen mögliche Gefährdungen informiert wird.

> *[…] voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern.* (§ 289 Abs. 1 HGB)

§ 315 Abs. 1 HGB legt fest, dass diese Regelung analog für den Konzernlagebericht gilt.

Abschließend werden in § 317 HGB Regelungen für die Prüfung des Abschlussberichts dargelegt. Ergänzend zu § 289 Abs. 1 HGB dient auch § 317 Absatz 2 HGB dazu, den Aufsichtsrat umfassender über die Lage des Unternehmens und dessen mögliche Gefährdung zu unterrichten.

> *[…] zutreffendes Bild der Lage […] Dabei ist auch zu prüfen, ob die Chancen und Risiken der künftigen Entwicklungen zutreffend dargestellt sind.* (§ 317 Abs. 2 HGB)

Absatz 4 schließt die Verbindung zum bereits zuvor beschriebenen Aktiengesetz und den Aufgaben des Vorstandes.

> *Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.* (§ 317 Abs. 4 HGB)

Zusammenfassend wird anhand dieser Änderungen festgelegt, dass ein angemessenes Risikomanagement im Unternehmen zu erfolgen hat und dies auch auf seine Funktion und Wirkung geprüft wird. Eine Vorgabe zu konkreten Maßnahmen wird nicht gemacht, was einen gewissen Auslegungsspielraum des Gesetzes erlaubt. In folgenden Standards werden Rahmenbedingungen für den Inhalt des Systems gegeben.

Transparenz und Publizitätsgesetz (2002)

Das TransPuG wurde im Jahr 2002 verabschiedet. Auch hier sind diverse Unternehmenskonkurse ausschlaggebend. Eine entscheidende Rolle spielte hierbei die Unternehmenskrise der Phillipp Holzmann AG, welche bis zum Konkurs im Jahr 2002 als das größte deutsche Bauunternehmen galt. Nach 150-jährigem Bestehen wurde 1999 bekannt, dass das Unternehmen aufgrund versteckter Schulden überschuldet war. Nach diversen Sanierungsmaßnahmen und von der Bundesregierung initiierten Rettungspaketen scheiterte die Sanierung im Jahr 2002 und der Konkurs Phillipp Holzmann AG folgte. Diese und ähnliche Unternehmensinsolvenzen gaben Anlass zu Verschärfungen und Konkretisierungen im Unternehmens- und insbesondere im Bilanzrecht. (vgl. Stephan 2006, S.1)

Das TransPuG bringt erweiterte Berichtspflichten und Formvorgaben mit sich. Ziel dieses Änderungsgesetzes ist es, die Unternehmensführung und deren Entscheidungen transparenter zu machen und durch diese Transparenz die Attraktivität des deutschen Anlegermarktes für ausländische Investoren zu erhöhen. (vgl. Diederichs 2012, S. 24)

Eine konkrete neue Vorschrift für den Vorstand stellt die Entsprechenserklärung gemäß § 161 AktG dar. Hierbei müssen sich die Führungsorgane von börsennotierten Gesellschaften jährlich zum deutschen Corporate Governance Codex[3] bekennen. Diese Erklärung ist der Öffentlichkeit entsprechend zugänglich zu machen.

> *„Vorstand und Aufsichtsrat der börsennotierten Gesellschaft erklären jährlich, dass den vom Bundesministerium der Justiz und für Verbraucherschutz im amtlichen Teil des Bundesanzeigers bekannt gemachten Empfehlungen der „Regierungskommission Deutscher Corporate Governance Kodex" entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht. Gleiches gilt für Vorstand und Aufsichtsrat einer Gesellschaft, die ausschließlich andere Wertpapiere als Aktien zum Handel an einem organisierten Markt im Sinn des § 2 Absatz 11 des Wertpapierhandelsgesetzes ausgegeben hat und deren ausgegebene Aktien auf eigene Veranlassung über ein multilaterales Handelssystem im Sinn des § 2 Absatz 8 Satz 1 Nummer 8 des Wertpapierhandelsgesetzes gehandelt werden." (§ 161 Abs. 1 AktG)*
>
> *„Die Erklärung ist auf der Internetseite der Gesellschaft dauerhaft öffentlich zugänglich zu machen." (§ 161 Abs. 2 AktG)*

Bilanzrechtsreformgesetz (2004)

Aufgrund des Bilanzrechtsreformgesetzes (BilReG) wurden Unternehmen verpflichtet, eine Darstellung von Chancen und Risiken unter Angabe der zugrundeliegenden Annahmen im Lagebericht zu veröffentlichen. Dieses Gesetz ist von allen mittelgroßen und großen Unternehmen gemäß HBG sowie von Konzernen anzuwenden. Ebenso wurden auch die Pflichten des Wirtschaftsprüfers erweitert. (vgl. Diederichs 2012, S. 24)

Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (2005)

Das UMAG ist auf Aktiengesellschaften anzuwenden. Durch dieses Gesetz wurde im Aktiengesetz unter § 93 I die „*Business Judgement Rule*" eingeführt. Diese erweitert die Sorgfaltspflichten im Rahmen unternehmerischer Entscheidungen. Entscheidungen sind demnach *„auf Grundlage angemessener Informationen zu treffen".* (Diederichs 2012, S. 24)

Bilanzrechtsmodernisierungsgesetz (2009)

Im BilMoG, welches für Aktiengesellschaften gilt, wurden sowohl die Überwachungspflichten des Aufsichtsrates als auch die Prüfungspflichten des Wirtschaftsprüfers konkretisiert. Demnach unterliegt der Aufsichtsrat der Pflicht, das vorgeschriebene IKS, das Risikomanagementsystem sowie das interne Revisionssystem auf deren Wirksamkeit zu überprüfen und zu überwachen. Ebenso muss der Rechnungslegungsprozess überwacht werden. Der Wirtschaftsprüfer hat diese Systeme zu überprüfen. (vgl. Diederichs 2012, S. 24)

[3] Der DCGK ist nicht Bestandteil der vorliegenden Arbeit. Dieser kann unter https://www.dcgk.de/de/ abgerufen werden.

IDW PS 981 (2017)

Der Prüfungsstandard 981 behandelt die Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen. Der Standard erläutert den Inhalt von freiwilligen Prüfungen eines Risikomanagementsystems sowie die Aufgaben des Wirtschaftsprüfers. Unter anderem werden die Grundelemente eines Risikomanagementsystems sowie anerkannte Rahmenbedingungen definiert und erläutert. Aufgrund des Umfangs des Prüfungsstandards wird auf eine detaillierte Beschreibung verzichtet, der vollständige IDW PS 981 befindet sich im Anhang dieser Arbeit (A1).

IDW PS 340 (1999/2020)

Im Jahr 2020 wurde der ursprüngliche IDW Prüfungsstandard 340 aus dem Jahr 1999 überarbeitet. Insbesondere enthält die Neufassung des Standards folgende Elemente:

- Elemente eines Risikofrüherkennungssystems werden spezifiziert
- Unternehmenspflichten zu Risikotragfähigkeit und Risikoaggregation
- Konkretisierung der Dokumentationspflichten basierend auf der aktuellen Gesetzgebung
- Überarbeitung Berichterstattung des Abschlussprüfers

Der IDW Prüfungsstandard 340 enthält ähnlich dem IDW PS 981 Begriffsdefinitionen, Umsetzungshinweise, Erläuterungen sowie Beschreibungen von Maßnahmen der gesetzlichen Anforderungen in HGB und AktG, insbesondere § 92 Abs. 2 AktG, und konkretisiert somit die zuvor beschriebenen Anforderungen aus den verschiedenen Gesetzestexten. (vgl. IDW EPS 340 n.F.)

Die nach § 92 Abs. 2 AktG geforderten Maßnahmen zum Risikofrüherkennungssystem werden systematisch definiert und erläutert. Zu den Grundelementen zählen hiernach eine Risikokultur im Unternehmen, die Ziele sowie Organisation der Maßnahmen, die Identifikation, Bewertung, Steuerung und Kommunikation des Risikos, sowie abschließend die Überwachung und Verbesserung. Zudem müssen die Maßnahmen durch den Vorstand umfassend dokumentiert werden. Konzernunternehmen müssen in die Maßnahmen miteinbezogen werden, insofern von ihnen bestandsgefährdende Entwicklungen für das Mutterunternehmen ausgehen können. (vgl. IDW EPS 340 n.F.)

Auch der Prüfumfang des Abschlussprüfers sowie dessen Kompetenzen und Pflichten werden in diesem Prüfungsstandard beschrieben. Dies reicht von der Auftragsannahme über die Planung und Durchführung der Prüfung bis zur Berichterstattung nach erfolgter Abschlussprüfung des Risikomanagementsystems. (vgl. IDW EPS 340 n.F.)

Abschließend befinden sich im Anhang des Prüfungsstandards 340 detaillierte Informationen zu verwendeten Begrifflichkeiten und Umsetzungshinweise. Unter anderem werden hier in Ziffer A3 bestandsgefährdende Risiken im Sinne des § 92 Abs. 2 AktG erläutert. (vgl. IDW EPS 340 n.F.)

Stabilisierungs- und Restrukturierungsgesetz (2021)

Das StaRUG gilt seit Beginn des Jahres 2021. Dieses Gesetz beinhaltet erweiterte Restrukturierungsmaßnahmen für Unternehmen abseits eines Insolvenzverfahrens. Auch die bereits zuvor für Aktiengesellschaften geltende Verpflichtung zu einem Risikofrüherkennungssystem wurde auf alle haftungsbeschränkten Unternehmen erweitert. Zudem bedarf es einem Krisenmanagementsystem. Dies wird in §1 StaRUG *„Krisenfrüherkennung und Krisenmanagement bei haftungsbeschränkten Unternehmensträgern“* verankert. Die Geschäftsführung solcher Unternehmen wird verpflichtet, bestandsgefährdende Entwicklungen zu überwachen und bei deren Eintreten mit entsprechenden Gegenmaßnahmen zu reagieren. (vgl. Ebner Stolz 2021; Volmer und Köllmer 2020)

3.2.3 Österreichische Gesetzgebung und Standards

In Österreich wird das Gesellschaftsrecht durch das Unternehmensgesetzbuch (UGB) sowie einzelnen Gesetzen für jede Gesellschaftsform geregelt. Für die vorliegende Arbeit sind neben dem UGB das Aktiengesetz sowie das GmbH-Gesetz relevant. Im Vergleich zur deutschen Gesetzgebung gab es hier in der Vergangenheit wenige Anpassungen. Im Betrachtungszeitraum stellt das Unternehmensrechtsänderungsgesetz aus dem Jahr 2008 die nationale gesetzliche Verankerung für das Risikomanagement dar.

URÄG 2008

Eine Änderung in der österreichischen Gesetzgebung, welche das Risikomanagement betrifft, wurde 2008 durch das Unternehmensrechts-Änderungsgesetz 2008 *(URÄG 2008)* vorgenommen. Hier wurde sowohl eine Änderung im Unternehmensgesetzbuch UGB, im GmbH-Gesetz als auch im Aktiengesetz getroffen. Unter anderem muss durch die Änderung des Aktiengesetzes 1965 bei börsennotierten Unternehmen ein von der Geschäftsführung unabhängiger Prüfungsausschuss eingerichtet werden, welcher auch für „*die Überwachung der Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems, und des Risikomanagementsystems der Gesellschaft;“* verantwortlich ist (URÄG 2008, Art 2 Abs 2).

Das URÄG ist eine Reaktion des österreichischen Staates auf den zuvor bereits beschriebenen Sarbanes-Oxley Act. Die Gesetzesänderung soll im österreichischen Recht Mängel

bei Rechnungslegung sowie Abschlussprüfung beheben. Zudem setzt das Gesetz die Europäische Änderungsrichtlinie, welche die Bilanzierung betrifft, um. Im Folgenden werden die bedeutendsten Änderungen und Ergänzungen, welche das Risikomanagement und dessen Berichterstattung behandeln, beschrieben. (vgl. Milla et al. 2008, S. 16f)

Grundsätzlich lassen sich die Änderungen in die Gruppen Berichterstattung und Aufgaben der unterschiedlichen Unternehmensorgane untergliedern. Mit § 243a UGB erfolgt eine Erweiterung des Inhaltes des Lageberichts, dieser muss die wichtigsten Merkmale des IKS sowie des RMS enthalten.

> *„Eine Gesellschaft […] hat im Lagebericht darüber hinaus die wichtigsten Merkmale des internen Kontroll- und Risikomanagementsystems in Hinblick auf den Rechnungslegungsprozess zu beschreiben." § 243a (2) UGB*

Gemäß § 267 (3b) UGB gilt dies auch für den Konzernlagebericht von Muttergesellschaften. Im Konzernlagebericht muss somit über das IKS und RMS auf Konzernebene berichtet werden.

Zudem wird die Berichterstattung um einen verpflichtenden Corporate Governance Bericht erweitert. In dieser nicht finanziellen Erklärung müssen unter anderem bestandsgefährdende Risiken sowie deren Handhabung durch das Unternehmen und alle Informationen, welche zum Verständnis des Geschäftsverlaufs, des Ergebnisses sowie der Lage notwendig sind, bereitgestellt werden.

> *„Die nichtfinanzielle Erklärung hat diejenigen Angaben zu enthalten, die für das Verständnis des Geschäftsverlaufs, des Geschäftsergebnisses, der Lage der Gesellschaft sowie der Auswirkungen ihrer Tätigkeit erforderlich sind […]" § 243b (2) UGB*

> *„Die Die Angaben nach Abs. 2 haben zu umfassen:*
> *[…]*
> *5. die wesentlichen Risiken, die wahrscheinlich negative Auswirkungen auf diese Belange haben werden, und die Handhabung dieser Risiken durch die Gesellschaft […]" § 243b (3) UGB*

Zusätzlich müssen auch Risiken und Vorteile von außerbilanziellen Geschäften unter den ergänzenden Angaben aufgeführt werden, sofern diese als wesentlich für das Unternehmen angesehen werden können. Diese Angaben sind für eine realitätsgetreue Einschätzung der Unternehmenslage essentiell. Die ergänzenden Angaben werden in § 237 Z. 8a UGB spezifiziert.

Neben den Ergänzungen zur Berichterstattung werden durch das URÄG Aufgaben für die verschiedenen Gesellschaftsorgane definiert beziehungsweise konkretisiert. Dem Prüfungsausschuss wird im Aktiengesetz als auch im GmbH-Gesetz die Aufgabe übertragen, die Wirksamkeit des IKS sowie des RMS zu überwachen. Es werden allerdings keine weiteren Angaben zum genauen Umfang und Inhalt der Aufgaben gemacht.

„Zu den Aufgaben des Prüfungsausschusses gehören:
[…]
2. die Überwachung der Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems, und des Risikomanagementsystems der Gesellschaft;“ § 92 (4a) AktG; § 30g (4a) GmbHG

ONR 49000 ff. (2014/2008/2004)

Die österreichische Norm ONR 49000 existiert seit 2004 und wurde 2008 sowie 2014 überarbeitet. Seit Einführung der ISO 31000 konkretisiert die ONR 49000 die Anwendung der internationalen Norm. Dies wurde im Zuge der Überarbeitungen in 2008 sowie 2014 bewirkt. So stellt auch die ONR eine Unterstützung zur Umsetzung des geforderten Risikomanagements dar. Bereits in 2004 wurde die erste Version der Risikomanagementnorm mit Begriffsdefinitionen und Anwendungshinweisen in Österreich veröffentlicht, welche wiederum in die Erarbeitung der späteren ISO Norm einfloss. (vgl. Brühwiler 2008)

Da die Norm ISO 31000 bereits in Kapitel 3.2.1 beschrieben wurde, wird auf eine detaillierte Ausführung zu den ONR 49000 Versionen aus 2008 sowie 2014 verzichtet.

3.2.4 Schweizer Gesetzgebung

Auch in der Schweiz existieren im Vergleich zu Deutschland deutlich weniger in nationalen Gesetzen verankerte Vorgaben zum unternehmerischen Risikomanagement. Hier wurde im Jahr 2005 im Obligationenrecht eine gesetzliche Berichtspflicht für eine Risikobeurteilung im Rahmen des Jahresabschlusses eingeführt, welche allerdings sehr knapp ausfällt.

„Der Anhang enthält:
[…]
12. Angaben über die Durchführung einer Risikobeurteilung;“ Art. 663b Ziff. 12 OR

Im Jahr 2008 fand eine Revision des Schweizer Aktienrechts (AR) statt. Nach dieser Gesetzesänderung trägt der Verwaltungsrat die Verantwortlichkeit für das Vorhandensein eines IKS sowie dessen Wirksamkeit. Risikomanagement wird hier nicht explizit erwähnt, allerdings beinhaltet das IKS sowie weitere Vorgaben einzelne Komponenten des Risikomanagements. (vgl. VR Wissen)

Die Risikobeurteilung wurde dem Anhang zugeordnet und stellte somit einen ordentlichen Bestandteil des Jahresberichts dar. Im Obligationenrecht fanden sich keine Angaben, ob diese Regelung auch für Konzerne zutrifft. Die Regelungen waren lediglich für einzelne Aktiengesellschaften ausgelegt. (vgl. Bitterli und Fallegger 2018, S. 117f)

Im Jahr 2013 trat ein neues Rechnungslegungsgesetz in Kraft, welches die Regelung zur Risikobeurteilung im Jahresbericht auf große Unternehmen beschränkt. Große Unternehmen müssen ab dieser Revision anstatt im Anhang darüber zu berichten, einen Lagebericht mit Risikoeinschätzung erstellen. (Art. 691c OR)

Vorgaben zu Struktur und Form des Lageberichts werden im Rahmen des Obligationenrechts nur sehr wenige gemacht. Gestaltungshinweise und Prinzipen werden beispielsweise durch das „Schweizer Handbuch der Wirtschaftsprüfung“ oder andere Artikel des OR gegeben. (vgl. Bitterli und Fallegger 2018, S. 119)

In der Schweiz wird die gesetzliche Verankerung zur Risikoberichterstattung neben den Entwicklungen rund um den Sarbanes-Oxley Act auch mit nationalen Unternehmenskonkursen, wie beispielsweise dem Swissair Konkurs 2002 begründet. (vgl. KMU-Portal 2021; VR Wissen)

3.3 Covid-19 als Großereignis

Auch die weltweite Covid-19 Pandemie wird Auswirkungen auf das Risikomanagement in Konzernen haben. Um das Risikomanagement ganzheitlicher auszurichten und somit das Unternehmen für künftige unerwartete Ereignisse besser aufzustellen, muss sich das Risikomanagement schneller an neue Situationen anpassen können. Oft wird Risikomanagement vergangenheitsorientiert ausgerichtet, was bedeutet, dass das eigene Risikomanagement aufgrund vergangener Ereignisse oder Gesetzesänderungen angepasst wird. In der Corona-Pandemie ist das aufgrund der neuartigen Situation nicht möglich, wodurch neue Ansätze im Risikomanagement erarbeitet und verfolgt werden müssen. Die Neuausrichtung des Risikomanagements muss in Einklang mit den aktuell geltenden behördlichen Verordnungen aber auch den persönlichen Bedürfnissen aller Stakeholder der Organisation stehen. (vgl. Boecker und Zwirner 2020)

Erste Studien zum Thema Risikomanagement und Covid-19 zeigen, dass vor Beginn der Pandemie nur circa 30% der befragten Unternehmen in der EMEA Region einen Pandemieplan vorweisen konnten. Das Risiko einer Pandemie zählte bei über 80% der Unternehmen nicht zu den Top-10 Risiken, in 2019 lag eine Pandemie auf Platz 60 der laut Studie 69 identifizierten Risiken. Durch die Covid-19 Pandemie wird eine neue Priorisierung der Risiken, insbesondere Risiken durch Pandemien/Epidemien stattfinden. (vgl. AON 2021; AssCompact 2021)

Unterschiedliche Branchen, aber auch unterschiedliche Bereiche innerhalb einer Organisation, sind unterschiedlich schwer von der Pandemie betroffen. Eine weitere Studie zeigt, dass insbesondere die Supply Chain, Umsatz und Gewinnmarge sowie die Auftragslage

negativ von der Krise beeinflusst werden, wohingegen die Pandemie keine signifikante Auswirkung auf die Produktivität von Mitarbeitenden hat. In dieser Studie zeigt sich auch, dass für ein effektives Risikomanagement dieses eng mit der strategischen Planung der Organisation vernetzt sein muss. Zudem muss die Digitalisierung im Risikomanagement vorangetrieben sowie die allgemeine Datenqualität verbessert werden. (vgl. Braumann et al. 2020)

Eine der ersten gesetzlichen Reaktionen auf die Pandemie stellt das in Kapitel 3.2.2 beschriebene Stabilisierungs- und Restrukturierungsgesetz dar, welches es Unternehmen ermöglicht, beziehungsweise erleichtert Maßnahmen außerhalb der Insolvenz zu ergreifen.

Die genauen Auswirkungen der Covid-19 Krise auf das Risikomanagement und dessen Umsetzung in Organisationen kann zum Zeitpunkt der Verfassung dieser Arbeit noch nicht abgeschätzt werden.

3.4 Diskussion von Zusammenhängen zwischen Ereignissen und Gesetzen

Zunächst wird der zeitliche Zusammenhang der beschriebenen Ereignisse sowie Gesetze, beginnend mit dem KonTraG 1998 bis zum StaRuG 2021, verdeutlicht (Abbildung 10). Diese Abbildung stellt neben den betrachteten Ereignissen die beobachteten gesetzlich und quasi-gesetzlich bedingten Weiterentwicklungen des Risikomanagements und Risikomanagementsystemen in Unternehmen seit dem Jahr 2000 dar.

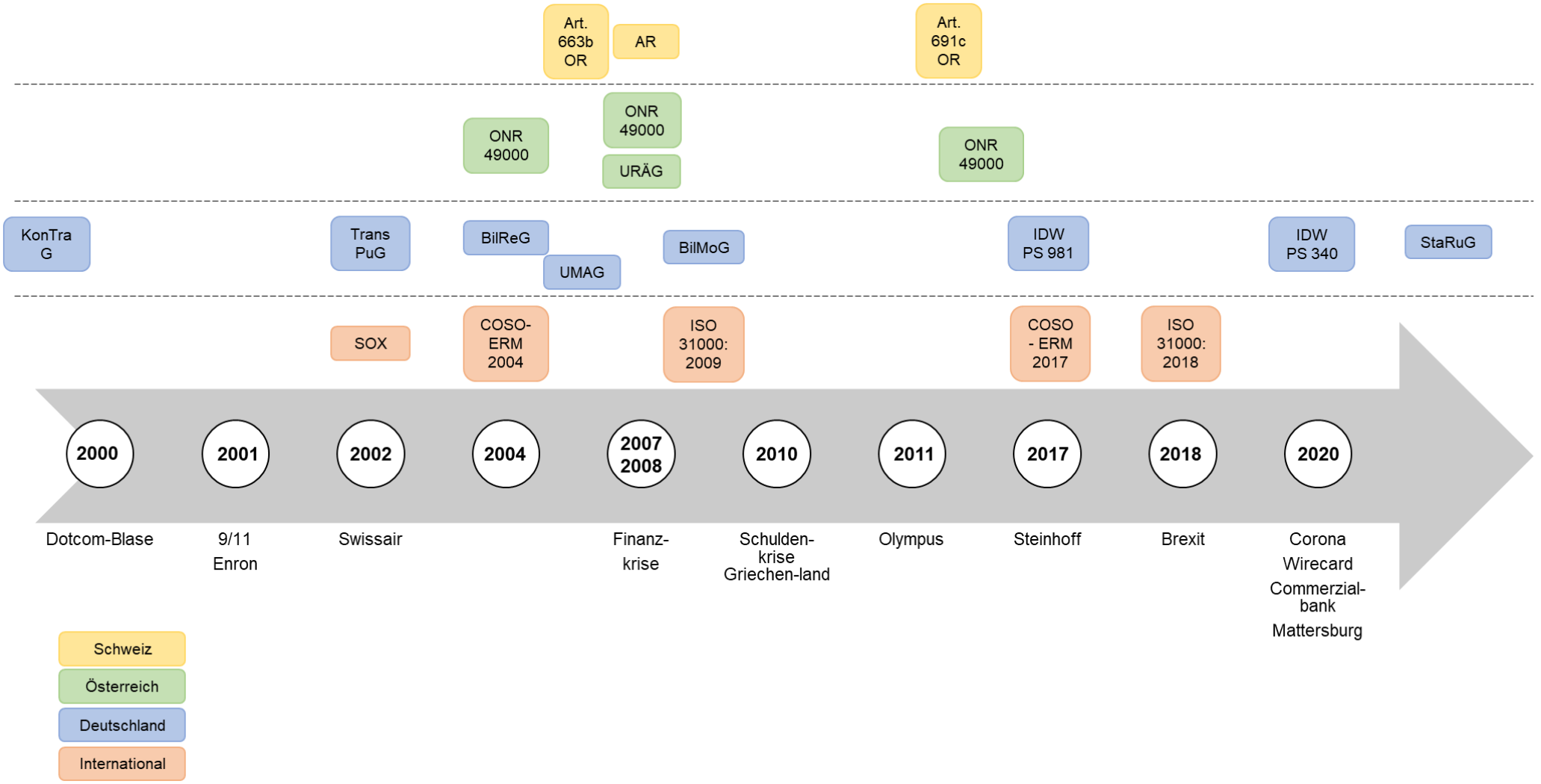

Abbildung 10: Zeitlicher Zusammenhang Ereignisse, Gesetze und Standards

Quelle: Eigene Darstellung

Die Analyse sowie die Darstellung zeigen, dass insbesondere zwischen den Jahren 2004 und 2009 zahlreiche Änderungen in Gesetzen sowie Standards erfolgt sind. Auch ab dem Jahr 2017 kam es zu bedeutenden Änderungen in den das Risikomanagement betreffenden Standards und Gesetzen. Auffällig ist, dass in den Jahren nach der Finanzkrise bis zur Neufassung der ONR 49000 im Jahr 2014 keine Änderungen erfolgt sind. Eine weitere Auffälligkeit bildet die Häufung von Ereignissen in der jüngeren Vergangenheit. So gab es neben der Corona-Pandemie und der Finalisierung des Brexit im Jahr 2020 mit Wirecard und der Commerzialbank Mattersburg zwei weitreichende Bilanzskandale in der DACH-Region.

Allgemein fanden in Deutschland die meisten Änderungen in den Gesetzestexten statt, wohingegen es in der Schweiz lediglich drei Änderungen im Betrachtungszeitraum gab. Auch in Österreich wurde mit dem URÄG 2008 lediglich eine Gesetzesänderung betreffend Risikomanagement verabschiedet. Die Änderungen durch das URÄG sind allerdings sehr weitreichend und können mit den Änderungen in Deutschland bis zum Bilanzmodernisierungsgesetz verglichen werden.

International ist der Sarbanes-Oxley Act, welcher eine Reaktion auf verschiedene Bilanzskandale, insbesondere dem Fall Enron, war, von größter Bedeutung. Der SOX bildet sowohl eine Basis für die anschließend in Deutschland, Österreich und der Schweiz verabschiedeten Gesetze, als auch gilt dieser für alle Gesellschaften aus diesen Ländern, welche entweder selbst oder ein Tochterunternehmen an der amerikanischen Börse gelistet haben. Entgegengesetzt gilt dies auch für europäische Töchter amerikanischer Unternehmen, wenn diese im Konzern konsolidiert werden.

Auch die Standards, welche Anhaltspunkte zur konkreten Umsetzung eines Risikomanagementsystems in der Organisation bieten, wurden stetig überarbeitet. So wurde 2004 der COSO Standard als Rahmenwerk veröffentlicht. Dieser beinhaltet bereits die Vorgaben des SOX und stellt somit ebenso eine Reaktion auf den Enron-Skandal dar. Während im SOX die Vorgaben geschaffen wurden, bietet der COSO Standard eine Möglichkeit zur effektiven Implementierung und Umsetzung zum Risikomanagement im Unternehmen. Nach der Finanzkrise, deren Auswirkung in Unternehmen weltweit spürbar waren, wurde mit der neu geschaffenen ISO 31000 ein einheitlicher internationaler Standard verabschiedet, welcher die Grundlagen des Risikomanagements abdeckt und ein international einheitliches Verständnis schaffen soll.

In 2017 folgte nach dem Abklingen der Auswirkungen der Finanzkrise sowie der damit einhergehenden Schuldenkrise in Europa und weiteren Bilanzskandalen wie der von Olympus und Steinhoff, die Veröffentlichung des überarbeiteten COSO Rahmenwerks. Ein Jahr da-

rauf wurde auch die Norm ISO 31000 überarbeitet. Laut beiden Standards ist das Risikomanagement ein kontinuierlicher Prozess, welcher sowohl auf externen als auch internen Input angewiesen ist. Auch wurde der Prozess rund um das Risikomanagementsystem mit der strategischen Ausrichtung sowie den Unternehmenszielen und Werten verknüpft. Zudem wurde die Verantwortlichkeit für das Risikomanagement innerhalb der Organisation im Top-Management verankert. Dies betont die Priorität des Risikomanagements in der Organisation. Andererseits kann diese eventuelle Doppelfunktion des Vorstandes oder ähnlichen Organen auch dazu führen, dass beispielsweise ein Bilanzbetrug erst spät bekannt wird. Im Fall von Enron als auch bei Wirecard und der Commerzialbank Mattersburg war maßgeblich das Top-Management für die Bilanzfälschungen verantwortlich. Da diese Personen auch für das Risikomanagement verantwortlich sind, besteht die Möglichkeit, hier vorsätzlich das Risikomanagement zu korrumpieren.

In Deutschland werden die internationalen Standards wiederum von den Prüfungsstandards des Instituts der Wirtschaftsprüfer ergänzt. Der initiale Prüfungsstandard aus 1999 wurde im Jahr 2020 nach Veröffentlichung des PS 981, welcher sich eigens der Prüfung im Rahmen des Risikomanagements widmet, erneuert. Im Jahr 2020 wurde der IDW PS 340 nach zahlreichen Ereignissen und Gesetzesänderungen auf den aktuellen Stand angepasst. Insbesondere wird hier auf die Risikofrüherkennung sowie Risikoaggregation hingewiesen. Dies kann darauf zurückgeführt werden, dass in der Vergangenheit Risiken und deren Auswirkungen nicht früh genug erkannt wurden, wie es unter anderem bei der Finanzkrise und der Schuldenkrise in Griechenland der Fall war.

Auch die Berichterstattung zum Risikomanagement ist in zahlreichen Standards und Änderungen enthalten. Die Änderungen zur Berichterstattung können besonders auf die verschiedenen Bilanzskandale zurückgeführt werden, allerdings konnte auch die weitreichende Transparenz keine neuen Bilanzfälschungen verhindern. Es ist aber davon auszugehen, dass die Berichterstattungspflicht zum Risikomanagement dazu beigetragen hat, die Zahl der Bilanzfälschungen zu senken.

Allgemein kann ein Zusammenhang zwischen den beschriebenen Ereignissen und den gesetzlichen Anforderungen bestätigt werden. Oft führen mehrere Ereignisse aggregiert zu einer notwendigen Anpassung der Standards und Gesetze sowohl auf internationaler als auch nationaler Ebene. Standards, welche Anhaltspunkte zur Umsetzung des Risikomanagements bilden, werden nach gesetzlichen Änderungen angepasst, sowie nach einiger Zeit aufgrund der gesammelten Erfahrungswerte sowie zwischenzeitlich neu eingetretenen Ereignissen und neuen gesetzlichen Entwicklungen überarbeitet. Durchaus tragen hier neben Ereignissen und Gesetzen noch andere Umwelteinflüsse zu Überarbeitungen bei. Unter

anderem wird das Risikomanagement auch von voranschreitender Digitalisierung sowie der steigenden Menge und verschiedener Qualität der zur Verfügung stehenden Daten beeinflusst.

So können gewisse gesetzliche Änderungen, wie der Sarbanes-Oxley Act, direkt auf ein externes Ereignis (hier: Enron Bilanzskandal) zurückgeführt werden. Auch die Änderung im Schweizer Obligationenrecht kann direkt auf den Konkurs der Swissair zurückgeführt werden. Andere Änderungen resultieren aus einem Zusammenspiel der vorhergehenden Ereignisse und anderen Gesetzen. Somit besteht zwar ein Unterschied zwischen direkten und indirekten Verbindungen zwischen externen Ereignissen und (quasi-) gesetzlichen Änderungen, allerdings ist ein Zusammenhang klar erkennbar und gegeben.

4. Metastudie zum Umsetzungsstand des Risikomanagements in Unternehmen

Nach Beantwortung der ersten Forschungsfrage zu Zusammenhängen zwischen eingetretenen, relevanten Ereignissen und den das Risikomanagement betreffenden gesetzlichen und sonstigen Änderungen, soll im folgenden Kapitel der Umsetzungsstand in Unternehmen der DACH-Region analysiert werden. Insbesondere dient die Analyse der Überprüfung, ob die Umsetzung in Organisationen in Einklang mit den Änderungen und Vorgaben steht. Hierzu werden zunächst Studien aus verschiedenen Jahren und Kriterien zur Auswertung des Umsetzungsstandes definiert. Anschließend werden jene Studien anhand der Kriterien analysiert und somit Rückschlüsse auf Änderungen gezogen. Ziel dieser Auswertung ist insbesondere festzustellen, ob seitens der Unternehmen lediglich gesetzliche Vorgaben umgesetzt werden (compliance), oder ob das Risikomanagement aktiv zur Unternehmenssteuerung genutzt wird (performance).

4.1 Auswahl der Studien

Die Studien zur Analyse des Umsetzungsstandes wurden anhand der in der jeweiligen Studie betrachteten Branche, der lokalen Einordnung der betrachteten Unternehmen sowie des Jahres der Durchführung ausgewählt. Um einen breitgefächerten Überblick zu erhalten, wurden vorrangig Studien gewählt, in welchen Unternehmen aus verschiedenen Branchen befragt wurden.

Studien, welche rein den Finanz- bzw. Bankensektor betreffen wurden aufgrund des Ausschlusses dieser Branchen in der vorliegenden Arbeit nicht berücksichtigt.

Die herangezogenen Studien lassen sich in die folgenden beiden Kategorien unterteilen:

- Benchmark- & Best-Practice-Studien von Wirtschaftsprüfungs- & Consultingunternehmen
- Lokale Enterprise-Risk-Managementstudien aus der DACH-Region

Anhand der Benchmark-Studien wird eine allgemeine Ableitung zum Umsetzungsstand getroffen, welche anschließend mit den lokalen Enterprise Risk Managementstudien verglichen wird. Die folgende Tabelle zeigt eine Übersicht über die herangezogenen Studien unter Angabe von Herausgeber, Titel, Erscheinungsjahr sowie einer zugewiesenen Kurzbezeichnung.[4]

[4] Vollständige Bibliographieangaben sind im Literaturverzeichnis angegeben

Nr.	Jahr	Herausgeber	Titel	Kurzbez.
1	2005	Ernst & Young AG	Ernst & Young Best Practice Survey "Risikomanagement 2005"	EY 2005 DE
2	2007	The Economist	Best practice in Risk Management	Eco 2007
3	2010	PricewaterhouseCoopers AG (PwC); Martin-Luther-Universität Halle-Wittenberg	Compliance und Unternehmenskultur	PwC/MLU 2010 DE
4	2010	PricewaterhouseCoopers AG (PwC)	Risk-Management-Benchmarking 2010	PwC 2010 DE
5	2011	Bundesverband der Deutschen Industrie e.V (BDI); PricewaterhouseCoopers AG (PwC)	Risikomanagement 2.0	MS 2011a DE
6	2011	PricewaterhouseCoopers AG (PwC)	Von der Krise zu einer neuen Risikokultur?	PwC 2011 DE
7	2011	Funk RMCE GmbH; Rödl & Partner GmbH; Weissman & Cie. GmbH & Co. KG	Risikomanagement im Mittelstand	MS 2011b DE
8	2012	PricewaterhouseCoopers AG (PwC)	Risk-Management Benchmarking 2011/12	PwC 2012 DE
9	2013	i-Risk GmbH; ETH Zürich	Risikomanagement in Schweizer Organisationen	Risk 2013 CH
10	2014	GrECo International AG; Handelsverband	Der Handel - Risikomanagement und Versicherungen für operationelle Risiken	GrEco 2014 AT
11	2014	Theuermann, Christian; Meiregger, Peter	Risikomanagement im österreichischen Mittelstand	MS 2014 AT
12	2015	Allianz SE and Allianz Global Corporate & Specialty SE	Allianz Risk Barometer	Allianz 2015
13	2015	PricewaterhouseCoopers AG (PWC)	Risk-Management Benchmarking 2015	PwC 2015 DE
14	2015	Ernst & Young AG	There´s no reward without risk	EY 2015
15	2017	Deloitte	Risikomanagement Benchmarkstudie 2017	Deloitte 2017 DE
16	2018	Hunziker, Stefan; Balmer, Patrick	Enterprise Risk Management in Schweizer Unternehmen	ERM 2018 CH
17	2019	AON	Global Risk Management Survey 2019	AON 2019
18	2020	Deloitte	Risikomanagement Benchmarkstudie 2020	Deloitte 2020 DE
19	2020	Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern	ERM Report 2020	ERM 2020 DE CH

Tabelle 1: Übersicht analysierte Studien

4.2 Kriterien zur Auswertung des Umsetzungsstands

Abgeleitet sowohl aus den Ergebnissen aus Kapitel 3 sowie der Literatur ergeben sich Kriterien, welche zur Auswertung der gewählten Studien verwendet werden. Hierbei lassen sich die gewählten Kriterien in drei übergeordnete Kategorien einteilen:

- Organisation des Risikomanagements
- Strategisches Risikomanagement und Risikomanagementprozess
- Operatives Risikomanagement und Risikomanagementprozess

Im Rahmen der Organisation werden die Verantwortlichkeiten sowie die Aufbauorganisation des Risikomanagements in den betrachteten Unternehmen analysiert.

Die Verantwortlichkeit für das Risikomanagement innerhalb einer Organisation hat sich in den vergangenen Jahren verändert. Je mehr das Risikomanagement an Bedeutung gewann, desto höher in der Organisationshierarchie sollte sich die Verantwortlichkeit für das Risikomanagement befinden. Gegenwärtig wird die Rolle des/der RisikomanagerIn[5] und den damit einhergehenden Aufgaben im Top-Management einer Organisation angesehen, ungeachtet dessen, ob dies eine eigene Rolle darstellt oder in beispielsweise Vorstandsaufgaben integriert ist. Hieraus resultiert das erste Kriterium:

Kriterium 1: Verantwortlichkeit Risikomanagement innerhalb der Organisation

- Wo ist die Verantwortlichkeit in Unternehmen verankert?
- Existiert eine eigene Rolle, welche das Risikomanagement betreut?

In die Kategorie des strategischen Risikomanagements fallen Risikokultur sowie -strategie, Chancen als Bestandteil des RMS sowie dessen Ausrichtung.

Der in Kapitel 2.3 beschriebene Unterschied zwischen compliance-orientierten und performance-orientierten Risikomanagement bildet die Basis für das nächste Auswertungskriterium. Hierbei wird geprüft, ob Unternehmen lediglich die gesetzlichen Mindestanforderungen bezüglich Risikomanagement umsetzen oder ob Risikomanagement auch zur aktiven Risikosteuerung eingesetzt wird. Es soll analysiert werden, ob das Risikomanagement über die gesetzlichen Anforderungen hinausgeht. Hieraus ergeben sich die folgenden Kriterien:

Kriterium 2: Kultur & Strategie

- Existiert in den betrachteten Unternehmen eine Risikokultur?

[5] Die Verfasserin der vorliegenden Masterarbeit bekennt sich zu einer geschlechtergerechten Sprachverwendung. Um die Lesbarkeit zu gewährleisten und zugunsten der Textökonomie wird in Einzelfällen die Kürzung ohne männliche Endung notwendig (zB der/die ManagerIn). Diese – grammatisch nicht ganz korrekte – Kurzform findet im Sinne einer „positiven Diskriminierung“ als kompensatorische Maßnahme Anwendung.

Kriterium 3: Chancen

- Werden auch Chancen im Rahmen des Risikomanagements behandelt?

Kriterium 4: Ausrichtung des RM

- Werden lediglich gesetzliche Anforderungen erfüllt und werden diese explizit genannt?
- Wird Risikomanagement aktiv genutzt und in welcher Art?

Zuletzt werden Bestandteile des operativen Risikomanagementprozesses betrachtet.

In der Vergangenheit wurden Risiken durch bestimmte Ereignisse wie den Terroranschlag auf das World Trade Center schlagartig nach oben priorisiert, wohingegen diesen Risiken in den Vorjahren nur ein niedriger Stellenwert eingeräumt wurde. Auch in jüngster Vergangenheit wurde durch den Ausbruch des Covid-19 Virus das zuvor eher vernachlässigte Risiko einer Pandemie/Epidemie innerhalb weniger Wochen zu einem hochpriorisierten Risiko. Daraus ergibt sich folgendes Kriterium für die Auswertung der Studien:

Kriterium 5: Risikopriorisierung

- Sind Terrorismus und Pandemie (o.Ä.) als Risiko berücksichtigt?

Neben der Priorisierung von einzelnen Risiken ist auch die Risikoaggregation von hoher Bedeutung. Das Gesamtrisiko einer Organisation, welches sich aus den Einzelrisiken und deren Bewertungen und Eintrittswahrscheinlichkeiten ergibt, spiegelt die gesamte Exposition des Unternehmens gegenüber Risiken wider. Dies kann am Beispiel der Finanzkrise und der darauffolgenden Bankenkrise in Europa und insbesondere der Schuldenkrise in Griechenland aufgezeigt werden. Hierbei führte nicht ein Einzelrisiko zum Zusammenbruch verschiedener Organisationen, sondern die Wechselwirkung verschiedener Ereignisse und deren Gesamtausmaß führte schlussendlich zum Konkurs von Lehman-Brothers. Auch die darauffolgende Schuldenkrise in Griechenland resultierte aus einer Vielzahl an eingetretenen Risiken. Daraus resultiert Kriterium 6:

Kriterium 6: Risikoaggregation und Risikokorrelation

- Wird eine Wechselwirkung der Risiken berücksichtigt?
- Findet eine Aggregation der identifizierten Risiken statt und in welchem Umfang?

In diversen Gesetzesänderungen fand unter anderem eine Änderung der geforderten Berichterstattung zum Risikomanagement statt. Diese wurde durch Erweiterungen tiefgreifender und umfangreicher. Von einer einfachen Aufzählung oder Beschreibung der Risiken und Chancen wurde zu einer detaillierten Beschreibung zum Umgang mit ebendiesen über-

gegangen, sodass sich Organisationen intensiv mit identifizierten Risiken und deren möglichen Auswirkungen, Vermeidung, Abmilderung, Eintrittswahrscheinlichkeiten und Gegenmaßnahmen auseinandersetzen müssen. Die Berichterstattung bildet das nächste Kriterium:

Kriterium 7: Berichterstattung zum Risikomanagement

- Umfang und Inhalt der Berichterstattung

Neben der Berichterstattung bildet auch die interne und externe Prüfung des RMS einen wichtigen Bestandteil des operativen Risikomanagementprozesses. Für die Prüfung und Überwachung muss eine Prüfbarkeit des RMS gegeben sein. Dies wird in folgendem Kriterium analysiert:

Kriterium 8: Prüfung Überwachung und Prüfbarkeit von RMS

- Findet eine Prüfung (extern oder intern) des RMS statt?
- Ist eine Prüfbarkeit des eingeführten RM gegeben?

Ebenso ergeben sich aus gesetzlichen Änderungen notwendige Anpassungen in Risikomanagementsystemen. Diese können verschiedene Bereiche innerhalb des organisationsweiten Risikomanagements betreffen. Im finalen Auswertungskriterium wird daher untersucht, in welchen Bereichen die Teilnehmer der Studien Optimierungspotential sehen und wie oft bzw. regelmäßig eine Anpassung des RMS oder dessen Bestandteile (bspw. Risikoidentifikation, Risikorichtlinie) stattfindet.

Kriterium 9: Optimierungspotential von RMS und deren Bestanteilen sowie Frequenz der Anpassungen

- In welchen Bereichen des RM besteht insbesondere Optimierungspotential?
- Wie oft werden RMS bzw. deren Bestandteile angepasst oder überarbeitet?

Für sämtliche Kriterien wird der Verlauf im betrachteten Zeitraum dargestellt, bevor in Kapitel 5 ein Gesamtzusammenhang zwischen Änderungen, Ereignissen und dem Umsetzungsstand im Unternehmen dargestellt wird.

4.3 Entwicklung des Risikomanagements der Unternehmen

In den folgenden Unterkapiteln wird systematisch, anhand der Kriterien aus Kapitel 4.2, die Entwicklung der Organisation des Risikomanagements sowie des strategischen und operativen Risikomanagementprozesses beschrieben. Einige Daten wurden anhand von Diagrammen visualisiert. Die Farbgebung orientiert sich an Abbildung 10, entsprechend dem folgenden Schema. Die vollständige Auswertung befindet sich im Anhang (A3-digital).

Abbildung 11: Farblegende Diagramme

4.3.1 Aufbauorganisation des Risikomanagements

Die Aufbau- und Ablauforganisation des Risikomanagements im Unternehmen stellt insbesondere die Verankerung der Verantwortlichkeiten dar. Die betrachteten Studien stimmen überein, dass die (übergeordnete) Verantwortung für das Risikomanagement in der oberen Führungsetage der Organisation angesiedelt ist. Entsprechend der jeweiligen Gesellschaftsform betrifft dies beispielsweise den Vorstand oder die Geschäftsführung. Oft wird dies mit dem Satz „*Risikomanagement ist Chefsache*“ (Theuermann und Ebner 2014, S. 19) beschrieben.

Dieses Ergebnis gilt sowohl über die gesamte Zeitspanne der Studien als auch in den verschiedenen betrachteten Ländern.

> *„Während die Unternehmensleitung zumeist die übergeordnete Verantwortung für das RMS trägt, haben die Risikoverantwortlichen das effiziente Einleiten und Umsetzen der für die Risikosteuerung erforderlichen Gegenmaßnahmen und die regelmäßige und zeitnahe Risikoberichterstattung innerhalb ihres Verantwortungsbereichs sicherzustellen.“ (Klenk und Reetz 2010, S. 18)*

> *„Die Verantwortung für das Risikomanagement ist bei neun von zehn Unternehmen gebündelt und in der Regel auf Ebene des Vorstands bzw. der Geschäftsführung verankert.“ (Herre und Tüllner 2011, S. 7)*

> *„97 Prozent der Studienteilnehmer geben an, dass sich die Unternehmensleitung regelmäßig mit dem RMS und der sich auf dessen Basis eingeschätzten Risikosituation beschäftigt.“ (Deloitte 2020, S. 15)*

Ein weiteres Ergebnis ist, dass häufig eine eigene Rolle oder Abteilung für das Risikomanagement in einer Organisation eingerichtet wurde. Der Anteil der Unternehmen mit einem/einer eigenen RisikomanagerIn beziehungsweise einer eigenen Risikoabteilung hat sich im betrachteten Zeitraum überwiegend vergrößert (vgl. Abbildung 12 und Abbildung 13). Die Bezeichnung der für das Risikomanagement geschaffenen Rolle unterscheidet sich in einigen Organisationen. Diese reicht von „Risikomanager“ über „Chief Risk Officer (CRO)“ bis „Risikokoordinator“ oder „Corporate Risk Manager“.

> *“CROs are already in place at 38% of those organisations represented in this survey, and a further 21% have plans to appoint an individual to this role over the next three years.” (Economist Intelligence Unit 2007, S. 9)*

Abbildung 12 zeigt die Entwicklung des Anteils an Unternehmen mit einer eigenen Risikomanagement-Abteilung. Im deutschen Mittelstand haben 2011 deutlich weniger Organisationen eine eigens für das Risikomanagement zuständige Abteilung als 2012 in deutschen Großunternehmen. Im österreichischen Mittelstand waren dies in 2014 13 Prozent. Ein deutlicher Anstieg lässt sich beim Vergleich der Jahre 2012 und 2015 erkennen. Hier stieg der Anteil um 22 Prozentpunkte. Auch die Schweiz weist mit 46% im Jahr 2017 einen hohen Anteil an Organisationen mit eigener Risikoabteilung auf.

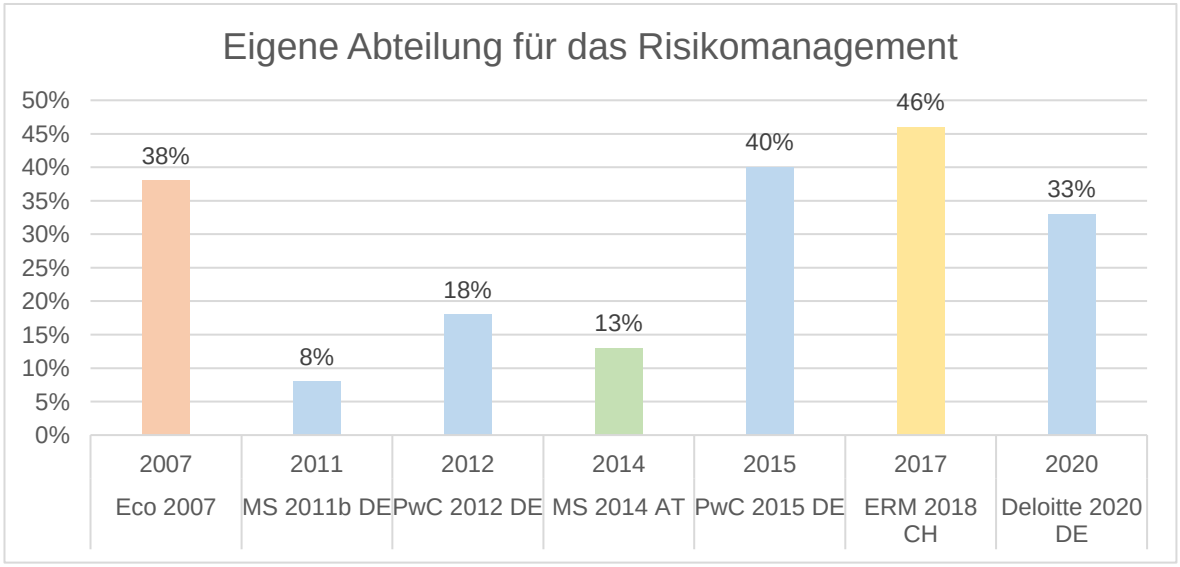

Abbildung 12: Anteil Organisationen mit eigener Risikoabteilung
Quelle: Eigene Darstellung. Datenquellen in Diagramm ersichtlich.

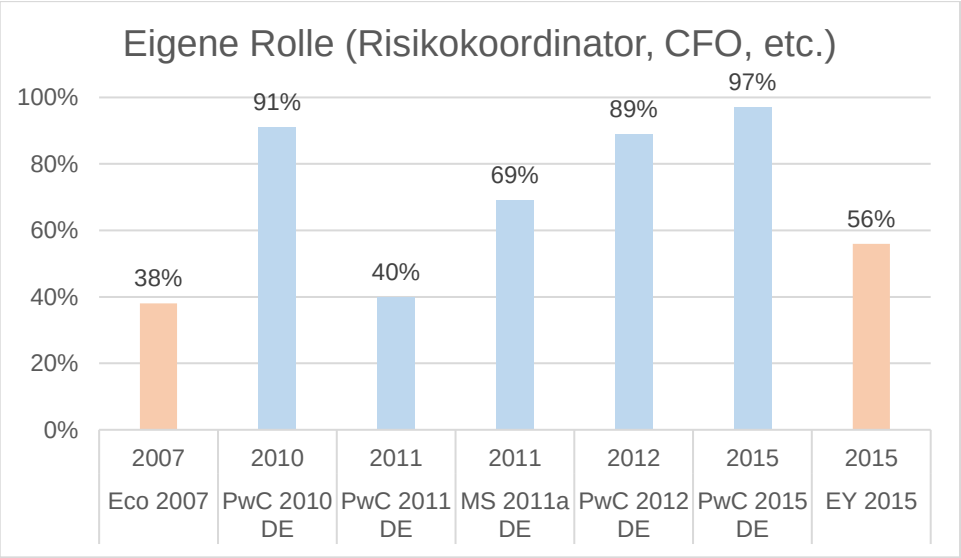

Abbildung 13: Anteil Organisationen mit eigener Rolle für das Risikomanagement
Quelle: Eigene Darstellung. Datenquellen in Diagramm ersichtlich.

In Organisationen ohne eigene Risikomanagementabteilung wird die Verantwortlichkeit oft in der Controlling-Abteilung beziehungsweise im übergeordneten Finanzbereich verankert.

> *"Overall, the finance department continues to be responsible for risk management." (AON 2019, S. 62)*

4.3.2 Strategisches Risikomanagement und Risikomanagementprozess

In der Kategorie des strategischen Risikomanagements und dessen Prozess werden das Vorhandensein einer Risikokultur sowie einer Risikostrategie, die Integration von Chancen in das Risikomanagementsystem sowie die Ausrichtung des Risikomanagements analysiert.

Risikokultur und Risikostrategie

Bereits zu Beginn des Betrachtungszeitraums wird der Stellenwert eines einheitlichen Risikoverständnisses in einer Organisation verdeutlicht. Ein einheitliches Verständnis kann durch verschiedene Maßnahmen erreicht werden, unter anderem durch unternehmensweite Richtlinien und Handbücher.

> *„Bei den Maßnahmen zur Schaffung eines einheitlichen Risikoverständnisses im Unternehmen stehen Richtlinien und Handbücher zum Risikomanagement sowie die Vorgabe einer Risikotoleranz an erster Stelle." (Ernst & Young AG 2005, S. 10)*

Handbücher und Richtlinien stellen über den Betrachtungszeitraum das meist verwendete Instrument zur Vermittlung des Verständnisses und einer Risikostrategie dar. Hierbei sind keine Abweichungen bei länderspezifischer Betrachtung festzustellen.

> *„Nahezu alle von uns betrachteten Unternehmen (94 %) haben ihre Vorgaben zum RMS in Form einer Risikorichtlinie dokumentiert." (Herre et al. 2012, S. 17)*

> *„Generell besteht bei ca. 20% der befragten Unternehmen bereits ein eigenes Risikomanagementhandbuch, in welchem diesem Thema die volle Aufmerksamkeit gewidmet wird." (Theuermann und Ebner 2014, S. 24)*

Eine anwendbare Risikostrategie als Weiterentwicklung ist in deutlich weniger Organisationen etabliert. Zudem sind hier lokale beziehungsweise Branchenunterschiede zu erkennen.

2010 gaben 12% der befragten Unternehmen an, eine nachvollziehbare beziehungsweise anwendbare Risikostrategie zu haben. (Klenk und Reetz 2010, S. 7) In 2012 traf dies hingegen bereits auf 29% der Organisationen zu. (Herre et al. 2012, S. 18)

Im österreichischen Handel gaben 2014 bereits 65% der befragten Unternehmen an, eine verbindliche und definierte Risikostrategie in ihrer Organisation etabliert zu haben. (Koller und Vogl 2014, 9;16)

Eine Risikokultur ist gemäß der Deloitte Benchmarkstudie aus 2020 essentiell, um die Verbindung zwischen Risikoerkennung und Risikosteuerung herzustellen.

> *„Positiv ist zu deuten, dass laut 81% der befragten Unternehmen die Risikokultur das Verständnis fördert, dass das Erkennen von Risiken der erste Schritt zur adäquaten Risikosteuerung ist." (Deloitte 2020, S. 19)*

2011 gaben 30% der befragten Unternehmen an, dass *„die Etablierung einer umfassenden Risikokultur ein wichtiges Langfristziel"* darstellt. (Herre und Tüllner 2011, S. 7)

2017 galt die „Risikokultur" immer noch bei 66% der Organisationen als ein besonders ausbaufähiges Element des eigenen Risikomanagements. (Deloitte 2017, S. 13)

Erwähnenswert ist hierbei auch, dass 2017 bereits 90% der Schweizer Unternehmen bestätigten, dass in ihrer Organisation eine positive Risikomanagementkultur zumindest teilweise verankert ist. (Bitterli und Fallegger 2018, S. 92)

Integration von Chancen in Risikomanagement

Ein weiterer wichtiger Bestandteil des strategischen Risikomanagementprozesses ist, ob neben Risiken auch Chancen in die jeweiligen Betrachtungen einbezogen werden. Hierbei

ist ein eindeutiger Trend nach oben erkennbar. Während in 2005 lediglich bei 25% der Organisationen auch Chancen berücksichtigt und berichtet wurden, sind es im Jahr 2020 bereits zwei Drittel der Unternehmen, welche zumindest unregelmäßig auch über Chancen berichten. Dies wird durch Abbildung 14 verdeutlicht.

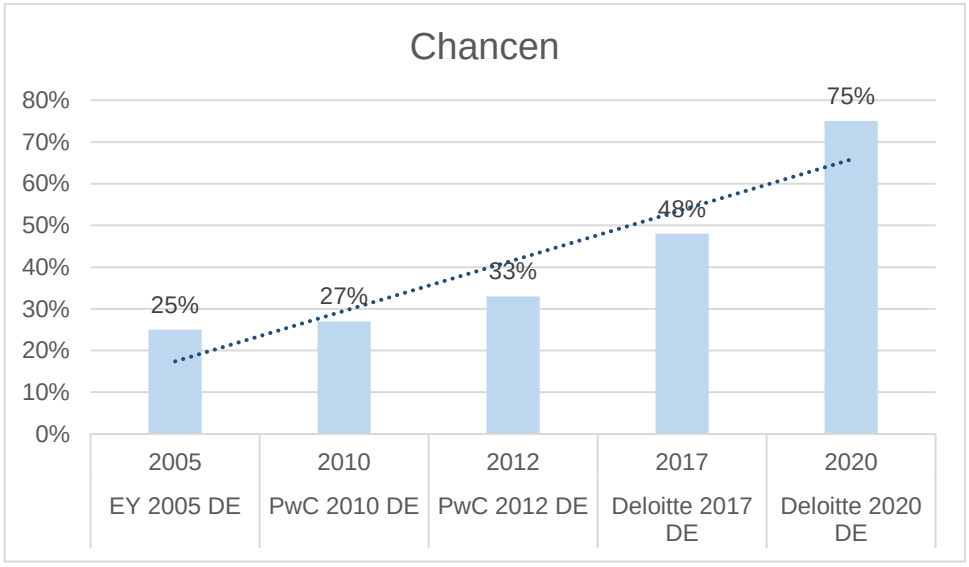

Abbildung 14: Berücksichtigung von Chancen im Risikomanagement
Quelle: Eigene Darstellung. Datenquellen in Diagramm ersichtlich.

Ausrichtung und Ziele des Risikomanagements

Eine der wichtigsten strategischen Entscheidungen im Rahmen des Risikomanagements stellt die Ausrichtung dar. Hierbei wird insbesondere zwischen dem compliance- und performance-orientiertem Risikomanagement (vgl. Kapitel 2.3) unterschieden.

Auch hier können beim Umsetzungsstand in den Organisationen Unterschiede im Verlauf der Zeit festgestellt werden. Im gesamten Betrachtungszeitraum bestätigt ein Großteil der Organisationen, ein Risikomanagement zur Erfüllung der gesetzlichen und compliance-Anforderungen etabliert zu haben. Allerdings geht die Begründung für ein Risikomanagementsystem auch darüber hinaus. So wird das Risikomanagement beispielsweise auch als Instrument zur werteorientierten Unternehmenssteuerung, als Wettbewerbsvorteil gegenüber der Konkurrenz oder auch als Mittel zur Unternehmenszielerreichung sehen.

So gaben in der Ernst & Young Best Practice Studie 2005 bereits 49% der befragten Unternehmen an, das Risikomanagement als Unterstützung wertorientierte Unternehmensführung anzusehen (S. 7). In der gleichen Studie gaben alle Teilnehmer an, das Risikoma-

nagement zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen zu verwenden. (S. 7) 92% gaben außerdem die Konformität gesetzlicher Anforderungen als Grund für die Implementierung eines Risikomanagementsystems an. (S.7)

In der PWC-Risk Management Benchmarkstudie aus dem Jahr 2010 wurde die Erfüllung der gesetzlichen Anforderungen untersucht. Hierbei ließ sich feststellen, dass die Risikobewertung bei den befragten Unternehmen die gesetzlichen Anforderungen erfüllt, jedoch zum einen die Systematik hinter der Risikobewertung zwischen den Unternehmen abweicht und zum anderen noch ungenutztes Potential insbesondere bei der Früherkennung besteht. (Klenk und Reetz 2010)

> *„Die Ergebnisse unserer Studie zeigen, dass die große Mehrheit der untersuchten Großunternehmen die gesetzlichen Anforderungen erfüllt. In Bezug auf ein umfassendes RMS besteht jedoch noch viel ungenutztes Potenzial." (Klenk und Reetz 2010, S. 7)*

> *„Nur 15 % der Unternehmen haben für alle wesentlichen Risiken Frühwarnindikatoren definiert." (Klenk und Reetz 2010, S. 22)*

Auch in der Neuauflage der Benchmarkstudie 2012 wurde ein ähnliches Ergebnis wiedergegeben. Auch zwei Jahre später wurde angegeben, dass weiterhin ungenutztes Potential in Sachen Risikomanagement besteht. (Herre et al. 2012)

Das Ziel, mit dem implementierten Risikomanagementsystem gesetzliche Anforderungen zu erfüllen, hat sich über die Jahre nicht verändert, denn auch 2020 gaben 98% der im Rahmen der Deloitte-Benchmarkstudie befragten Unternehmen die *„Erfüllung verpflichtender Anforderungen"* an. (Deloitte 2020, S. 14) Dies wird auch von einer anderen Studie bestätigt:

> *„Erfreulicherweise berichteten alle Schweizer und 99 % der deutschen Unternehmen über ihr Risk Management und kamen damit ihrer Verpflichtung zur Risikoberichterstattung nach. Das fehlende 1 % bei den deutschen Unternehmen kommt zustande, da der Geschäftsbericht der Wirecard AG nach wie vor nicht veröffentlicht wurde." (Hunziker et al. 2020, S. 28)*

Neben der Erfüllung der gesetzlichen und regulatorischen Anforderungen, welche hier auf Platz drei liegt, existieren auch in Schweizer Unternehmen noch zahlreiche weitere Ziele des Risikomanagementsystems. (Boutellier et al. 2013, S. 6)

Die Ergebnisse der Deloitte Studie aus dem Jahr 2020 zeigen, dass neben den Hauptgründen der gesetzlichen Anforderungen und der damit einhergehenden Berichterstattung, die Mehrheit der befragten Unternehmen das Risikomanagementsystem auch zur Unternehmenssteuerung nutzt. Ein kleinerer Anteil gab an, das System für eine verbesserte Risikosteuerung zu verwenden. (Deloitte 2020, S. 14)

Tabelle 2 stellt einen Überblick über die beschriebenen Ziele und Hintergründe des Risikomanagementsystems dar. In Klammern ist jeweils der Anteil der Unternehmen (EY 2005 DE; Deloitte 2020 DE) beziehungsweise die Priorisierung (Risk 2013 CH) angegeben.

2005	**2013**	**2020**
EY 2005 DE	**Risk 2013 CH**	**Deloitte 2020 DE**
Frühzeitige Entwicklung bestandsgefährdender Entwicklungen *(100%)*	Früherkennung und verbesserte Kontrolle von Risiken *(1.)*	Erfüllung verpflichtender Anforderungen *(98%)*
Konformität mit den gesetzlichen Anforderungen *(92%)*	Förderung einer internen Risikokultur *(2.)*	Nutzung des RMS für die interne und externe Berichterstattung *(98%)*
Prüfbarkeit des Systems durch die Revision/den Wirtschaftsprüfer *(65%)*	Erfüllung regulatorischer oder gesetzlicher Anforderungen *(3.)*	Nutzung des RMS als Instrument für die Unternehmenssteuerung *(67%)*
Unterstützung einer werteorientierten Unternehmensführung *(49%)*	Schutz der Reputation der Organisation *(4.)*	Nutzung des RMS zur verbesserten Steuerung wesentlicher Risiken *(39%)*
Transparenz über wesentliche Unternehmenschancen *(36%)*	Erkennung und Abwägung von Chance-Risiko-Verhältnissen *(5.)*	
Senkung der Risikokosten *(32%)*	Input für die Strategie *(6.)*	
	Steuerung und Controlling von Projekten *(7.)*	
	Sicherung der Liquidität und des Cash Flows *(8.)*	

Tabelle 2: Ziele und Hintergründe des Risikomanagementsystems
Datenquelle in Tabelle ersichtlich.

Zusammenfassend stellt die Erfüllung der gesetzlichen Anforderungen im gesamten Betrachtungszeitraum ein Ziel des Risikomanagements für die Mehrheit der Unternehmen dar. Eine Nutzung des Risikomanagementsystems darüber hinaus erfolgt ebenfalls in einer Vielzahl der betrachteten Unternehmen, wobei das Ausmaß der Nutzung divergiert.

Der Trend entwickelt sich positiv in Richtung eines performance-orientierten Risikomanagements. Dies ist zum einen daran zu erkennen, dass in jüngerer Vergangenheit die Erfüllung gesetzlicher Anforderungen nicht mehr auf Platz eins der Hintergründe angegeben wird. Zum anderen wird dies anhand Tabelle 2 deutlich, welche zeigt, dass zwei Drittel der Unternehmen aktuell das RMS bereits zur Unternehmenssteuerung nutzen.

4.3.3 Operatives Risikomanagement und Risikomanagementprozess

Nach den organisatorischen und strategischen Aspekten der Umsetzung des Risikomanagements in Unternehmen erfolgt die Analyse der operativen Umsetzung. Hierbei wird zunächst auf die Aggregation und Korrelation der identifizierten Risiken eingegangen. Darauf folgend werden Aspekte der Berichterstattung und Prüfung sowie der Prozess der Überarbeitung des Risikomanagementsystems anhand der Studien erarbeitet.

Risikopriorisierung

Eine detaillierte Auflistung und Reihung der Risiken finden sich nur in wenigen Studien. Auch in diesen sind beide betrachteten Risiken nicht in den hoch priorisierten Risiken enthalten.

2007 wurde Terrorismus als Risiko angegeben, allerdings besaß dies gemäß der Studie von „The Economist" keine Priorität. Eine Pandemie oder Ähnliches wurde hier nicht genannt. (Economist Intelligence Unit 2007, S. 6)

Im „Risk Barometer" der Allianz aus 2015 wird Terrorismus unter den Top fünf Risiken der Kategorie *„Top 5 risk for which businesses are least prepared"* gelistet. Das Risiko einer Pandemie oder Ähnlichem ist in diesem Report nicht erwähnt. (Allianz SE and Allianz Global Corporate & Specialty SE 2015, S. 7)

Im AON Global Risk Management Survey aus 2019 finden sich die beiden Risiken auf Platz 55 („*Terrorism/Sabotage*") und auf Platz 60 („Pandemic risk/health crisis") wieder. (AON 2019, S. 15)

2020 nach Ausbruch der Corona-Pandemie gaben weniger als die Hälfte der befragten Führungskräfte an, das Risiko einer Pandemie bereits zuvor im Risikomanagement integriert zu haben.

> *„Erstaunlicherweise haben lediglich 46 % (13) der befragten Risk Manager angegeben, dass sie das Pandemierisiko bereits vor der Corona-Krise im Risikoinventar aufgeführt hatten." (Hunziker et al. 2020, S. 34)*

Nach Beginn der Pandemie im Jahr 2019 zeigte sich in Deutschland und in der Schweiz ein unterschiedliches Bild.

> *„Von den 198 untersuchten Schweizer Unternehmen haben 2019 52 das Risiko Pandemie in ihrem Lagebericht aufgeführt. COVID-19 wurde von 92 erfasst. In Deutschland berichteten 101 Unternehmen über das Pandemierisiko und 149 über COVID-19.Das bedeutet, dass die Hälfte der deutschen Unternehmen über die Pandemie berichtete, wohingegen es in der*

Schweiz nur 1/4 der Unternehmen taten. In Deutschland erfassten 3/4 der Unternehmen CO-VID-19 als Risiko. In der Schweiz waren es nur 1/2 der Unternehmen." (Hunziker et al. 2020, S. 26)

Risikoaggregation und Korrelation

Zu Beginn des Betrachtungszeitraums wurden lediglich von einem Drittel der nicht börsennotierten und der Hälfte der börsennotierten Unternehmen jeweils Korrelationen zwischen den einzelnen identifizierten Risiken erfasst. (Ernst & Young AG 2005, S. 8)

Der zeitliche Verlauf des Anteils an Unternehmen, welche Korrelationen zwischen Risiken berücksichtigen, ist in folgender Abbildung dargestellt.

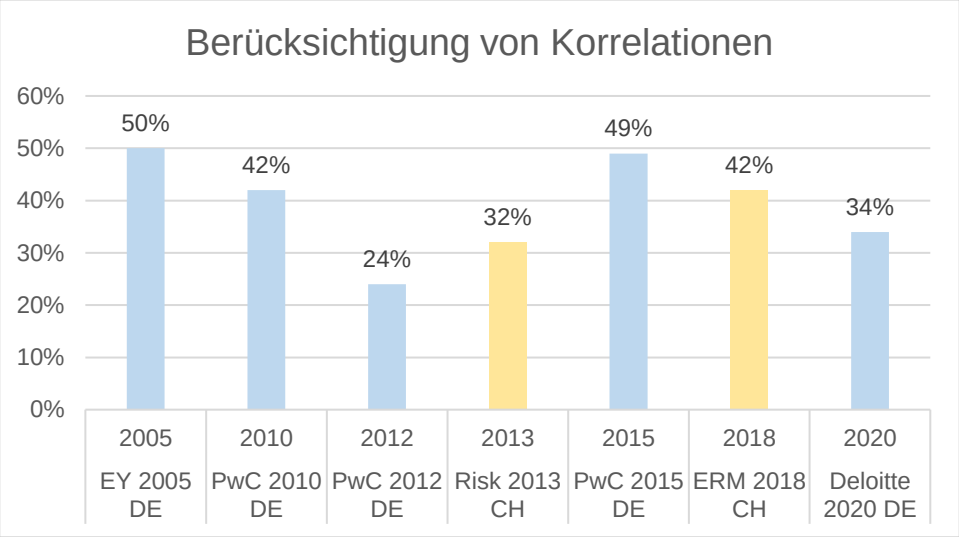

Abbildung 15: Anteil der Unternehmen mit Berücksichtigung von Risikokorrelationen
Quelle: Eigene Darstellung. Datenquellen in Diagramm ersichtlich.

In der Schweiz wurden Wechselwirkungen zwischen Einzelrisiken im Jahr 2013 von 32% der Unternehmen berücksichtigt. (Boutellier et al. 2013, S. 12)

Neben den Wechselwirkungen wurde auch die Aggregation der Einzelrisiken zu einer Gesamtrisikobelastung untersucht. Zu Beginn des Betrachtungszeitraumes betrachteten zwei Drittel der börsennotierten Unternehmen ihre Risiken vorrangig quantitativ, was eine Risikoaggregation ermöglicht. Ob diese zu diesem Zeitpunkt stattfand wurde im Rahmen der Studie nicht untersucht. (Ernst & Young AG 2005, S. 8)

Im Jahr 2011 ergab die PWC-Benchmarkstudie, dass 77% der Unternehmen eine quantitative Bewertung hinsichtlich Eintrittswahrscheinlichkeit und Schadensausmaß vornahmen. (Bundesverband der Deutschen Industrie e.V (BDI) und PricewaterhouseCoopers AG (PWC) 2011, S. 20)

Im Jahr 2010 wurde die Aggregation von Risiken konkret abgefragt. Hier wiesen 30% der Unternehmen eine Systematik zur Aggregation von Risiken auf. (Klenk und Reetz 2010, S. 7)

Im Jahr 2012 wurde von 21% der Unternehmen keine Risikoaggregation durchgeführt. Die übrigen 79% verwendeten verschiedene Methoden und Umfänge. Im Jahr 2015 wurde in einer Nachfolgestudie bei 14% der betrachteten Unternehmen keine Konsolidierung vorgesehen. Abbildung 16 zeigt eine Übersicht der verwendeten Aggregationsmethoden in den Jahren 2012 und 2015. Im Rahmen der Befragungen waren in beiden Jahren Mehrfachnennungen möglich.

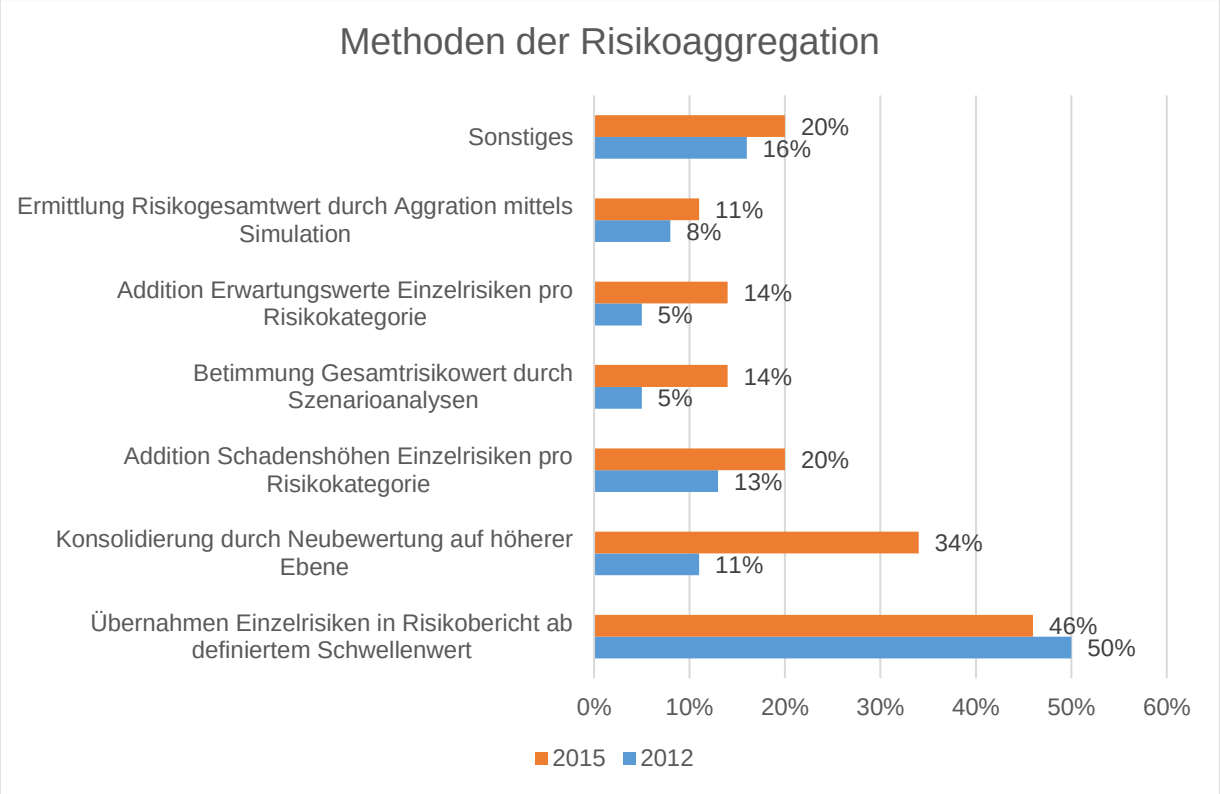

Abbildung 16: Methoden der Risikoaggregation 2012 und 2015
Quelle: Eigene Darstellung nach Herre et al. 2012, S. 31; Tilch et al. 2015, S. 33

Im Jahr 2017 nutzten 30% der Unternehmen verschiedene Verfahren zur Risikosimulation und damit zur Aggregation. (Deloitte 2017, S. 18)

Aktuell nehmen 75% der Unternehmen eine Aggregation der Einzelrisiken zu einer Gesamtrisikobetrachtung vor.

> *„69% der befragten Unternehmen verdichten Risiken durch Bildung von Aggregaten nach Risikoarten und 75% leiten inzwischen eine Einschätzung der Gesamtrisikosituation des Unternehmens auf Basis der gemeldeten Einzelrisiken ab.“ (Deloitte 2020, S. 21)*

Berichterstattung

Bereits 2005 erfolgte in 80% der börsennotierten Unternehmen neben einer regulären Berichterstattung auch eine Ad-hoc Berichterstattung über wesentliche Änderungen der Risikosituation an den Vorstand. (Ernst & Young AG 2005, S. 5)

Fünf Jahre später waren in 9% der betrachteten Organisationen keine Ad-hoc Berichtsprozesse etabliert. (Klenk und Reetz 2010, S. 29) Dieser Anteil sank 2012 auf 8%. (Herre et al. 2012, S. 34)

Im Jahr 2011 wurde die Anpassung der Berichterstattung nach der Finanzkrise untersucht, hierbei ergaben sich folgende Änderungen.

> *„Knapp 60 % der Befragten haben ihre Risikoberichterstattung angepasst, 55 % setzen häufiger qualitative Methoden ein als vor der Krise. Gut vier von zehn Befragten geben an, dass Risiken nunmehr anders bzw. mit neuen Modellen gemessen werden, während knapp 40 % ihr Risikomanagement auf weitere Unternehmensbereiche ausgedehnt haben." (Herre und Tüllner 2011, S. 13)*

Auch die Empfänger der Risikoberichterstattung haben sich im Betrachtungszeitraum entwickelt. Neben dem Vorstand beziehungsweise ersten Führungsebene wird auch an den Aufsichtsrat und tiefere Führungsebenen berichtet.

2010 sowie 2011 berichteten alle Organisationen an die Unternehmensleitung, 97% berichteten ebenfalls an den Aufsichtsrat. (Herre et al. 2012, S. 35) In 2015 berichteten bereits alle Unternehmen auch an den Aufsichtsrat. (Tilch et al. 2015, S. 41)

Dies wurde auch in Studien aus den Jahren 2017 und 2020 bestätigt.

> *„Ferner lassen sich die Aufsichtsräte aller Studienteilnehmer regelmässig über den Stand des RMS und die Risikosituation berichten." (Deloitte 2017, S. 8, 2020, S. 15)*

Prüfung, Überwachung und Prüfbarkeit des Risikomanagementsystems

Bei 67% der Organisationen war 2005 eine Möglichkeit zur Prüfung durch die Gremien der Revision und Wirtschaftsprüfer gegeben. Zudem wurde angegeben, dass „*die Bereitschaft/Nachfrage zur freiwilligen, unabhängigen Prüfung ihres Risikomanagementsystems bei nicht börsennotierten Gesellschaften zu steigen scheint" (Ernst & Young AG 2005, S. 7–8)*

2012 wird insbesondere die interne Revision als Überwachungsorgan für das Risikomanagementsystem gesehen.

„Die Interne Revision überwacht hingegen als prozessunabhängige Überwachungsinstanz vor allem die Anwendung der Maßnahmen, die vollständige Erfassung der Risikofelder und die Einhaltung prozessintegrierter Kontrollen. In 41 % der Unternehmen wurde im Berichtsjahr keine prozessunabhängige Überwachungstätigkeit des RMS durchgeführt. Hier zeichnet sich eine Verbesserung gegenüber dem Vorjahr um 11 % ab." (Herre et al. 2012, S. 12)

In der gleichen Studie wird auch auf den Prüfungsstandard 340 des IDW erwähnt.

„Die im IDW PS 340 definierten Prüfungsbereiche, die unter anderem danach fragen, ob alle Risikofelder vollständig erfasst sind, ob die Maßnahmen kontinuierlich angewendet und Bewertungskriterien und prozessintegrierte Kontrollen eingehalten werden, wurden lediglich in 35 % bzw. 38 % der Unternehmen im Rahmen der prozessunabhängigen Überwachung untersucht." (Herre et al. 2012, S. 42)

2015 gaben 57% der Unternehmen an, dass im vergangenen Berichtsjahr in deren Organisation eine *„konkrete Revisionsprüfungen mit direktem Fokus auf das RMS"* stattgefunden hat. (Tilch et al. 2015, S. 47)

Im österreichischen Mittelstand gaben im Jahr 2014 41 Prozent der betrachteten Unternehmen an, noch nie ein *„Risiko-Assessment"* durchgeführt zu haben. (Theuermann und Ebner 2014, S. 27)

Optimierung des Risikomanagementsystems und dessen Bestandteile sowie Frequenz

Allgemein wird das Risikomanagementsystem beziehungsweise einzelne oder mehrere Bestandteile dessen, in der Mehrheit der Organisationen zumindest jährlich analysiert und gegebenenfalls angepasst. (Vgl. Klenk und Reetz 2010, S.15; Boutellier et al. 2013, S.16; vgl. Tilch et al. 2015, S.19, S.27)

Beispielsweise gaben im Jahr 2010 75 Prozent der befragten Unternehmen an, ihre Risikorichtlinie im letzten Jahr überarbeitet zu haben, bei 45% fand dies innerhalb des letzten Halbjahres statt. Darüber hinaus gab es bei 41% noch Bedarf, die Vorgaben zum Risikomanagementsystem zu überarbeiten. Unter anderem da die vorangegangenen Anpassungen lediglich Teilaspekte des RMS abdeckten. (Klenk und Reetz 2010, S. 15)

In der Folgestudie 2012 waren es bereits 58% der Unternehmen, welche einen Bedarf zur Anpassung des RMS sahen. Hier wird unter anderem das BilMoG als Grundlage für eine notwendige Überarbeitung genannt.

„Der vom Gesetzgeber im Rahmen des BilMoG ergänzte rechtliche Rahmen – insbesondere die Verdeutlichung der Überwachungsaufgaben der Aufsichtsräte – hat in den Unternehmen bisher nur vereinzelt zur Überarbeitung des Risikomanagements geführt. Im Vergleich zur

letzten Studie konnten deshalb nur leichte Qualitätsverbesserungen beobachtet werden." (Herre et al. 2012, S. 43)

In einer weiteren Folgestudie 2015 verringerten sich die oben genannten Anteile, was mit fehlenden Anpassungen der Regulatorien begründet wird.

„Unsere Untersuchung zeigt auch, dass nur noch 45% der Unternehmen innerhalb der letzten 12 Monate ihre Risikorichtlinie aktualisiert haben und nur in 28% der Fälle dies weniger als sechs Monaten. [...] Eine mögliche Erklärung liegt darin, dass wesentliche gesetzliche Neuregelungen in diesem Zeitraum nicht stattfanden und eine Aktualisierung vor diesem Hintergrund nicht unbedingt notwendig war." (Tilch et al. 2015, S. 19)

2017 planten 38% eine Überarbeitung des eigenen Risikomanagementsystems aufgrund des neuen IDW Prüfungsstandards 981. (Deloitte 2017, S. 20)

Im Jahr 2020 gaben 56% der Organisationen an, eine Überarbeitung des RMS zu planen, insbesondere mit Bezug zur Neufassung des IDW PS 340.

„Die Mehrheit der betrachteten Unternehmen [Anmerkung: 56%] plant zum Befragungszeitpunkt eine Überarbeitung des RMS, was auskunftsgemäß häufig auf die regulatorischen Neuerungen des IDW PS 340 n.F. zurückzuführen ist. Darüber hinaus bestehen weitere Anlässe bspw. aufgrund einer angestrebten besseren Verzahnung mit weiteren Governance- und Steuerungssystemen [...], RMS Softwareanpassungen bzw. -einführungen und Analysen zu Nutzungsmöglichkeiten der Digitalisierung für das RMS [...]." (Deloitte 2020, S. 23)

Aber auch außerhalb geplanter Zyklen finden Anpassungen statt. In einer Untersuchung nach der weltweiten Wirtschaftskrise gaben 60% der Organisationen an, ihr Risikomanagement als Reaktion auf die Krise überarbeitet zu haben. Die verbleibenden 40% gaben an, keinen Änderungsbedarf zu sehen. In der gleichen Studie gaben zudem 82% an, zufrieden mit der Performance des eigenen Risikomanagementsystems zu sein. 11% waren dies nicht und 7% antworteten mit „*weiß nicht*". (Herre und Tüllner 2011, S. 9–10)

Im gleichen Jahr gaben in einer anderen Studie ein Drittel der Befragten an, mit dem Risikomanagement zufrieden zu sein. Die Bereiche, in welchen die Unternehmen Potentiale zur Verbesserung sehen, sind in Abbildung 17 dargestellt.

„Nur 28 % der befragten Unternehmen sind mit ihrem Risikomanagement zufrieden. Viele sehen Verbesserungspotenzial bei Identifikation, Bewertung, Vermeidung und Reduzierung von Risiken sowie in Verbindung mit der Unternehmenssteuerung." (Bundesverband der Deutschen Industrie e.V (BDI) und PricewaterhouseCoopers AG (PWC) 2011, S. 8)

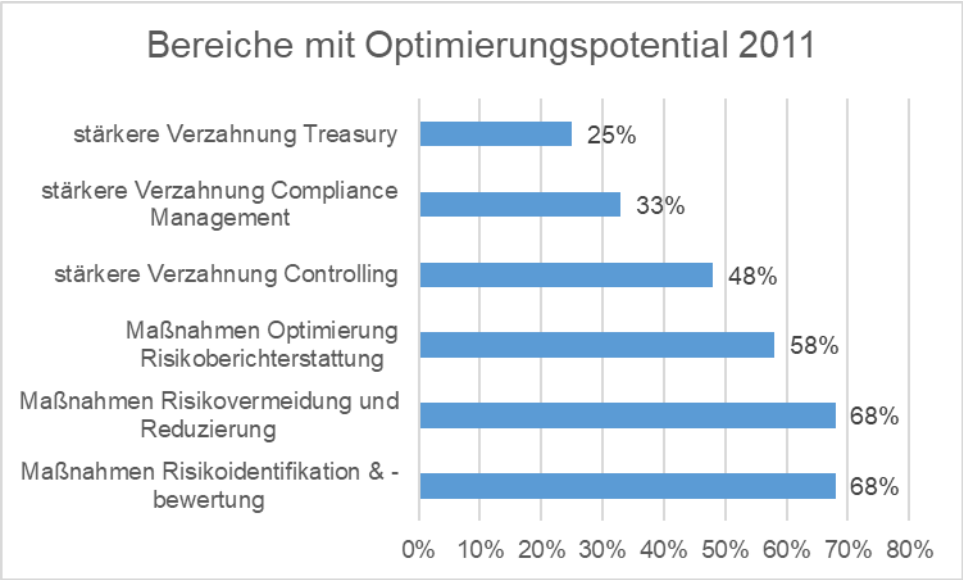

Abbildung 17: Bereiche mit Optimierungspotential im RM 2011
Quelle: Bundesverband der Deutschen Industrie e.V (BDI) und PricewaterhouseCoopers AG (PwC) 2011, S. 15

Auch in den von Deloitte durchgeführten Studien aus 2017 und 2018 wurde für die einzelnen Bereiche des Risikomanagements die Notwendigkeit einer Optimierung abgefragt. Hierbei waren für jeden Bereich die Antwortmöglichkeiten *„Sehr gut“*, *„Optimierungspotential“* und *„Handlungsbedarf“* möglich. Folgende Abbildung zeigt für die abgefragten Bereiche des RM den Anteil der Unternehmen jeweils im Jahr 2017 und 2020, welche Optimierungsbedarf sehen. Hierbei wurden die Anteile der Antworten *„Optimierungspotential“* und *„Handlungsbedarf“* zusammengefasst.

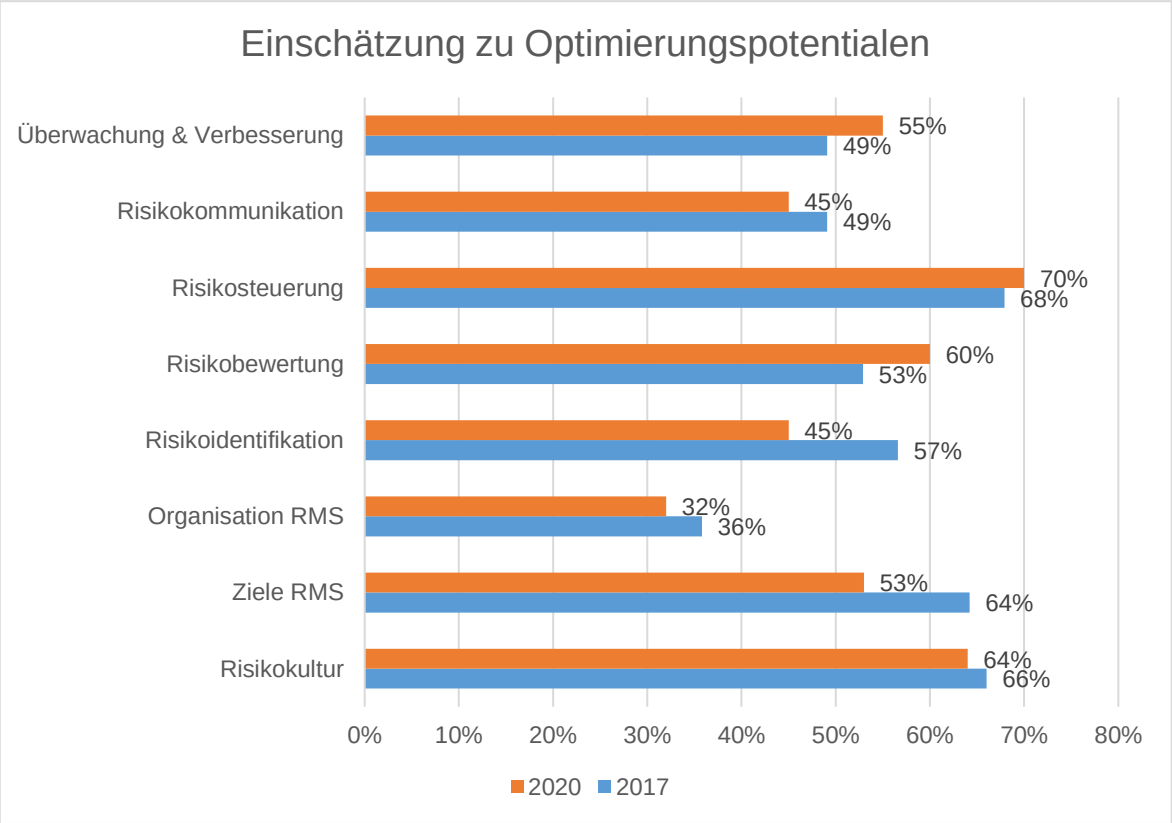

Abbildung 18: Vergleich Optimierungspotentiale 2017 und 2020
Quelle: Eigene Darstellung nach Deloitte 2017, S. 13, 2020, S. 18

Auch die Überarbeitung der Risikoidentifizierung und -bewertung als Bestandteil des Risikomanagements wird in verschiedenen Studien analysiert. Hierbei existieren unterschiedliche Frequenzen in den betrachteten Unternehmen.

Der Vergleich der Frequenz in den Jahren 2010, 2012 und 2015 zeigt, dass die Mehrheit der Unternehmen eine quartalsweise Risikoidentifizierung vornimmt. Der Anteil der Organisationen mit monatlicher Überarbeitung war 2015 (9%) deutlich niedriger als in den beiden Vorgängerstudien 2012 (16%) und 2010 (15%).

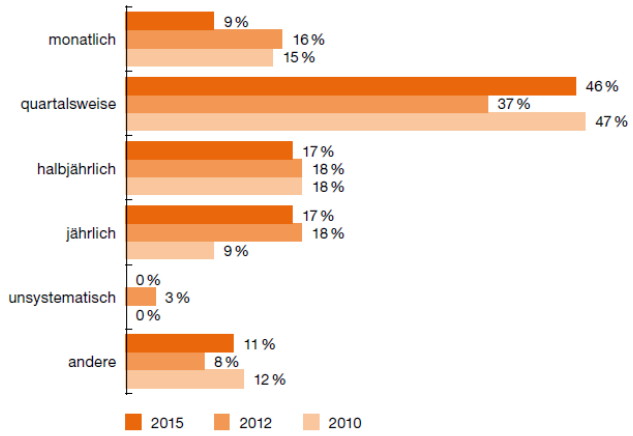

Abbildung 19: Vergleich der Frequenz der Risikoidentifikation 2010, 2012 & 2015
Quelle: Tilch et al. 2015, S. 27

Eine von EY bei Unternehmen aus 63 verschiedenen Ländern weltweit durchgeführte Studie aus dem Jahr 2015 zeigt, dass weltweit 77% der befragten Organisationen eine jährliche Risikobewertung vornehmen.

> *"77% of respondents evaluate their organization´s risk profile on an annual basis, limiting their ability to adjust their business strategy based on changes to their risk landscape." (Ernst & Young AG 2015, S. 17)*

In der Schweiz überwog 2013 eine jährliche Bewertung der Risiken, wohingegen gesetzte Gegenmaßnahmen quartalsweise überprüft wurden. (Boutellier et al. 2013, S. 16)

Im österreichischen Mittelstand zeigte sich 2014 ein Trend zu einer unterjährigen Planung im Risikomanagement. Hier arbeiteten 42% der befragten Unternehmen mit einem jährlichen Planungshorizont, 29% gaben eine unterjährige Planung an. (Theuermann und Ebner 2014, S. 25)

4.4 Diskussion Umsetzungsstand

Die in Kapitel 4.3 analysierten Studien zeigen, dass sich im Betrachtungszeitraum verschiedene Bereiche und auch das Risikomanagement und RMS als Gesamtes verändert hat, während manche Aspekte bereits zu Beginn des Betrachtungszeitraums gegeben waren.

Im gesamten Betrachtungszeitraum stimmen Studien dahingehend überein, dass die Verantwortung für das Risikomanagement innerhalb einer Organisation in der höchsten Führungsebene angesiedelt ist und dies auch nötig ist. Die Ausführung der operativen und strategischen Bestandteile innerhalb des Risikoprozesses können allerdings durchaus mithilfe andere Organe der Organisation erfolgen. Die endgültige Entscheidungsmacht liegt im Top-Management und sollte auch hier verankert bleiben. Die Rollen der Verantwortlichen im Top-Management können je nach Aufbauorganisation variieren. Während in manchen Unternehmen der CFO für das Risikomanagement verantwortlich ist, existieren in anderen Organisationen CROs, welche auf identischer Ebene agieren. In anderen Gesellschaftsformen wäre dies analog die (kaufmännische) Geschäftsführung oder andere Vorstandsmitglieder.

Entgegen der Annahme, dass der Anteil der Unternehmen mit eigener Abteilung und Rolle für das Risikomanagement stetig mit der wachsenden Bedeutung des Risikomanagements steigt, zeigt sich wie auch in den Abbildungen 12 und 13 ersichtlich, ein etwas anderes Bild. Hieraus geht hervor, dass der Anteil der Organisationen mit eigener Risikomanagementabteilung von 2007 auf 2012 sowie von 2015 auf 2020 im Allgemeinen abgenommen hat. Auffällig ist hier der geringe Anteil im Jahr 2012 von lediglich 18%.

Abbildung 13 zeigt deutlich, dass ein Teil der Schwankungen damit erklärt werden kann, dass die Teilnehmenden der Studien teils stark variieren. Während hier in einer Studie aus 2015 97% angeben, eine eigene RM-Rolle etabliert zu haben, sind dies im gleichen Jahr in einer anderen Studie lediglich 56%. Bei der Etablierung der Rolle lässt sich ein eindeutiger Trend nach oben erkennen. Ausreißer können zudem dadurch erklärt werden, dass abgefragte Rollenprofile zwischen den Studien abweichen können. Möglicherweise berücksichtigte hier ein Teil der Unternehmen lediglich, ob ein CRO auf Vorstandsebene existiert, während andere Organisationen auch Risikokoordinatoren auf tieferer Führungsebene angaben.

Diesem Trend folgend ist davon auszugehen, dass es aktuell in fast allen Organisationen eine Rolle gibt, welcher explizit das Management von Risiken zugeschrieben wird.

Ebenso geht aus den Studien hervor, dass das Risikomanagement in der Aufbauorganisation dem Finanz- bzw. Controlling Bereich zugeordnet wird, insofern kein eigener Bereich besteht. Dementsprechend wird auch zukünftig eine enge Zusammenarbeit zwischen der Controlling Abteilung und dem Risikomanagement notwendig sein, um die Unternehmensziele bestmöglich zu erreichen und die Organisation abzusichern. Natürlich ist auch eine Zusammenarbeit des Risikomanagements mit den übrigen Unternehmensbereichen notwendig, diese fokussiert sich allerdings insbesondere auf den operativen Risikomanagementprozess.

Durch die innerhalb des Unternehmens übergreifende Zusammenarbeit kann auch die Situation zur Risikokultur und -strategie verbessert werden, welche gemäß den analysierten Studien auch aktuell noch ausbaufähig sind. Für ein umfassendes Risikomanagement muss eine Risikostrategie des Unternehmens etabliert werden, welche allen Unternehmensmitarbeitenden bekannt ist und von diesen umgesetzt werden kann. Auch hier ist bereits ein positiver Trend erkennbar. Im Jahr 2012 hatte sich der Anteil der Unternehmen mit einer anwendbaren Risikostrategie im Vergleich zu 2010 bereits mehr als verdoppelt, was die Bedeutung einer solchen Strategie unterstreicht. Ebenfalls positiv zu deuten ist hierbei, dass die Bedeutung auch im länder- und branchenspezifischen Vergleich gleichbleibt. In allen Ländern der DACH-Region gewann eine Risikokultur bzw. Strategie in den betrachteten Studien an Bedeutung. Bei Annahme der Fortführung dieses positiven Trends liegt der Anteil der Schweizer Unternehmen mittlerweile bei über 90%, was den Wert aus 2017 darstellt. Auch im österreichischen Handel dürfte sich aktuell eine ähnliche Zahl wiederspiegeln. Hier waren es 2014 bereits 65%.

Auch Chancen als Bestandteil des Risikomanagements folgen über den Betrachtungszeitraum einem positiven Trend. Waren es zu Beginn noch lediglich ein Drittel der Unternehmen, welche auch Chancen im Rahmen des Risikomanagements berücksichtigen, hat sich dieser Anteil bis zum Jahr 2020 verdreifacht. Insbesondere in der jüngeren Vergangenheit seit 2017 erfolgte hier ein steiler Anstieg. Dies stimmt auch mit den Beobachtungen zur Risikostrategie überein. Um eine umfassende Risikostrategie zu erarbeiten, ist auch die Betrachtung und folglich die Berichterstattung zu Chancen neben Risiken unerlässlich. Daher erhöhte sich erwartungsgemäß mit steigendem Anteil der Unternehmen mit Risikokultur auch der Anteil der Unternehmen mit Chancenberichterstattung.

Die Ausrichtung des organisatorischen Risikomanagements geht mittlerweile weit über eine reine Erfüllung von gesetzlichen und anderen regulatorischen Anforderungen hinaus. Das Risikomanagement soll unter anderem dazu beitragen, Unternehmensziele zu erreichen sowie der Organisation einen Wettbewerbsvorteil gegenüber Mitbewerbenden zu verschaffen. Die Untersuchung zeigt beispielsweise, dass über den gesamten Betrachtungszeitraum in der Mehrheit der befragten Unternehmen die gesetzlichen Anforderungen erfüllt werden. Im Jahr 2020 waren dies 98%. (Deloitte 2020, S. 14)

Für die verbleibenden zwei Prozent gilt es ebenfalls, die Anforderungen zu erfüllen. Allerdings kann dies hier damit erklärt werden, dass in der betroffenen Studie lediglich die Ziele abgefragt wurden. Somit kann davon ausgegangen werden, dass bei dem verbleibenden Anteil die gesetzlichen Anforderungen durchaus erfüllt werden, dies aber kein gesondertes Ziel der Unternehmen darstellt. In der Zielsetzung findet sich auch der Punkt der Risikokultur wieder. In der Schweiz lag die Förderung einer internen Risikokultur im Jahr 2013 auf Platz 2 der Hintergründe zur Einführung eines Risikomanagements im Unternehmen, noch vor der Erfüllung der gesetzlichen Anforderungen, welche auf Platz 3 folgten. (Boutellier et al. 2013, S. 6) Diese Einstellung von Schweizer Unternehmen bestätigt sich im Jahr 2017, in welchem über 90% angaben, eine Risikokultur etabliert zu haben.

Insgesamt zeigt der Trend in der Risikomanagementausrichtung klar von einer reinen Erfüllung von gesetzlichen uns sonstigen Anforderungen zu einer aktiven Nutzung des RM und RMS im Rahmen verschiedener Aspekte der Unternehmensführung. Auch wenn der Anteil an Organisationen, welche das RM bereits weiterführend nutzen, stetig steigt, existieren noch zahlreiche Verbesserungsmöglichkeiten in Sachen RMS. Um den Anteil weiter auszubauen, ist unter anderem ein weitreichenderes Risikoverständnis und -bewusstsein notwendig. Insbesondere muss die Nutzung der Risikomanagementsysteme auch im Bereich der Risikosteuerung ausgebaut werden. Eine aktive Steuerung von Risiken wirkt sich durchaus auf die Unternehmenssteuerung und den Unternehmenserfolg aus. Denn wenn

bereits im Vorhinein ein konkretes Planungsszenario zum Umgang mit den jeweiligen Risiken besteht, kann bei deren Eintritt schneller gehandelt werden und somit negative Auswirkungen auf die Organisation und deren Erfolg minimiert werden.

Hierzu ist auch eine geeignete Risikopriorisierung notwendig. Da die konkrete Priorisierung beziehungsweise Reihung von Risiken nur in wenigen Studien erfolgte, kann hier keine repräsentative Diskussion der Ergebnisse erfolgen. Jedoch zeigt sich, dass auch in den wenigen Studien die Risiken von Terrorismus und einer Pandemie bzw. Gesundheitskrise nicht ausreichend betrachtet werden. Diese sind meist am unteren Ende einer Priorisierungsliste oder auch gar nicht genannt. Dies impliziert auch, dass Unternehmen auf den Eintritt dieser Risiken nicht oder nicht ausreichend vorbereitet sind.

Neben einer Betrachtung von Einzelrisiken, ist auch die Einbeziehung von Wechselwirkungen und eine Gesamtrisikobetrachtung von großer Bedeutung. Erstaunlicherweise lässt sich bei Betrachtung der Wechselwirkungen ein schwankender Trend beobachten. Während 2005 die Hälfte der Unternehmen eine solche Betrachtung vornahm, sank der Anteil bis 2012 auf 24%. 2015 waren es wieder knapp die Hälfte der Organisationen, während es zum Ende des Betrachtungszeitraumes im Jahr 2020 wieder lediglich 34% der Unternehmen waren. Allerdings stellt die Betrachtung von Risikokorrelationen eine wichtige Komponente eines RMS dar. Hier gibt es derzeit also in zumindest zwei Dritteln der Unternehmen einen dringenden Aufholbedarf, um die Risikosituation und -exposition der Organisation umfassend abzubilden.

Ein besseres Bild zeigt sich bei der Risikoaggregation. Hier waren es zuletzt 75% der Organisationen, welche neben der Betrachtung von Einzelrisiken auch eine Gesamtrisikobetrachtung vornahmen. (Deloitte 2020, S. 21)

Auch generell ist der Anteil der Unternehmen mit Gesamtrisikobetrachtung über den gesamten Betrachtungszeitraum höher als der Anteil mit Betrachtung von Wechselwirkungen. Unter anderem kann dies darauf zurückgeführt werden, dass eine Gesamtrisikobetrachtung mit geringerem Aufwand als eine Korrelationsbetrachtung vorgenommen werden kann. Natürlich existieren verschiedene unterschiedliche Möglichkeiten zur Risikoaggregation, welche auch einen unterschiedlichen Komplexitätsgrad aufweisen, was in die Betrachtung miteinbezogen werden muss. Die sowohl 2012 als auch 2015 meist verbreitetste Methode stellte eine reine Übernahme von Einzelrisiken in den Risikobericht dar, sobald diese einen bestimmten Wert überschreiten. Hierbei sind keine aufwendigen Berechnungen oder Simulationen notwendig. Komplexere Methoden, wie die zuletzt genannte Simulation werden von einem deutlich geringeren Teil von Unternehmen eingesetzt. Dies kann sowohl mit dem erhöhten Bedarf an personellen als auch systemtechnischen und zeitlichen Ressourcen

erklärt werden. Es lässt sich ableiten, dass Methoden mit geringerem Aufwand von deutlich mehr Organisationen eingesetzt werden als aufwendigere aber auch aussagekräftigere und verlässlichere Methoden. Hier ist der Bedarf gegeben, dass Organisationen vermehrt auch auf komplexere Simulationen zur Risikoaggregation zurückgreifen, um auch hierdurch die Abbildung der Risikosituation zu verbessern. Es ist davon auszugehen, dass mit einer vermehrten Nutzung von Simulationen und Berechnungen auch der Anteil an Unternehmen steigt, welche Wechselwirkungen zwischen Risiken betrachten, da diese Korrelationen unbedingt in die Gesamtrisikoanalyse miteinbezogen werden müssen.

Bei Berichterstattung sowie Prüfung bzw. Prüfbarkeit des RMS ergaben sich im Betrachtungszeitraum lediglich wenige Änderungen. Zum einen kann dies damit erklärt werden, dass bereits zu Beginn der 2000er Jahre ein großer Anteil der Organisationen eine Berichterstattung zur Risikosituation vornahm. Durchaus ergaben sich aber Anpassungen in der Form und Frequenz der Berichterstattung. Inzwischen findet in allen Unternehmen neben einem Bericht an den Vorstand auch eine Berichterstattung an den Aufsichtsrat statt. Auch etablierte sich eine mögliche Ad-Hoc Berichterstattung im Betrachtungszeitraum.

Eine ähnliche Situation ist bei Betrachtung der Prüfung und Prüfbarkeit zu erkennen. Zum einen steigt die Bereitschaft zu einer regelmäßigen internen Prüfung und Überwachung des RMS insbesondere durch die interne Revision. Dies ist positiv zu bewerten, da nur durch eine stetige Überwachung und Prüfung eine Weiterentwicklung der organisationsweiten RM und RMS sichergestellt werden kann. Ein Verbesserungspotential ist hier durchaus eine mögliche vermehrte Inanspruchnahme von externen Prüfungen. Durch eine externe Prüfung können noch mehr Schwachstellen und Optimierungspotentiale im RM gefunden werden, welche anschließend zur gezielten Weiterentwicklung des RMS genutzt werden können.

Damit einhergehend werden abschließend Optimierungen des RMS, deren Bestandteile und Frequenz diskutiert. Es zeigt sich ein kontinuierlicher Bedarf zu Überarbeitungen über den gesamten Betrachtungszeitraum. Zum einen zeigt sich dadurch, dass das RM der Organisationen noch nicht ausgereift ist, zum anderen zeigt dies aber auch deutlich, dass die Bereitschaft besteht, das eigene RMS zu verbessern und dadurch die Organisation besser gegen Risiken abzusichern. Insbesondere in den Bereichen Risikobewertung und dessen Vermeidung und Reduzierung zeigt sich seit 2011 Optimierungspotential. Dies kann mit dem zuvor beschriebenen Potential im Rahmen der Risikokorrelation und -aggregation gesehen werden. Nur wenn eine entsprechende Risikobewertung stattfindet, ist auch die Einschätzung von Wechselwirkungen sowie die Berechnung einer Gesamtrisikosituation möglich. Auch in Sachen Risikokultur und Ziele des RMS zeigt sich ein deutliches Bild. Hier

sehen aktuell noch mehr als die Hälfte der Unternehmen Bedarf zur Verbesserung. Auch hier zeigt sich eine Übereinstimmung mit der Veränderung der Ausrichtung des RM. Im Rahmen der Diskussion der Ausrichtung des RMS wurde die Notwendigkeit eines verbesserten Risikoverständnisses beschrieben. Dies sieht aktuell auch die Mehrheit der Unternehmen so. Die vergleichsweise hohe Einschätzung des Bedarfs zu Optimierungen ist positiv zu bewerten, da nur so eine Weiterentwicklung des RMS gewährleitet werden kann. Dies trägt auch zur Absicherung des Unternehmenserfolges bei. Ebenfalls positiv zu bewerten ist die Verkürzung der Frequenz der Überarbeitung von Risiken. Diese hat sich inzwischen auf eine quartalsweise Neubetrachtung etabliert. Nur durch eine Evaluierung der Situation und Risiken in regelmäßigen Abständen können notwendige Maßnahmen zu Vermeidung, Verringerung und zum Umgang mit aktuellen Risiken eingeleitet und angepasst werden. Hierzu kann eine planmäßige quartalsweise Betrachtung in Verbindung mit einer gegebenenfalls erforderlichen Ad-hoc Analyse empfohlen werden.

5. Zeitlicher Zusammenhang von gesetzlichen Änderungen, relevanten Ereignissen und Umsetzungsstand

In diesem Kapitel werden die Ergebnisse aus Kapitel 3 sowie Kapitel 4 zusammengeführt und ein Zusammenhang diskutiert.

5.1 Zusammenführung der Ereignisse, gesetzlichen und quasigesetzlichen Änderungen sowie Umsetzungsstand

Um einen Überblick über die zeitliche Einordnung der betrachteten Studien zu erlangen, werden diese in die zuvor erstellte Abbildung 10 eingefügt. Hierfür wurden die in Tabelle 1 vergebenen Nummern für die jeweilige Studie verwendet.

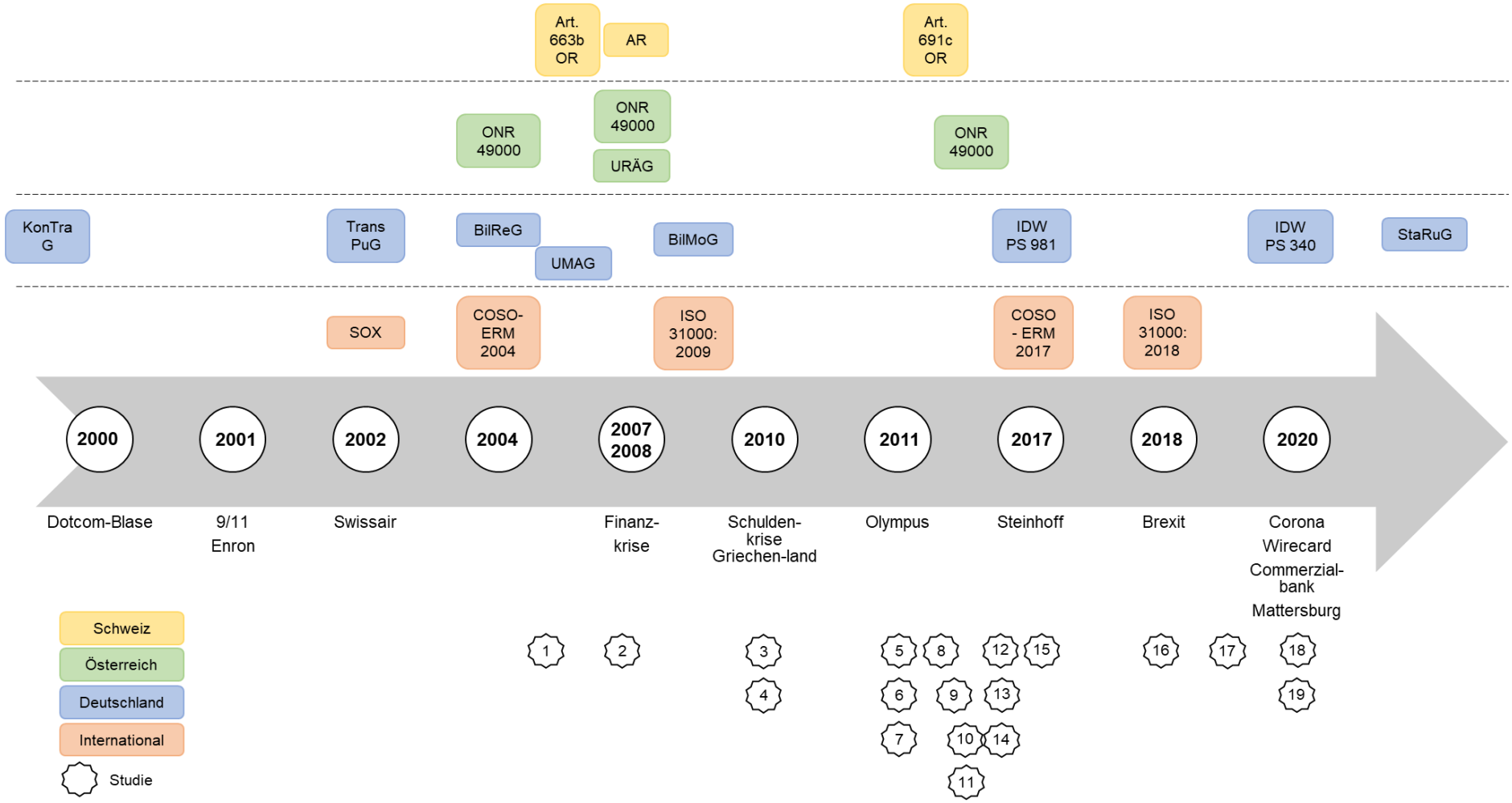

Abbildung 20: Zeitlicher Zusammenhang Ereignisse, Gesetze, Standards und Studien

Quelle: Eigene Darstellung

5.2 Diskussion des Gesamtzusammenhangs

Zunächst erfolgt eine Beschreibung der Erwartungshaltung sowie der sich aus Abbildung 20 ergebenden visuell ersichtlichen Erkenntnisse. Anschließend werden die Zusammenhänge anhand der Gesetzes- und Standardänderungen diskutiert.

5.2.1 Erwartungshaltung und visueller Zusammenhang

Folgende Abbildung stellt die Erwartungshaltung zum zeitlichen Zusammenhang der betrachteten Komponenten in der vorliegenden Arbeit dar.

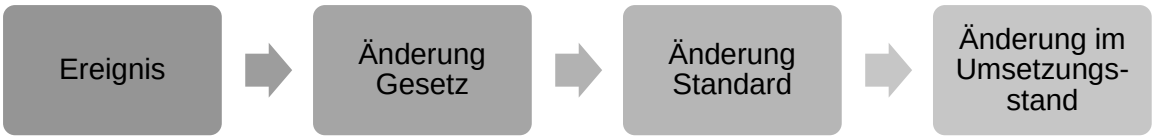

Abbildung 21: Erwartungshaltung zeitlicher Zusammenhang
Quelle: Eigene Darstellung

Wie Abbildung 20 verdeutlicht, lässt sich bei gesetzlichen und sonstigen Anforderungen eine klare Kumulation zwischen den Jahren 2004 und 2009 erkennen. Auch im und um das Jahr 2017 lässt sich eine kleine Konzentration an Änderungen erkennen. Auffällig ist zudem, dass es in den Jahren 2010 bis 2014 keine Änderungen der Gesetze und Standards gab.

Die betrachteten Studien hingegen fanden größtenteils in diesem Zeitraum statt, in welchem keine beziehungsweise nur einzelne Änderungen vorgenommen wurden. In der vorliegenden Arbeit wurden die meisten Studien in den Jahren 2010 bis 2015 durchgeführt. Dies ist insofern nicht verwunderlich, da Organisationen eine gewisse Zeitspanne benötigen, um erfolgte Änderungen in die Praxis umzusetzen und innerhalb des Unternehmens zu etablieren. Bei rein zeitlicher Betrachtung der Ereignisse, Gesetze, sonstigen Anforderungen sowie den Zeitpunkten der durchgeführten Studien lässt sich feststellen, dass der Großteil der Studien nach der Häufung an Gesetzesänderungen durchgeführt wurde.

Im Allgemeinen zeigt sich der Zusammenhang zwischen Gesetzen beziehungsweise Standards und dem Umsetzungsstand deutlich in den abgefragten Zielen und Grundlagen der jeweiligen Risikomanagementsysteme in den Organisationen. Jeweils in allen bzw. nahezu allen befragten Unternehmen stellt die Erfüllung gesetzlicher und regulatorischer Anforderungen ein Ziel des RMS oder die Grundlage dessen dar. Somit kann ein genereller Zusammenhang zwischen gesetzlichen/regulatorischen Änderungen und dem RM-Umsetzungsstand in Organisationen bestätigt werden.

Folgende Tabelle zeigt eine Übersicht über die bedeutendsten Gesetzesänderungen und anschießend beobachtete Änderungen beziehungsweise erkannte Potentiale zur Verbesserung des RMS im Umsetzungsstand.

Gesetz/Standard	**Beobachtete Änderungen & erkannte Potentiale im Umsetzungsstand**
SOX	Allgemeines Vorhandensein Risikomanagementsystem in Unternehmen
KonTraG	Lediglich 25% berichtet über Chancen Verbesserungsbedarf Chancenberichterstattung
TransPuG	Öffentlich abrufbare Entsprechenserklärung zum DCGK
COSO ERM 2004 ONR49000ff 2004	Nutzung des RMS auch außerhalb gesetzlicher Anforderungen, Schnittstellen zu anderen Unternehmensbereichen (positiver Trend)
BilReG	Intensivierung der Chancenberichterstattung (positiver Trend)
Art. 663b OR	(Formaler) Risikomanagementprozess im Unternehmen und in Berichterstattung etabliert
URÄG	Etablierung & aktive Nutzung Risikomanagementsystem sowie entsprechende Berichterstattung
BilMoG	Anpassung der RM-Berichterstattung (Ad-hoc Berichtsprozess) Angabe der Notwendigkeit zur Überarbeitung des RMS
ONR49000ff 2008 ISO 31000	Positiver Trend bei Einrichtung einer eigenen RM-Rolle und RM-Abteilung
Art. 691c OR	Performance orientiertes RM in Schweizer Unternehmen (alle Unternehmensgrößen)
ONR49000ff 2014 COSO ERM 2017 ISO 31000 2018	Positiver Trend bei Risikokultur und Risikostrategie in österreichischen Unternehmen Vorhandensein einer positiven Risikokultur in Schweizer Unternehmen Verbesserungsbedarf zu Risikokultur in deutschen Unternehmen Verantwortung RM im Top-Management (in Mehrheit der Unternehmen bereits zuvor gegeben)
IDW PS 981 (freiwillige Anwendung)	Bereitschaft zur Anpassung des RMS an IDW PS 981 in deutschen Unternehmen Positiver Trend bei Risikokultur in deutschen Unternehmen Rückgang Anteil Unternehmen mit RMS als aktives Steuerungsinstrument
IDW PS 340 n.F. (verpflichtende Anwendung)	Verbesserungspotential bei Durchführung von Risikoaggregation & Risikokorrelation Keine weiteren empirischen Werte vorhanden

Tabelle 3: Übersicht Gesetze und Standards sowie resultierende Änderungen im Umsetzungsstand

Im folgenden Abschnitt wird der konkrete Zusammenhang von einzelnen Ereignissen mit Änderungen in den diversen Anforderungen und Umsetzungspraktiken im Detail diskutiert. Die Diskussion erfolgt chronologisch nach den gesetzlichen und sonstigen Änderungen. Diese stellen das Bindeglied zwischen den Ereignissen und dem Umsetzungsstand dar.

5.2.2 Einführung eines Risikomanagementsystems nach KonTraG und SOX

Bereits in der Analyse der Literatur zu Ereignissen, der Gesetze und der Studien wurden einige konkrete Zusammenhänge zwischen einzelnen Ereignissen, Gesetzen und Umsetzungsstand genannt. Insbesondere der Sarbanes-Oxley Act, welcher die Basis für zahlreiche Gesetzesänderungen weltweit darstellt, wird durch den Bilanzskandal um das Unternehmen Enron begründet. (vgl. Biel 2005; Nicklisch 2007) Hierbei handelt es sich sicherlich nicht um die alleinige Grundlage für den SOX, allerdings lässt sich der Fall Enron als direkter Auslöser der Verabschiedung des Gesetzes beschreiben. Erwähnenswert ist hierbei die sehr zeitnahe Erarbeitung und Einführung des Sarbanes-Oxley Acts. Nur ein Jahr nach dem Skandal um Enron im Jahr 2001 wurde dieser bereits eingeführt.

Die erste analysierte Studie stammt aus dem Jahr 2005 und behandelt deutsche Unternehmen. Ein direkter Zusammenhang zwischen dem SOX und dem Umsetzungsstand lässt sich nicht erkennen.

Allerdings wird in der weltweit durchgeführten Studie des *Economist* aus dem Jahr 2007 erwähnt, dass Gesetze und Regulatorien eine große Rolle in der Weiterentwicklung des unternehmerischen Risikomanagements spielen. Zuvor wird neben branchenspezifischen Regulatorien wie *Basel II* auch der Sarbanes-Oxley Act als weitreichender, umzusetzender Standard im Risikomanagement der Organisationen beschrieben. (Economist Intelligence Unit 2007, S. 5f) Weltweit lässt sich also ein Zusammenhang zwischen dem SOX und der Risikomanagementumsetzung in Unternehmen erkennen. Erweitert um den Fall Enron als Auslöser des SOX, kann hier die erwartete Reihung gemäß Abbildung 21 zumindest teilweise bestätigt werden. Die nur teilweise Bestätigung wird damit begründet, dass in der vorliegenden Studie des Economist keine konkreten Umsetzungsaspekte direkt mit dem SOX in Verbindung gebracht werden, sondern lediglich der allgemeine Status des Risikomanagements in den Unternehmen.

Durch das KonTraG wurde ein Bericht über Chancen und Risiken im Unternehmen gesetzlich verankert. Umso erstaunlicher ist es, dass im Jahr 2005 lediglich 25 Prozent der Unternehmen angaben, auch Chancen im Risikomanagement implementiert zu haben. Auch die durchführende Wirtschaftsprüfungsgesellschaft PWC sieht hier deutlichen Verbesserungsbedarf. (Ernst & Young AG 2005, S. 9)

Möglicherweise wurden Chancen seitens der Organisationen im Lagebericht beziehungsweise im Jahresabschluss berichtet, allerdings wurden diese nicht aktiv und explizit in den Risikomanagementprozess eingebunden. Hierdurch werden die Anforderungen des KonTraG zwar erfüllt, allerdings können Chancen nur bedingt genutzt werden und somit auch nur bedingt zum Unternehmenserfolg beitragen. Da der Betrachtungszeitraum der Ereignisse erst zwei Jahre nach Veröffentlichung des KonTraG beginnt, erfolgt im Rahmen der vorliegenden Arbeit keine weitere Analyse zu einem möglichen Zusammenhang zwischen einem auslösenden Ereignis und dem KonTraG.

Ebenfalls im Jahr 2002 wurde in Deutschland das TransPuG, welches die Berichts- und Prüfpflichten gemäß KonTraG erweiterte, verabschiedet. In der Literatur werden dem TransPuG verschiedene vorangegangene deutsche Unternehmenskonkurse zugrunde gelegt. Unter anderem der Zusammenbruch der Philipp Holzmann AG. (Stephan 2006, S. 1) Hier ist also ein klarer Zusammenhang zwischen Ereignissen und der Gesetzesänderung gegeben. Das TransPuG wurde zur gleichen Zeit wie der SOX eingeführt. Somit besteht die Möglichkeit, dass hier neben den deutschen Unternehmenskrisen auch der Fall Enron und der Sarbanes-Oxley Act eine Rolle spielten. Im Rahmen des TransPuG sollen Unternehmensentscheidungen für Außenstehende transparent begründet werden und somit nachvollziehbar sein. Unter anderem muss der Vorstand in Zusammenarbeit mit dem Aufsichtsrat auch die Entsprechenserklärung zum DCGK abgeben. Da diese allerdings nicht im Rahmen des Jahresberichtes abgegeben werden muss und kein Bestandteil der analysierten Studien ist, kann hier kein direkter Vergleich angestellt werden. Aktuell sind Entsprechenserklärungen laut § 161 AktG allenfalls auf den Webseiten von deutschen Konzernen zu finden vgl. (vgl. BMW AG 2020; Hugo Boss AG 2020; vgl. Lufthansa Group 2020)

5.2.3 Entwicklung der Risikomanagementsysteme bis zur ISO 31000:2009

Im Jahr 2004 folgte auf die Verabschiedung des SOX die Veröffentlichung des Coso ERM Standards. In diesem Standard wurden die durch den Sarbanes-Oxley Act vorgeschriebenen Richtlinien berücksichtigt. Der COSO Standard soll allerdings nicht nur dazu dienen, den Organisationen ein Rahmenwerk zur Erfüllung gesetzlicher Vorgaben zu stellen, sondern insbesondere auch ein ganzheitliches Risikomanagement, welches auch zur Unternehmenssteuerung beiträgt, zu etablieren. Da der COSO Standard bei der Empfehlung zur Umsetzung eines Risikomanagementsystems insbesondere auf die Vorgaben des SOX eingeht, kann auch dieser indirekt auf Unternehmenskonkurse wie den Enron-Skandal zurückgeführt werden.

Eine Verbindung zwischen dem Standard und dem Trend zu einer Nutzung des Risikomanagements, welche über die reine Anforderung gesetzlicher Anforderungen hinausgeht,

kann insofern gezogen werden, dass mit Veröffentlichung des COSO Standards eine Unterstützung zur Umsetzung in Organisationen gegeben wurde. Zuvor wurden durch die Gesetze lediglich Vorgaben geschaffen. Wie genau und in welcher Form diese umzusetzen und zu implementieren sind, wurde nicht vorgegeben. Der COSO Standard hingegen stellt ein konkretes Modell zur Umsetzung des unternehmensweiten Risikomanagements zur Verfügung, welches auf die verschiedenen Bestandteile, Komponenten und Zielkategorien eines ganzheitlichen RMS eingeht. Auch wenn in Bezug auf ein ganzheitliches Risikomanagement gemäß verschiedenen Studien noch Potential besteht, kann ein positiver Trend beobachtet werden. 2005 gaben 49% der Unternehmen an, das RM auch im Rahmen einer werteorientierten Unternehmensführung zu nutzen. Hierzu sind insbesondere Schnittstellen zu verschiedenen Unternehmensbereichen nötig. Diese Schnittstellen wurden in der PWC Benchmarkstudie aus 2010 untersucht. Hier zeigt sich deutlich, dass bei einem Großteil der Organisationen Schnittstellen zwischen dem Risikomanagement und zumindest den relevantesten Unternehmensbereichen wie der operativen Planung und der Managementberichterstattung bestehen.

Der COSO Standard, als Grundlage zur Umsetzung eines über die gesetzlichen Vorgaben hinausgehenden Risikomanagements, kann durchaus in Zusammenhang mit dem positiven Trend hinsichtlich RM als Instrument zur werteorientierten Unternehmensführung und Implementierung von Schnittstellen zu anderen Unternehmensbereichen gesehen werden. Diese Annahme resultiert daraus, dass den Organisationen durch das detaillierte Rahmenmodell eine Unterstützung und zudem neue Ideen für das eigene Risikomanagementsystem gegeben wurden. Durch diese Hilfestellung, welche auch die gesetzlichen Anforderungen abdeckt, kann die Bereitschaft der Organisationen zu einem ganzheitlicheren Risikomanagement gesteigert werden.

Im gleichen Jahr wurde in Österreich die erste Fassung der ONR 49000 veröffentlicht. Diese Norm stellt später unter anderem die Basis für die international gültige ISO 31000 dar und ist die erste Norm, welche, zunächst für Österreich, einen Standard für den Aufbau eines Risikomanagementsystems bildet. Da in Österreich zu diesem Zeitpunkt noch keine expliziten Gesetzesänderungen hinsichtlich Risikomanagement stattfanden, kann hier ein Zusammenhang mit dem deutschen KonTraG hergestellt werden. (vgl. Integrierte Managementsysteme 2008)

Ebenfalls im Jahr 2004 folgte in Deutschland auf das TransPuG eine weitere Gesetzesänderung, das Bilanzrechtsreformgesetz. Im BilReG wird insbesondere nochmals auf die Einbeziehung von Chancen in das Risikomanagement und der dahingehenden Berichterstattung eingegangen. In der Ernst & Young Studie aus dem Jahr 2005 wird das BilReG explizit

dahingehend erwähnt, dass Unternehmen sich aufgrund dessen, in der Zukunft mehr mit Chancen auseinandersetzen müssen. (Ernst & Young AG 2005, S. 9)

Der in Abbildung 14 aufgezeigte durchwegs positive Trend zu Chancen im Risikomanagement bestätigt die Umsetzung dieser Gesetzesänderung durch die Unternehmen. Hier kann also ein deutlicher Zusammenhang zwischen BilReG und Umsetzungsstand des Chancenmanagements attestiert werden. Als Veranlassung zu dieser Gesetzesänderung wird kein konkretes Ereignis beschrieben, sondern eine Übernahme europäischer und internationaler Standards, speziell IFRS, in das deutsche Gesetz. (Pottgießer; Pottgießer 2006, S. 53–62)

Im Folgejahr 2005 erfolgte eine weitere geringfügige Anpassung der deutschen Gesetzgebung durch das UMAG. Da im Rahmen des TranPuG bereits Regelungen zur Offenlegung von Informationen bezüglich Unternehmensentscheidungen verabschiedet wurden, bringt die *Business Judgement Rule*, welche durch das UMAG verankert wurde, wenige bis keine nötigen Änderungen in der Umsetzung in Organisationen mit sich. Hinsichtlich Risikomanagement hat das UMAG also einen ergänzenden Charakter zum Transparenz- und Publizitätsgesetz.

Die 2005 in der Schweiz im Obligationenrecht eingeführte Gesetzesgrundlage für das Risikomanagement wird unter anderem mit dem Konkurs der Swissair im Jahr 2002 begründet. (KMU-Portal 2021) Ähnlich der Abläufe bei SOX und TransPuG, führten hier dieser und weitere kleinere Unternehmenskonkurse zur Einführung des Artikels, welcher eine Risikobeurteilung im Anhang des Jahresabschlusses fordert. Die erste analysierte Studie, welche Schweizer Unternehmen betrifft, stammt aus dem Jahr 2013. Hier war bei einem Großteil der Unternehmen bereits ein formaler Risikomanagementprozess vorzuweisen. (Boutellier et al. 2013, S. 3) Es ist davon auszugehen, dass die Änderung im Obligationenrecht bezüglich der Berichterstattung zur Risikosituation sowie die 2008 erfolgte Änderung im Aktienrecht zum IKS, auch in Zusammenhang mit dem hohen Anteil an Unternehmen mit formalem Risikomanagementprozess steht. Denn ohne einen zumindest formell begründeten Prozess zum Risikomanagement, ist auch keine Berichterstattung zur Risikosituation des Unternehmens möglich.

Im Jahr 2008 fanden in Österreich zwei Anpassungen der Gesetzgebung bzw. Standards statt.

Zum einen wurde die ONR 49000 überarbeitet. Dies resultiert aus der Erarbeitung des internationalen ISO Standards, welcher im Folgejahr veröffentlicht wurde. Im Rahmen der ONR Anpassung wurden die während der Erarbeitung der ISO gewonnenen Erfahrungen

integriert. Außerdem wurde ein entsprechendes Kapitel hinsichtlich Krisen- und Kontinuitätsmanagement ergänzt, welches dessen Integration in ein Risikomanagementsystem beschreibt. (vgl. Köcher 2009)

Die Änderung hinsichtlich der Integration des Krisenmanagements kann in Verbindung zur zu dieser Zeit beginnenden Finanzkrise gesetzt werden. Auch wenn das Ausmaß und die Folgen der Finanzkrise noch nicht bekannt waren, konnte durchaus eine Einordnung der erwarteten Schwere getroffen werden und somit die Notwendigkeit für Reglungen zum Krisenmanagement gesehen werden. Dies trifft auch auf die 2009 veröffentlichte Norm ISO 31000 zu. Nach den vorangegangenen Unternehmenskonkursen in ganz Europa sowie weltweit, wurde eine einheitliche, international gültige Norm dringend erforderlich.

Die zweite österreichische Änderung im Jahr 2008 stellt das URÄG dar. Auch für dieses Gesetz bildet die Grundlage wiederum der Sarbanes-Oxley Act. Durch das URÄG wurde auch in Österreich die Berichterstattung hinsichtlich der bedeutendsten Merkmale von IKS und RMS sowie deren Überwachung gesetzlich festgeschrieben. Zusätzlich wurde die Verpflichtung zur Erstellung eines Corporate Governance Berichts geschaffen. Die Studie aus dem österreichischen Handel (2014) sowie dem österreichischen Mittelstand (2014) zeigen, dass sich der Großteil der befragten Unternehmen aktiv mit Risikomanagement beschäftigt, dahingehend berichtet und somit auch die Anforderungen des UGB nach dem URÄG erfüllt.

2009 folgte in Deutschland das BilMoG. Das Gesetz, welches weitreichende Änderungen im Rechnungslegungsprozess mit sich brachte, basiert analog dem BilReG aus 2004 weitestgehend auf den Vorschriften des IFRS. Bezüglich Risikomanagement wurden hierbei die Überwachungsaufgaben für den Vorstand sowie die Prüfungspflichten konkretisiert. In der PWC Benchmarkstudie, welche im Jahr 2010 veröffentlicht wurde, wurden bei der Mehrheit der Unternehmen keine strategischen Risiken im Rahmen des Risikoberichts berichtet. Diese Dokumentation ist allerdings für die Sicherstellung der Prüfbarkeit und der vorgeschriebenen Überwachung nötig. Für die Überwachung seitens des Vorstandes ist eine entsprechende interne Berichterstattung an diesen notwendig, insbesondere Ad-hoc Berichte bei neuen Entwicklungen. Dies war bei knapp 10% der Unternehmen bei der 2010 veröffentlichten Befragung noch nicht gegeben.

Ein Jahr später wurde in der Mehrheit der Unternehmen die Risikomanagementberichterstattung angepasst. Dies resultiert vorrangig aus der Finanzkrise und den damit einhergehenden wirtschaftlichen Folgen. (Herre und Tüllner 2011, S. 13) Jedoch hatten im gleichen Jahr bzw. 2012 immer noch 8% der Organisationen keine Ad-Hoc Berichterstattung etabliert. (Herre et al. 2012, S. 34). In der gleichen Studie gaben allerdings auch knapp 60% an, dass eine Überarbeitung des RM noch notwendig sei. Konkret sagt diese Studie allerdings

auch aus, dass die durch das BilMoG vorgeschriebenen Richtlinien bis zum Zeitpunkt der Befragung nur *„vereinzelt zu einer Überarbeitung des Risikomanagements geführt“* haben. (Herre et al. 2012, S. 43)

Erwartungsgemäß wäre ein weiterer Effekt der Finanz- und Weltwirtschaftskrise, dass Risikoaggregation und Korrelation im Rahmen des unternehmerischen Risikomanagementprozesses stärker fokussiert werden. Hierzu existieren allerdings keine konkreten gesetzlichen Vorgaben. Erstaunlicherweise ist die Berücksichtigung von Korrelationen, welche im Jahr 2005 noch bei 50% der Unternehmen stattfand, nach der Wirtschaftskrise stark gesunken, sodass dies 2012 nur noch auf knapp ein Viertel der Unternehmen zutraf. Ein anderes Bild zeigt sich bei der Risikoaggregation, was darauf schließen lässt, dass die Analyse und Abbildung einer Gesamtrisikosituation nach der Krise höher priorisiert wurde. Dies ist insofern nicht verwunderlich, da für die gesetzlich geforderte umfassende Darstellung der Risikosituation eine Gesamtrisikobelastung von entscheidendem Vorteil ist. Die fehlende erwartete Steigerung bei Berücksichtigung von Risikokorrelationen kann auf fehlende gesetzliche Vorgaben zu dieser Thematik zurückgeführt werden.

Auffällig im, in diesem Kapitel betrachteten Zeitraum ist unter anderem die Häufung von gesetzlichen Änderungen in den Jahren 2004 sowie 2008/2009.

Die Konzentration im Jahr 2004 lässt sich unter anderem darauf zurückführen, dass zwei Jahre zuvor mit dem Sarbanes-Oxley Act eine entscheidende Basis für ein neues unternehmensweites Risikomanagement geschaffen wurde, welche auch eine Anpassung nationaler Gesetze erforderte. Durch die ONR 49000 sowie den COSO Standard wurde den Unternehmen Rahmenbedingungen und somit eine Unterstützung zu einer konkreten Umsetzung des ERM basierend unter anderem auf den Vorgaben des SOX.

Hier wird bereits deutlich, dass der Sarbanes-Oxley Act eine entscheidende Rolle im Risikomanagement einnimmt. Sowohl in internationaler sowie lokalen Gesetzgebungen als auch in den Standards zur Umsetzung in Organisationen.

Eine noch stärkere Konzentration ist in den Jahren 2008 und 2009 zu beobachten. Hier fanden jeweils in allen drei Ländern der DACH Region sowie auch international zumindest eine gesetzliche bzw. quasi-gesetzliche Änderung statt. Hier zeigt sich ein Zusammenhang mit der Finanzkrise, welche bereits im Jahr 2007 begonnen hat und im Jahr 2008 mit dem Zusammenbruch der Investmentbank Lehman Brothers ihren Höhepunkt nahm. Auch wenn zu diesem Zeitpunkt die genauen Ursachen noch nicht aufgearbeitet und die langfristigen Folgen noch nicht abschätzbar waren, herrschte dennoch Klarheit darüber, dass ein Kurswechsel beziehungsweise Konkretisierungen in Sachen Risikomanagement erforderlich

waren. Zudem wurden auch in 2008 noch in Österreich (URÄG) sowie in der Schweiz (Änderung im Aktienrecht) Änderungen basierend auf dem SOX verabschiedet.

5.2.4 Risikomanagementsysteme nach der Finanzkrise bis zur aktuellen Coronapandemie

In den Jahren zwischen 2009 und 2013 fanden keine in der vorliegenden Arbeit betrachteten Änderungen statt.

Nach der Erneuerung im Jahr 2008 sowie der ISO 31000 im Jahr 2009 folgte eine Überarbeitung der ONR49000 im Jahr 2014. Diese stellt nach wie vor eine Empfehlung zur Umsetzung der internationalen Norm ISO 31000 dar. Die Begriffsdefinitionen wurden in dieser Neufassung allerdings breiter gefasst, als dies zuvor der Fall war. Auch die Anforderungen an den/die *„RisikomanagerIn“,* also die Person mit der Verantwortlichkeit für das Risikomanagement und dessen Umsetzung im Unternehmen, wurden angepasst. Insbesondere soll mit dieser Änderung das Risikomanagement besser in die Führung des Unternehmens integriert werden. (vgl. Heynen und Wartenweiler 2014)

Nach der endgültigen Veröffentlichung der ISO 31000 in 2009 sowie der Finanzkrise und europäischen Schuldenkrise stellt diese offenere Definition von Risiko und anderen Begriffen sowie der Schritt zur engeren Verknüpfung von Unternehmensführung und Risikomanagement eine logische Folge dar. Im Umsetzungsstand spiegelt sich diese engere Verknüpfung ebenfalls wieder. Im Jahr 2015 hatten bereits 97% der befragten Organisationen eine eigene Rolle für das Risikomanagement eingerichtet. Ebenso hatten in diesem Jahr 40% auch eine spezielle Risikomanagementabteilung etabliert. In beiden Bereichen stellen diese Anteile eine Steigerung zum zuvor beobachteten Wert dar.

Im Jahr 2013 erfolgte die Anpassung im Schweizer Obligationenrecht. Durch diese musste die Risikoberichterstattung bei großen Unternehmen spätestens ab dem Jahr 2015 Teil des Lageberichts sein, anstatt wie zuvor des Anhangs. Dies kann als Aufwertung der Risikoberichterstattung verstanden werden. Während die Angaben zuvor lediglich im Anhang aufzuführen waren, sind diese nun elementarer Bestandteil des Lageberichtes. Dies ist positiv zu bewerten, da der Lagebericht eine umfassende Darstellung der aktuellen Unternehmenssituation geben soll. Hierfür ist die Risikosituation sowie das Risikomanagement von essentieller Bedeutung, da Risikoexposition und Umgang mit Risiken einen wesentlichen Teil der Gesamtsituation des Unternehmens ausmachen.

Allerdings wird der Kreis der Unternehmen, welche das Risikomanagementsystem im Lagebericht anführen müssen, auch eingeschränkt. Wohingegen zuvor keine Einschränkung des Unternehmenskreises stattfand, da der Risikobericht im Anhang enthalten war, gilt dies

nun nur noch für Unternehmen, „*die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind",* da nur diese gem. Art. 961 OR zur Erstellung eines Jahresberichtes verpflichtet sind. Insbesondere sind dies große Unternehmen und Konzerne, KMUs sind hiervon weniger betroffen. (vgl. Bitterli und Fallegger 2018, S. 118)

Einerseits entlastet diese Änderung KMUs, da kein Bericht mehr über die Risikosituation erstellt werden muss. Andererseits bedeutet die angepasste Berichterstattung keinesfalls, dass KMUs weniger von Risiken und deren Auswirkungen betroffen sind. Daher sollten auch KMUs eine Risikobewertung vornehmen, ungeachtet dessen, ob eine Verpflichtung zur diesbezüglichen Berichterstattung besteht. Dass Schweizer Unternehmen auch neben der gesetzlichen Verpflichtung Risikomanagement betreiben, zeigt sich durch den Umsetzungsstand im Jahr 2013. Hier war die Erfüllung der gesetzlichen Verpflichtung nicht der Hauptgrund für Schweizer Unternehmen Risikomanagement zu betreiben, sondern lag lediglich auf Platz drei. Viel mehr wird hier als Top Argument zur Umsetzung eines Risikomanagementprozesses die Früherkennung und damit einhergehende bessere Kontrolle von Risiken angegeben. (Boutellier et al. 2013, S. 6) Dies zeigt, dass sich Schweizer Unternehmen verschiedener Größenordnungen trotz weniger gesetzlicher Vorgaben, ihrer Verantwortung im Thema Risikomanagement durchaus bewusst sind und diese auch umsetzen.

Im Jahr 2017 fand eine Anpassung des COSO ERM Standards statt. Die Neufassung beinhaltet ein angepasstes, noch umfassenderes Modell zum unternehmerischen Risikomanagementsystem. Zudem sind die einzelnen Bestandteile detaillierter beschrieben. Auch hier wird der Fokus ähnlich der ONR 49000ff von 2014 stärker auf die Zusammenarbeit von Risikomanagement und Unternehmensführung und Unternehmenskultur gerichtet. Der Trend zu Risikokultur und Risikostrategie gestaltet sich, insbesondere in österreichischen Unternehmen, positiv. Während in Deutschland im Jahr 2012 weniger als ein Drittel der Unternehmen eine anwendbare Risikostrategie hatten, waren dies im Jahr 2014 in Österreich bereits knapp zwei Drittel. Dies kann über die frühere Einführung der ONR 49000ff in Österreich erklärt werden. Hier gab es bereits deutlich früher einen Standard, welcher die Verknüpfung von Risikomanagement zu anderen Unternehmensbereichen, vorrangig der Unternehmensführung, empfiehlt. Durch den internationalen neuen COSO Standard wird dies nun auch auf die übrigen Länder übertragen. Im Jahr der Veröffentlichung war die Risikostrategie und -kultur bei zwei Drittel der deutschen Unternehmen nach eigenen Angaben noch ausbaufähig. Dies impliziert allerdings auch, dass zumindest eine Risikokultur im Unternehmen vorhanden ist.

Auch beim Thema Risikokultur und Risikostrategie bestätigt sich der zuvor beschriebene Eindruck des hohen Verantwortungsbewusstseins in Schweizer Unternehmen. Hier waren

es 2017 etwa bereits 90% der Organisationen, welche eine positive Risikokultur zumindest teilweise verankert hatten.

Es zeigt sich diesbezüglich ein Aufholbedarf bei deutschen Unternehmen. In Deutschland wurde, ebenfalls im Jahr 2017, der Prüfungsstandard IDW PS 981 veröffentlicht. Hierin sind neben den Prüfungsanforderungen für Risikomanagementsysteme auch die Grundelemente dieser. Das Wirtschaftsprüfungsunternehmen Deloitte befragt 2017 deutsche Unternehmen zum Umsetzungsstand des Risikomanagementsystems hinsichtlich der Bestandteile laut dem IDW PS 981. Diese Studie bestätigt, dass hier noch Optimierungspotential besteht. Zu diesem Zeitpunkt planten knapp 40 Prozent der Unternehmen bereits eine Überarbeitung des eigenen Risikomanagementsystems gemäß dem neuen Prüfungsstandard im folgenden Jahr. Dies zeigt, dass diesem Prüfungsstandard trotz seines freiwilligen Charakters eine hohe Bedeutung beigemessen wird, aber auch, dass die Risikomanagementsysteme noch nicht ausgereift sind. Der größte Handlungsbedarf wurde hierbei wiederum bei der Risikokultur gesehen, was zeigt, dass auch die Unternehmen selbst hier den größten Aufholbedarf sehen. Erfreulicherweise zeigt sich in der Nachfolgestudie aus 2020, dass sich der Anteil der Unternehmen mit Handlungsbedarf in diesem Feld deutlich verringert hat. Auch im Allgemeinen sehen die Unternehmen in 2020 im Vergleich zu 2017 deutlich weniger Handlungsbedarf in den verschiedenen Elementen des Risikomanagements. Ein Zusammenhang zwischen dem verbesserten Umsetzungsstand in 2020 und dem IDW PS 981 ist somit gegeben.

Im IDW PS 981 wird ein starker Zusammenhang zwischen Unternehmenszielen und Zielen des Risikomanagements hergestellt. Dies impliziert, dass Unternehmen ihr Risikomanagementsystem noch stärker mit der Unternehmensführung verknüpfen müssen. Im Vergleich zwischen 2017 und 2020 wird somit eine Steigerung des Anteils an Unternehmen, welche ihr RMS zur aktiven Unternehmensführung und -steuerung einsetzen, erwartet. Erstaunlicherweise zeigt ein Vergleich der Studien ein anderes Bild. Der Anteil der Unternehmen, welche das RMS als aktives Steuerungsinstrument zum Erreichen der Unternehmensziele sehen, verringerte sich um 16 Prozentpunkte. Hier ist eine engere Verzahnung des RMS mit den übrigen Unternehmensbereichen, insbesondere der strategischen Planung und auch der Unternehmensführung selbst notwendig. (Deloitte 2017, 2020; IDW PS 981)

2018 wurde die Neufassung der ISO 31000 veröffentlicht. Die Neuerungen lassen sich insbesondere mit dem COSO Standard 2017 verknüpfen. Auch in der Neufassung der ISO wird das Risikomanagement nun als Prozessmodell beschrieben. Auch die in der Praxis bereits gelebte Tatsache, dass Risikomanagement im Top-Management eines Unternehmens angesiedelt sein sollte, wird in der ISO 31000 festgehalten. Sowohl vorhergehende

als auch folgende Studien bestätigen, dass dieser Grundsatz bereits zur Unternehmenspraxis gehört und auch zukünftig erhalten bleibt.

Im Jahr 2020 wurde eine Neufassung des IDW Prüfungsstandards 340 veröffentlicht. Die bis dorthin gültige Version stammte aus dem Jahr 1999, was die aktuelle Überarbeitung aufgrund der diversen Gesetzesänderungen seit 1999 dringend notwendig machte. Im Gegensatz zum IDW PS 981 besitzt der Prüfungsstandard 340 und dessen Neufassung keinen freiwilligen Charakter und ist somit von Unternehmen verpflichtend anzuwenden. Insbesondere werden in der Neufassung die Elemente eines Risikofrüherkennungssystems gemäß § 92 Abs 2 AktG beschrieben sowie Pflichten zur Risikoaggregation und der Risikotragfähigkeit des Unternehmens erläutert. Im Jahr 2020 wurde zwar von einem Großteil der Unternehmen eine Risikoaggregation vorgenommen, allerdings beinhaltet dies in den meisten Fällen lediglich eine Addition der Einzelrisiken oder eine rein qualitative Bewertung der Gesamtsituation. Eine aussagekräftige Aggregation muss allerdings auch Korrelationen zwischen den Einzelrisiken beinhalten. Dieser bereits zuvor als ausbaufähig beschriebener Punkt wird erfreulicherweise im IDW PD 340 n.F. unter Ziffer 11 aufgenommen. Hier wird die notwendige Aggregation mit dem *„Zusammenwirken mehrerer Risiken“* beschrieben, *„die bei isolierter Betrachtung an sich nicht bestandsgefährdend sind.“* (IDW EPS 340 n.F.)

Diese Neufassung lässt sich neben den diversen Gesetzes- und Standardüberarbeitungen sicherlich auch auf die Erkenntnisse der Finanzkrise zurückführen. Der lange Zeitraum zwischen der ursprünglichen Ausgabe und der Neufassung von 21 Jahren ist einerseits als zu lang zu beurteilen, da innerhalb dieser Zeitspanne diverse Ereignisse zu Änderungen der Rahmenbedingungen führten. Andererseits stellt das in der ursprünglichen Fassung berücksichtigte KonTraG nach wie vor die Basis der Risikomanagementgesetzgebung dar und durch die späte Überarbeitung konnten zahlreiche neue Standards und Gesetze bereits in die Neufassung einfließen. Allerdings ereigneten sich im Jahr 2020 mit der Corona Pandemie und dem Wirecard Skandal gleich zwei weitere Ereignisse, welche mit Sicherheit weitere Änderungen in den gesetzlichen und anderen Rahmenbedingungen zum Risikomanagement nach sich ziehen werden.

Erwähnenswert ist hierbei auch, dass die die verschiedenen Standards keinesfalls widersprechen, sondern viel mehr aufeinander aufbauen. Somit kann sichergestellt werden, dass Unternehmen, insbesondere Konzerne mit Unternehmenssitzen in verschiedenen Ländern mit unterschiedlicher Gesetzgebung, ein Risikomanagementsystem sowie eine dazugehörige Berichterstattung implementieren können, welche den unterschiedlichen Gesetzen und Standards gleichzeitig entspricht.

Die letzte in der vorliegenden Arbeit betrachtete Gesetzesanpassung bildet das deutsche StaRuG aus dem aktuellen Jahr 2021. Dieses Gesetz lässt sich, wenn auch nicht ausschließlich, direkt mit der noch andauernden Coronapandemie in Zusammenhang bringen. Wie sich dieses Gesetz allerdings auf den Umsetzungsstand der Risikomanagementsysteme in den Organisationen auswirkt, kann aufgrund der noch nicht vorliegenden Informationen nicht bewertet und diskutiert werden.

5.3 Allgemeine Implikationen zum Zusammenhang von Ereignissen, (quasi-) gesetzlichen Änderungen und Umsetzungsstand

Allgemein kann ein Zusammenhang zwischen den definierten Ereignissen, den gesetzlichen beziehungsweise sonstigen Änderungen sowie dem praktischen Umsetzungsstand in den Unternehmen bestätigt werden. Dieser Beziehung lässt sich in eine zeitliche sowie eine inhaltliche Komponente gliedern.

Zeitlich wird, wie in Abbildung 20 visualisiert, kein eindeutiger einzelner Zusammenhang sichtbar. Hier kann jedoch die Konzentration der (quasi-) gesetzlichen Änderungen um die Jahre 2004, 2008 sowie 2017 beobachtet werden. Zudem sind die fehlenden beziehungsweise nur sehr geringen Änderungen zwischen 2009 und 2017 erwähnenswert. Insbesondere nach Beginn der Finanzkrise und der darauf in Europa folgenden Schuldenkrise Griechenland brechen die Anpassungen für einen längeren Zeitraum ab.

Gewisse gesetzliche und quasi-gesetzliche Änderungen können direkt auf ein spezielles Ereignis zurückgeführt werden, wie beispielsweise der Sarbanes-Oxley Act auf den Enron-Bilanzskandal oder die Änderung im Schweizer Obligationenrecht auf den Konkurs der Swissair. Andere Änderungen können wiederum indirekt ebenfalls auf diese Ereignisse zurückgeführt werden. Diese stellen lokale Reaktionen auf internationale Gesetzgebungen und Standards dar, welche wiederum auf ein Ereignis zurückgeführt werden können.

Generell können der Bilanzskandal des Enron Konzerns sowie der darauffolgende Sarbanes-Oxley Act als Grundlage für diverse Gesetzgebungen und Anpassungen angegeben werden. Dies betrifft unter anderem das URÄG 2008 in Österreich, sowie der COSO ERM Standard aus 2004. Der Sarbanes-Oxley Act und damit auch der Fall Enron können als Basis für das Risikomanagement ab 2002 bezeichnet werden.

Einige der analysierten Änderungen können zwar nicht namentlich auf ein bestimmtes Ereignis zurückgeführt werden, allerdings können die Inhalte der neuen Gesetze und Standards in Verbindung zu den aus den Folgen des Ereignisses gewonnenen Erkenntnissen gebracht werden. Hier ist insbesondere die Finanzkrise mit ihren Auswirkungen zu nennen.

Auch der Umsetzungsstand in den Unternehmen wird im Allgemeinen jeweils auf die vorangegangenen gesetzlichen Änderungen angepasst, sodass das jeweilige Risikomanagementsystem den geltenden regulatorischen Anforderungen entspricht, was positiv zu bewerten ist. Teilweise werden neue Regulatorien als direkter Grund für eine Überarbeitung des RMS angegeben. Allerdings wäre zu erwarten gewesen, dass Organisationen ihr Risikomanagement weitaus mehr auch aufgrund vorangegangener Ereignisse anpassen, um sich auch außerhalb der gesetzlichen Rahmenbedingungen weiter abzusichern und dem Risikomanagement einen vorausschauenden anstatt einen vergangenheitsbezogenen Charakter zu verleihen.

Insbesondere bei der Risikopriorisierung zeigt sich hierbei deutlicher Aufholbedarf. Insbesondere zu erwähnen sind hierbei die Risiken „Terrorismus“ sowie „Pandemie/Gesundheitskrise“. Auch nach vorangegangenen Ereignissen, wie dem Terroranschlag auf das World Trade Center am 11. September 2001 und dessen wirtschaftlicher Folgen, hätten terroristische Bedrohungen im unternehmerischen Risikomanagement stärker eingebunden werden müssen. Auch, da dieses Risiko Wechselwirkung zu anderen Risiken auslösen kann. Auch das Risiko einer gesundheitlichen Krise wurde in der Vergangenheit nicht ausreichend betrachtet und damit unterschätzt, wie die derzeitige Coronapandemie deutlich zeigt. Im Betrachtungszeitraum existieren verschiedene Gesundheitskrisen wie beispielsweise der Ebola-Ausbruch in 2014 oder die bereits als Pandemie klassifizierte Schweinegrippe in 2009. Dennoch existierte weitreichend dahingehend kein ausreichendes Risikomanagement, wodurch die Coronapandemie viele Organisationen unvorbereitet traf.

Durch eine verbesserte Priorisierung und Identifizierung von Risiken sowie Betrachtung von Wechselwirkungen zwischen den Einzelrisiken, können Organisationen ihr Risikomanagementsystem noch weiter ausbauen und sich damit besser gegen externe Einflüsse absichern. Die Berücksichtigung von Wechselwirkungen ermöglicht auch eine quantitative Gesamtrisikoaggregation.

Speziell die aktuelle Coronapandemie wird zukünftig Auswirkungen auf das Risikomanagement haben. Dies betrifft sowohl die Gesetzgebung als auch die Anwendung und Umsetzung der Unternehmen. Wie anhand der Finanzkrise, nach welcher es einige Jahre keine Anpassungen gab, erkennbar ist, wird auch eine entsprechende Anpassung aufgrund der Coronapandemie vermutlich erst mittelfristig erfolgen. Hintergrund ist, dass die wirtschaftlichen und sonstigen Folgen analog der Finanzkrise, zunächst abgewartet und anschließend aufgearbeitet werden müssen. Diesbezüglich ist auch noch unklar, ob hier zunächst lokale Gesetzgebungen oder ein international gültiger Standard veröffentlicht werden wird.

Die Analyse des Umsetzungsstandes im Betrachtungszeitraum zeigt, dass Unternehmen neben anderen Zielen des Risikomanagements stets bestrebt sind, die aktuellen regulatorischen Anforderungen zu erfüllen. Daher empfiehlt es sich, die Berücksichtigung von Wechselwirkungen zwischen Einzelrisiken sowie einen verpflichtenden Umfang an bestimmten Risiken in die Regulatorien aufzunehmen. So kann in weiterer Folge auch die Qualität der Gesamtrisikosituation beziehungsweise der Aggregation verbessert werden.

Auch wenn die Mehrheit der Organisationen das Risikomanagement derzeit bereits über die gesetzlichen Regelungen hinaus auslegt und beispielsweise zur aktiven Unternehmenssteuerung einsetzt, gilt es, die Schnittstellen zwischen Risikomanagement und den übrigen Abteilungen und Bereichen des Unternehmens noch auszubauen. Denn nur durch Zusammenarbeit kann ein umfassendes Risikomanagementsystem gewährleistet werden.

Eine zusätzliche Empfehlung für Organisationen stellt die weitere Forcierung einer eigenen Abteilung für das Risikomanagement dar. Während eine spezielle Rolle mit der Verantwortlichkeit für das Risikomanagement längst zum Unternehmensalltag gehört, besitzen viele Unternehmen noch keine eigene Abteilung. Da das Risikomanagement mit seinen regulatorischen aber auch internen Anforderungen stets komplexer wird, empfiehlt es sich durchaus eine zentrale Abteilung zur Umsetzung und Planung des strategischen Risikomanagements zu etablieren. Die operative Umsetzung muss allerdings in den einzelnen Fachabteilungen verbleiben, da diese jeweils Experten auf ihrem Gebiet sind.

Zusammenfassend wird empfohlen, dass Unternehmen in Sachen Risikomanagement nicht nur direkt auf Änderungen von gesetzlichen und quasi-gesetzlichen Anforderungen reagieren, sondern auch externe Ereignisse und deren wirtschaftliche Folgen direkt in das Risikomanagement einbeziehen sollten. So können Risikomanagementsysteme schneller angepasst werden und damit eine verbesserte Position des Unternehmens in sowie außerhalb von Krisensituationen ermöglicht werden. Durch agile und dynamische Risikomanagementsysteme, welche sich nicht nur an (quasi-) gesetzlichen Anforderungen orientieren, kann somit ein deutlicher Mehrwert für das jeweilige Unternehmen geschaffen werden.

6. Fazit zu Veränderung von Risikomanagementsystemen in der Vergangenheit sowie Ausblick für die Zukunft

In diesem abschließenden Kapitel erfolgt eine Zusammenfassung sowie ein Fazit zu den untersuchten Änderungen. Zudem werden die Limitationen dieser Arbeit sowie ein Ausblick auf mögliche zukünftige Entwicklungen gegeben.

6.1 Fazit zu Veränderungen im Risikomanagement und deren Ursachen

Ziel der vorliegenden Masterarbeit war es, somit einen Zusammenhang zwischen definierten Ereignissen mit Relevanz für das Risikomanagement, gesetzlichen und quasigesetzlichen Änderungen zum Risikomanagement sowie dessen Umsetzungsstand in Unternehmen der DACH Region nachzuweisen und dessen Qualität und Tiefe zu untersuchen.

Zunächst wurden hierfür für das Risikomanagement relevante Ereignisse, definiert und hinsichtlich Ursachen, Auslösern und Folgen erörtert. Anschließend folgte eine systematische Analyse von gesetzlichen und quasi gesetzlichen Änderungen in Deutschland, Österreich und der Schweiz sowie ausgewählter relevanter internationaler Gesetze und Standards. Diese Änderungen wurden danach in einen zeitlichen Zusammenhang zu den definierten Ereignissen gesetzt. Anschließend wurden die dadurch bedingten Weiterentwicklungen im Risikomanagement sowie in Risikomanagementsystemen anhand einer Metastudie untersucht.

Die Fragestellungen der Forschungsfrage konnte mithilfe der beschriebenen Untersuchungen beantwortet werden.

Durch die durchgeführte Analyse der Änderungen in Gesetzen und sonstigen Standards beginnend mit dem KonTraG im Jahr 1998, wurden diese zunächst in Verbindung zu den zuvor definierten relevanten Ereignissen gesetzt. Anschließend wurde durch die durchgeführte Metastudie der Umsetzungsstand des Risikomanagements in Unternehmen untersucht. Die Erkenntnisse aus dieser Metastudie wurden wiederum in Zusammenhang zu den analysierten Änderungen und im letzten Schritt auch zu den definierten Ereignissen gesetzt.

Durch die durchgeführten Untersuchungen konnte ein Zusammenhang zwischen Ereignissen, Gesetzesänderung und sonstigen Standards sowie dem Umsetzungsstand in Unternehmen nachgewiesen werden. Insbesondere zwischen einzelnen Ereignissen und Gesetzen bestehen direkte Verbindungen.

Weiter hat die Analyse verdeutlicht, dass ebenfalls enge Zusammenhänge zwischen den unterschiedlichen Gesetzgebungen und Standards bestehen. Diese bauen aufeinander auf und stellen teilweise auch Reaktionen aufeinander dar.

Mit den Verbindungen zwischen den einzelnen Gesetzgebungen konnten auch indirekte Verbindungen zwischen Änderungen der Anforderungen und Ereignissen hergestellt werden.

Generell zeigt sich, dass einzelne spezielle Ereignisse deutlich mehr Einfluss auf die gesetzlichen Änderungen haben, als andere. Ebenso treten aber aufgrund von bestimmten Ereignissen erwartete Änderungen nicht ein.

Es ergeben sich im Betrachtungszeitraum zahlreiche Weiterentwicklungen im Organisationsaufbau des Risikomanagements sowie dessen strategischer und operativer Komponenten.

Der praktische Umsetzungsstand in Organisationen hängt stark mit den Veränderungen in den verschiedenen regulatorischen Anforderungen zum Risikomanagement zusammen. Hierbei konnten neben starken Verknüpfungen zwischen den jeweils lokalen Gesetzgebungen zur Unternehmenspraxis auch Beziehungen zu international gültigen Standards nachgewiesen werden. Weiters ergab die Metastudie auch, dass jeweils die Mehrheit der Unternehmen, die zum jeweiligen Zeitpunkt gültigen gesetzlichen und sonstigen regulatorischen Anforderungen umsetzen und erfüllen.

Die Ergebnisse der vorliegenden Masterarbeit stellen einen Gesamtzusammenhang hinsichtlich Risikomanagement über allgemeine Literatur, reale Ereignisse, (quasi-) gesetzliche Anpassungen bis hin zur praktischen Umsetzung im Unternehmen her.

6.2 Limitationen

Die Limitationen der vorliegenden Masterarbeit liegen im Ausschluss des Finanz- und Versicherungssektors und deren spezifischen Regulationen, dem Betrachtungszeitraum, der Auswahl der analysierten Gesetzesänderungen und Standards sowie der teils unterschiedlichen Fragestellungen in den analysierten Studien.

Aufgrund der sehr spezifischen Vorgaben hinsichtlich Risikomanagement für Unternehmen der Versicherungs- und Finanzbranche wurden sowohl die (quasi-) gesetzlichen Anforderungen als auch die Unternehmen selbst aus dieser Masterarbeit ausgeschlossen. Die Ergebnisse sind somit für diese beiden Branchen nicht repräsentativ.

Eine weitere Limitation stellt der Betrachtungszeitraum dar. Im Falle der Ereignisse beginnt dieser im Jahr 2000, bei den gesetzlichen Änderungen 1998. Es besteht die Möglichkeit,

dass sich auch vor Beginn dieses Betrachtungszeitraumes relevante Ereignisse ereignet haben, welche Einfluss auf Änderungen der regulatorischen Anforderungen, insbesondere zu Beginn des in dieser Arbeit definierten Betrachtungszeitraumes haben.

Die analysierten Änderungen wurden aufgrund des Umfangs und der Vielzahl auf die für den vorliegenden Fall relevanten Gesetzgebungen und Standards beschränkt. Hier existieren neben den erwähnten, noch weitere Gesetze und Standards, welche nicht Teil der vorliegenden Arbeit sind.

In den Studien, welche im Rahmen der Metastudie analysiert wurden, unterscheiden sich teilweise Details der Fragestellungen, sodass ein direkter Vergleich nur bedingt repräsentativ ist. Dies basiert insbesondere auf den verschiedenen herausgebenden Unternehmen und Auftraggebern.

Auch die zur Studienauswertung herangezogenen Kriterien sind erweiterbar. In dieser Arbeit wurden jene Auswertungskriterien herangezogen, welche abgeleitet aus den vorhergehenden Analysen, spezielle Relevanz besitzen.

6.3 Ausblick auf zukünftige Forschung insbesondere mit Bezug auf Covid-19

Basierend auf den zuvor beschriebenen Limitationen, bestehen noch weitere Felder für zukünftige Forschung auf diesem Gebiet.

Unter anderem könnte in weiterführender Forschung der Finanz- und Versicherungssektor analog dem Vorgehen in dieser Masterarbeit analysiert werden, um die Ergebnisse anschließend zu vergleichen.

Im Hinblick auf die hier definierten Gesetzgebungen und Standards erscheint es sinnvoll, in der Zukunft weitere noch nicht herangezogene Gesetze und Standards analog zu analysieren und diese ebenfalls in Zusammenhang mit Ereignissen und Umsetzungsstand zu bringen. Dies stellt eine Ergänzung der vorliegenden Analyse dar.

Weiter können innerhalb zukünftiger Forschung die definierten Kriterien zur Analyse des Umsetzungsstandes für Folgestudien verwendet werden. Diese können zur Auswertung zukünftig erstellter Studien, insbesondere auch für Studien zur Auswirkung der Coronapandemie auf den Risikomanagement-Umsetzungsstand, herangezogen werden. So kann auch eine Vergleichbarkeit zu den Ergebnissen der vorliegenden Arbeit hergestellt werden.

Die Coronapandemie stellt derzeit Unternehmen aber auch Gesetzgeber und Institutionen vor zahlreiche Herausforderungen hinsichtlich des Risikomanagements. Die Folgen und Auswirkungen der aktuellen Gesundheitskrise sind noch nicht abschätzbar und es können

lediglich Annahmen getroffen werden. Im Hinblick auf Forschung zur Veränderung des Risikomanagements bedeutet dies, dass es noch einige Zeit dauern kann, bis es tatsächlich zu weitreichenden Gesetzesänderungen und angepassten bzw. neuen Standards kommt. Folglich werden auch darauf basierenden Weiterentwicklungen der praktischen Umsetzung in Organisationen erst zu einem späteren Zeitpunkt erfolgen.

Literaturverzeichnis

3GRC (2018): Risikomanagement: Gesetzliche Regelungen in Europa und den USA. Online verfügbar unter https://www.corporate-governance-solutions.de/risikomanagement/risikomanagement-gesetzliche-regelungen-in-europa-und-den-usa/, zuletzt aktualisiert am 14.02.2018, zuletzt geprüft am 25.06.2021.

Agridopoulos, Aristotelis; Papagiannopoulos, Ilias (Hg.) (2016): Griechenland im europäischen Kontext. Krise und Krisendiskurse. 1. Aufl. 2016. Wiesbaden: Springer Fachmedien Wiesbaden (Staat - Souveränität - Nation).

Allianz SE and Allianz Global Corporate & Specialty SE (2015): Allianz Risk Barometer. Top Business Risks 2015. München.

AON (2019): Global Risk Management Survey 2019.

AON (2021): Reprioritizing Risk and Resilience for a Post-COVID-19 Future. Online verfügbar unter https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48136/covid-19_risk_management__insurance_survey_v7.55f9f69bd6f0.pdf, zuletzt geprüft am 25.06.2021.

AssCompact (2021): Aon-Umfrage: Wegen Corona müssen neue Risikomanagement-Strategien entwickelt werden. Online verfügbar unter https://www.asscompact.at/nachrichten/aon-umfrage-wegen-corona-m%C3%BCssen-neue-risikomanagement-strategien-entwickelt-werden, zuletzt aktualisiert am 11.03.2021, zuletzt geprüft am 25.06.2021.

Backes, Matthias (2019): Finanzwirtschaftliches Risikomanagement als Grundlage der Bestimmung der ökonomischen Substanz. In: Matthias Backes (Hg.): Grundsätze ordnungsmäßiger Sicherungsbilanzierung nach IFRS und HGB. Wiesbaden: Springer Fachmedien Wiesbaden, S. 29–47.

Biel, Alfred (2005): Der Sarbanes-Oxley Act (SOA) — Eine Controllerperspektive. In: *Z Control Manag* 49 (1), S. 15–18. DOI: 10.1007/BF03254982.

Bitterli, Christian; Fallegger, Marcel (2018): Risikoberichterstattung bei börsenkotierten Schweizer Unternehmen. In: Stefan Hunziker und Jens O. Meissner (Hg.): Ganzheitliches Chancen- und Risikomanagement. Wiesbaden: Springer Fachmedien Wiesbaden, S. 113–138.

BMW AG (2020): Erklärung des Vorstands und des Aufsichtsrats der Bayerische Motoren Werke Aktiengesellschaft zu den Empfehlungen der „Regierungskommission Deutscher Corpora. Online verfügbar unter https://www.bmwgroup.com/content/dam/grpw/websites/bmwgroup_com/company/downloads/de/2020/Entsprechenserklaerung_Dezember%202020.pdf, zuletzt geprüft am 25.06.2021.

Boecker, Corinna; Zwirner, Christian (2020): Corona-Krise. Risikomanagement in Zeiten der Corona-Pandemie. Hg. v. Dr. Kleeberg & Partner GmbH. München. Online verfügbar unter https://www.boersenverein.de/fileadmin/bundesverband/dokumente/beratung_service/Corona/Kleeberg_Kurzinformation_Corona_Virus_Risikomanagement_boev.pdf, zuletzt geprüft am 25.06.2021.

Boutellier, Roman; Montagne, Eric; Norell, Erik; Thomik, Marta (2013): Risikomanagement in Schweizer Organisationen. Eine Studie zum Reifegrad von Risikomanagement im privaten Sektor und bei der öffentlichen Hand. Hg. v. i-Risk GmbH und ETH Zürich.

Braumann, Evelyn; Klein, Aleksandra; Posch, Arthur (2020): Risikomanagement und Digitalisierung in Zeiten von Covid-19. Online verfügbar unter https://insights.controller-institut.at/wp-content/uploads/2021/01/Studie_Risk_ErsteErgebnisse.pdf, zuletzt geprüft am 25.06.2021.

Brauweiler (2019): Risikomanagement in Unternehmen: Springer Fachmedien Wiesbaden.

Brühwiler, Bruno (2008): Neue Standards für das Risikomanagement. Sicher(er) in die Zukunft. In: *QZ Qualität und Zuverlässigkeit* (7), S. 37–39. Online verfügbar unter https://www.wiso-net.de/document/QZ__QZ20080702372314301428291023131O, zuletzt geprüft am 25.06.2021.

Bundesverband der Deutschen Industrie e.V (BDI); PricewaterhouseCoopers AG (PWC) (Hg.) (2011): Risikomanagement 2.0. Ergebnisse und Empfehlungen aus einer Befragung in mittelständischen deutschen Unternehmen. Online verfügbar unter https://www.pwc.de/de/mittelstand/assets/bdi_risikomanagement_nov_2011.pdf, zuletzt geprüft am 25.06.2021.

Coates, John C., IV (2007): The Goals and Promise of the Sarbanes-Oxley Act. In: *The Journal of Economic Perspectives* 21 (1), S. 3–116. DOI: 10.1257/jep.21.1.91.

COSO (2004): Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk. Zusammenfassung. Hg. v. Committee of Sponsoring Organizations of the Treadway Commission.

COSO (2017): Enterprise Risk Management: Integrating with Strategy and Performance. Executive summary. Hg. v. Committee of Sponsoring Organizations of the Treadway Commission.

Deloitte (2017): Risikomanagement Benchmarkstudie 2017. Status Quo des Ausgestaltungsgrads gemäß der Anforderungen des PS 981.

Deloitte (2020): Risikomanagement Benchmarkstudie 2020. Analyse von Risikomanagementsystemen vor dem Hintergrund des IDW PS 981 und des IDW PS 340 n.F.

Denk, Robert; Exner-Merkelt, Karin; Ruthner, Raoul (2006): Risikomanagement im Unternehmen - Ein Überblick. In: *Wissenschaft und Management* 3 (4), S. 9–40.

Diederichs, Marc (Hg.) (2012): Risikomanagement und Risikocontrolling: Vahlen.

Diederichs, Marc (2013): Risikomanagement und Risikocontrolling. 3rd ed. München: Franz Vahlen (Finance Competence).

Dijsselbloem, Jeroen (2019): Die Eurokrise. Erfahrungsbericht eines Insiders. Wiesbaden: Springer (Sachbuch).

Ebner Stolz (2021): StaRUG macht Krisenfrüherkennung zur Pflicht! Online verfügbar unter https://www.ebnerstolz.de/de/1/0/3/3/3/4/Ebner_Stolz_StaRUG.pdf, zuletzt aktualisiert am 10.02.2021, zuletzt geprüft am 25.06.2021.

Eckhaus, Eyal; Sheaffer, Zachary (2018): Managerial hubris detection: the case of Enron. In: *Risk Management* 20 (4), S. 304–325. DOI: 10.1057/s41283-018-0037-0.

Economist Intelligence Unit (2007): Best practice in Risk Management. A function comes of age. Unter Mitarbeit von ACE, IBM und KPMG AG. Hg. v. The Economist.

Ernst & Young AG (2005): Ernst & Young Best Practice Survey “Risikomanagement 2005”. Online verfügbar unter https://www.risknet.de/fileadmin/template_risknet/dokumente/Studien/EY-Summary-Risikomanagement-2005.pdf, zuletzt geprüft am 25.06.2021.

Ernst & Young AG (2015): There´s no reward without risk. EY´s global governance, risk and compliance survey 2015. Hg. v. Ernst & Young AG.

Fiege, Stefanie (2006): Risikomanagement- und Überwachungssystem nach KonTraG. Prozess, Instrumente, Träger. 1. Aufl. Wiesbaden: Dt. Univ.-Verl. (Gabler Edition Wissenschaft).

FINANCE (2021): Wirecard-Ticker: Das Aktuellste zum Bilanzskandal. Online verfügbar unter https://www.finance-magazin.de/wirtschaft/deutschland/wirecard-ticker-das-aktuellste-zum-bilanzskandal-2059891/, zuletzt aktualisiert am 30.04.2021, zuletzt geprüft am 25.06.2021.

Fox, Alexander (2010): Einleitung. In: Alexander Fox (Hg.): Die Bewertung von Content-Anbietern unter besonderer Berücksichtigung von Web 2.0. Wiesbaden: Gabler, S. 1–4.

Francke, Swantje (2020): Corona verdeutlicht die Notwendigkeit von Risikomanagement. In: *springerprofessional.de*, 03.04.2020. Online verfügbar unter https://www.springerprofessional.de/risikomanagement/risikotransformation/corona-verdeutlicht-die-notwendigkeit-von-risikomanagement-/17862606, zuletzt geprüft am 25.06.2021.

Frentz, Clemens von (2003): Enron. Chronik einer Rekord-Pleite. Manager Magazin. Online verfügbar unter https://www.manager-magazin.de/unternehmen/artikel/a-178836.html, zuletzt geprüft am 25.06.2021.

Geiß, Stefan; Köhler, Christina (2013): Die Finanz- und Wirtschaftskrise. In: Oliver Quiring, Hans Mathias Kepplinger, Mathias Weber und Stefan Geiß (Hg.): Lehman Brothers und die Folgen. Wiesbaden: Springer Fachmedien Wiesbaden, S. 13–25.

Gleißner, Werner (2020): Controlling und Risikomanagement in der Corona-Krise: Lessons Learned (oder noch nicht?). In: *Controller Magazin*, S. 101–102. Online verfügbar unter https://rma-ev.org/fileadmin/user_upload/RMA-News_CM_Juli-August_2020.pdf, zuletzt geprüft am 25.06.2021.

Gleißner, Werner; Klein, Andreas (Hg.) (2017): Risikomanagement und Controlling. Chancen und Risiken erfassen, bewerten und in die Entscheidungsfindung integrieren. 2. Auflage. Freiburg, München, Stuttgart: Haufe Gruppe (Haufe Fachpraxis).

Hart, Oliver (2009): Regulation and Sarbanes-Oxley. In: *Journal of Accounting Research* 47 (2), S. 437–445. Online verfügbar unter http://www.jstor.org/stable/25548026.

Healy, Paul M.; Palepu, Krishna G. (2003): The Fall of Enron. In: *The Journal of Economic Perspectives* 17 (2), S. 3–26. Online verfügbar unter https://search.proquest.com/scholarly-journals/fall-enron/docview/212077863/se-2?accountid=188963.

Herre, Uwe; Sandmann, Thomas; Wehking, Julia; Winefeld, Christian (2012): Risk-ManagementBenchmarking 2011/12. Hg. v. PricewaterhouseCoopers AG (PWC).

Herre, Uwe; Tüllner, Jörg (2011): Von der Krise zu einer neuen Risikokultur? Eine Untersuchung zu den Konsequenzen, die deutsche Unternehmen aus der Wirtschaftskrise ziehen. Hg. v. PricewaterhouseCoopers AG (PWC).

Heynen, Nicole; Wartenweiler, Andreas (2014): ONR 49000:2014 – Alter Wein in neuen Schläuchen? Online verfügbar unter https://www.risknet.de/themen/risknews/onr-490002014-alter-wein-in-neuen-schlaeuchen/, zuletzt aktualisiert am 07.07.2014, zuletzt geprüft am 25.06.2021.

Holtemöller, Oliver (2010): Vermögenspreisblasen: Erklärungsansätze und wirtschaftspolitische Überlegungen. In: *Wirtschaft im Wandel* 16 (12), S. 558–564. Online verfügbar unter http://hdl.handle.net/10419/143871.

Hölzl, Markus (2020): Post-Covid-19-Risikomanagement. Ernst & Young AG. Online verfügbar unter https://www.ey.com/de_at/risk/post-covid-19-risikomanagement, zuletzt aktualisiert am 18.12.2020.

Hugo Boss AG (2020): Entsprechenheitserklärung. Online verfügbar unter https://group.hugoboss.com/de/unternehmen/corporate-governance/entsprechenserklaerung, zuletzt geprüft am 25.06.2021.

Hunziker, Stefan; Vanini, Ute; Durrer, Mirjam; Henrizi, Philipp; Unruh, Anjuli (2020): ERM Report 2020. Die Rolle der Risk Manager in der COVID-19 Krise. Hg. v. Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern.

Institut der Wirtschaftsprüfer (2017): IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981), zuletzt geprüft am 25.06.2021.

Institut der Wirtschaftsprüfer (Hg.) (2019): Entwurf einer Neufassung des IDW Prüfungsstandards: Die Prüfung der Maßnahmen nach § 91 Abs. 2 AktG im Rahmen der Jahresabschlussprüfung gemäß § 317 Abs. 4 HGB (IDW EPS 340 n.F.). IDW Verlag GmbH (IDW-Prüfungsstandards).

Institut für Interne Revision Österreich (2014): Das unternehmensweite Risikomanagementsystem aus der Sicht der Internen Revision. 2., vollst. überarb. und erw. Neuaufl. [Stuttgart etc.], Wien: Boorberg; Linde.

Integrierte Managementsysteme (2008): Risikomanagement ONR 49000 ff. Online verfügbar unter http://www.prozess-effizienz.de/Aktuelles/iM-Blick_Web/2080314_ON49000.pdf, zuletzt geprüft am 25.06.2021.

Kajüter, Peter (2012): Risikomanagement im Konzern. Eine empirische Analyse börsennotierter Aktienkonzerne. München: Vahlen.

Keitsch, Detlef (2007): Risikomanagement. Stuttgart: Schäffer-Poeschel (Handelsblatt Mittelstands-Bibliothek, Bd. 3).

Kiani-Kreß, Rüdiger (2001): Abgewickelt. Swissair. Die Nobellinie wird zerschlagen. Noch ist das Überleben der Schweizer Luftfahrt nicht gesichert. In: *Wirtschaftswoche* (41), S. 66–68.

Klein, Adam (2007): Die Kosten des Terrors. Wirtschaftliche Auswirkungen des internationalen Terrorismus. [Sankt Augustin], Berlin: Konrad-Adenauer-Stiftung (Analysen & Argumente / Konrad-Adenauer-Stiftung, Ausg. 41).

Klenk, Ralph; Reetz, Kristina (2010): Risk-Management-Benchmarking 2010. Eine Studie zum aktuellen Stand des Risikomanagements in Großunternehmen in der deutschen Realwirtschaft. Hg. v. PricewaterhouseCoopers AG (PwC).

KMU-Portal (2021): Gesetzliche Grundlagen und Normen: Vorschriften zum Risikomanagement. Schweizerische Eidgenossenschaft. Online verfügbar unter https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/finanzielles/risikomanagement/gesetzliche-grundlagen-und-normen.html, zuletzt aktualisiert am 07.05.2021, zuletzt geprüft am 25.06.2021.

Knoll, Leonhard (2020): Wirecard: Amazon gesucht - Enron gefunden. In: *WiSt - Wirtschaftswissenschaftliches Studium* 49 (9), S. 1. DOI: 10.15358/0340-1650-2020-9-1.

Köcher, Anette (2009): Rezension: Risikomanagement nach ISO 31000 und ONR 49000. Online verfügbar unter https://www.risknet.de/themen/risknews/risikomanagement-nach-iso-31000-und-onr-49000/, zuletzt geprüft am 25.06.2021.

Koller, Helga; Vogl, Jonhannes (2014): Der Handel - Risikomanagement und Versicherungen für operationelle Risiken. Eine Benchmark-Studie. Unter Mitarbeit von Sabine Hawlelka und Petra Steininger. Hg. v. GrECo International AG und Handelsverband. Wien.

Kolmar, Martin (2017): Grundlagen der Mikroökonomik. Ein integrativer Ansatz. Berlin, Heidelberg: Springer Berlin Heidelberg; Imprint; Springer.

Kraemer, Moritz; Wessel, Rhea (2021): A Storm Passes-Now, For A Recovery. In: *Global Finance* 35 (1), S. 44–45. Online verfügbar unter https://www.proquest.com/trade-journals/storm-passes-now-recovery/docview/2485064587/se-2?accountid=188963.

Löbig, Lisa; Wendt, Domenik Henning (2019): Brexit und der Finanzmarkt. Die rechtlichen Auswirkungen auf grenzüberschreitende Finanzdienstleistungen. 1. Auflage 2019. Wiesbaden: Springer Fachmedien Wiesbaden (essentials).

Lufthansa Group (2020): Entsprechenheitserklärung (§ 161 AktG). Online verfügbar unter https://investor-relations.lufthansagroup.com/de/corporate-governance/erklaerung-zur-unternehmensfuehrung-289f-hgb/entsprechenserklaerung-161-aktg.html.

Manager Magazin (2011): Olympus-Bilanzskandal: Verluste in Milliardenhöhe verschleiert. In: *manager magazin*, 06.12.2011. Online verfügbar unter https://www.manager-magazin.de/digitales/it/a-801974.html, zuletzt geprüft am 25.06.2021.

Mehring, Andreas (2019): PwC bestätigt Milliardenbetrug bei Steinhoff. FINANCE. Online verfügbar unter https://www.finance-magazin.de/finanzabteilung/bilanzierung/pwc-bestaetigt-milliardenbetrug-bei-steinhoff-2033351/, zuletzt aktualisiert am 18.03.2019, zuletzt geprüft am 25.06.2021.

Milla, Aslan; Vcelouch-Kimeswenger, Ruth; Weber, Martin (2008): Unternehmensrechts-Änderungsgesetz 2008. Praxiskommentar. Wien: Linde (Fachbuch Recht).

Nicklisch, Annette Christina (2007): Die Auswirkungen des Sarbanes-Oxley Act auf die deutsche Corporate Governance. Ein Beitrag zur Amerikanisierung des deutschen Aktienwesens. Berlin: Duncker & Humblot (Schriften zum internationalen Recht, 170).

Paetzmann, Karsten (2008): Corporate Governance: Springer Berlin Heidelberg.

Pottgießer, Gaby: Neuerungen der Rechnungslegung durch die IFRS-Verordnung und das Bilanzrechtsreformgesetz. Online verfügbar unter https://www.internerevisiondigital.de/ce/neuerungen-der-rechnungslegung-durch-die-ifrs-verordnung-und-das-bilanzrechtsreformgesetz/detail.html, zuletzt geprüft am 25.06.2021.

Pottgießer, Gaby (2006): Einflüsse internationaler Standards auf die handelsrechtliche Rechnungslegung und die steuerrechtliche Gewinnermittlung. Wiesbaden: Deutscher Universitäts Verlag.

Quiring, Oliver; Kepplinger, Hans Mathias; Weber, Mathias; Geiß, Stefan (2013): Einleitung. In: Oliver Quiring, Hans Mathias Kepplinger, Mathias Weber und Stefan Geiß (Hg.): Lehman Brothers und die Folgen. Wiesbaden: Springer Fachmedien Wiesbaden, S. 9–11.

Reuters (2020): Steinhoff bietet Klägern im Bilanzskandal 850 Millionen Euro. In: *Handelsblatt*, 27.07.2020. Online verfügbar unter https://www.handelsblatt.com/unternehmen/handel-konsumgueter/handelskonzern-steinhoff-bietet-klaegern-im-bilanzskandal-850-millionen-euro/26039874.html?ticket=ST-539975-PR6DR9dVZceAyjvq5cZr-ap2, zuletzt geprüft am 25.06.2021.

Rinker, Carola (2020): Der Bank Blog: Wirecard-Skandal: Internes Kontrollsystem hat nicht versagt - Dennoch Totalversagen des Compliance-Systems. In: *Newstex Finance & Accounting Blogs*. Online verfügbar unter https://search.proquest.com/blogs-podcasts-websites/der-bank-blog-wirecard-skandal-internes/docview/2428914567/se-2?accountid=188963, zuletzt geprüft am 25.06.2021.

ISO 31000:2009, 01.02.2010: Risikomanagement: Grundsätze und Richtlinien.

Rohlfs, Torsten; Mahnke, Alexander (2020): Risikomanagement im Unternehmen. In: Alexander Mahnke und Torsten Rohlfs (Hg.): Betriebliches Risikomanagement und Industrieversicherung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 3–16.

Romeike, Frank (2018): Risikomanagement. Wiesbaden: Springer Gabler (Studienwissen kompakt).

Romeike, Frank; Hager, Peter (2020): Erfolgsfaktor Risiko-Management 4.0. Methoden, Beispiele, Checklisten : Praxishandbuch für Industrie und Handel. 4., vollständig überarbeitete Auflage. Wiesbaden, Germany: Springer Gabler.

Schäfer, Dorothea (2020): Wirecard — ein Menetekel für die Wirtschaftsprüfung. In: *Wirtschaftsdienst* 100 (8), S. 562–563. DOI: 10.1007/s10273-020-2705-4.

Skorna, Alexander; Nießen, Philipp (2020): Risikoanalyse, -bewertung und -steuerung. In: Alexander Mahnke und Torsten Rohlfs (Hg.): Betriebliches Risikomanagement und Industrieversicherung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 41–65.

Stampfer, Erwin (2019): Risikosteuerung in der Industrie. Konzepte, Methoden und Verfahren für projektorientierte Unternehmen. [1. Auflage]. Wien: Linde.

Stephan, Jörg (2006): Finanzielle Kennzahlen für Industrie- und Handelsunternehmen. Eine wert- und risikoorientierte Perspektive. 1. Aufl. Wiesbaden: Deutscher Universitats-Verlag GWV Fachverlage GmbH, Wiesbaden (Gabler Edition Wissenschaft). Online verfügbar unter http://gbv.eblib.com/patron/FullRecord.aspx?p=751754.

Tekathen, Matthäus (2015): Enterprise Risk Management in der Unternehmenspraxis: Ein Zwischenfazit nach zehn Jahren ERM. In: *CON* 27 (6), S. 323–329. DOI: 10.15358/0935-0381-2015-6-323.

Theuermann, Christian; Ebner, Gerhart (2014): Risikomanagement im österreichischen Mittelstand. Vergleich 2012/2014: Verbreitung, Bedeutung und zukünftige Erwartungen. Unter Mitarbeit von Lisa Grieshofer, Laurens Knasar, Andrea Kren, Martina Pöttler und Sabrina Schrötter. Hg. v. Christian Theuermann und Peter Meiregger. Campus 02, Rechnungswesen & Controlling. Graz.

Tilch, Thomas; Lenz, Alexander; Scheffler, Rene; Andreas, Stephan; Obersdorf, Sebastian; Yilmaz, Yunus (2015): Risk-Management Benchmarking 2015. Hg. v. Pricewaterhouse-Coopers AG (PWC).

Tranchard, Sandrine (2018): The new ISO 31000 keeps risk management simple. Hg. v. iso.org. Online verfügbar unter https://www.iso.org/news/ref2263.html, zuletzt aktualisiert am 15.02.2018, zuletzt geprüft am 25.06.2021.

Vanini, Ute (2012): Risikomanagement. Grundlagen, Instrumente, Unternehmenspraxis. Stuttgart: Schäffer-Poeschel.

Volmer, Philipp; Köllmer, Christoph (2020): Restructuring Insights. Neuer Stabilisierungs- und Restrukturierungsrahmen ist am 1. Januar 2021 in Kraft getreten und erleichtert die Unternehmenssanierung. Hg. v. KPMG AG. Online verfügbar unter https://assets.kpmg/content/dam/kpmg/de/pdf/Themen/2021/01/restructuring-insights1.pdf, zuletzt geprüft am 25.06.2021.

Von der Crone, Hans Caspar; Roth, Katja (2003): Der Sarbanes-Oxley Act und seine extraterritoriale Bedeutung. In: *AJP/PJA* 2, S. 131–140. Online verfügbar unter https://www.ius.uzh.ch/dam/jcr:ffffffff-bd2f-a7a1-0000-00003fec14f5/Sarbanes_Oxley.pdf, zuletzt geprüft am 25.06.2021.

VR Wissen: Risikomanagement. Online verfügbar unter http://vr-wissen.ch/risiko.php, zuletzt geprüft am 25.06.2021.

Weis, Udo (2012): Risikomanagement nach ISO 31000. Risiken erkennen und erfolgreich steuern. Kissing: WEKA MEDIA (Weka-Praxislösungen).

WELT (2011): Bilanzskandal: Olympus vertuscht jahrelang Milliarden-Verlust. In: *WELT*, 06.12.2011. Online verfügbar unter https://www.welt.de/wirtschaft/article13753538/Olympus-vertuscht-jahrelang-Milliarden-Verlust.html, zuletzt geprüft am 25.06.2021.

Anhang

A1: IDW PS 981

IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)

(Stand: 03.03.2017)[1]

[1] Vorbereitet vom Arbeitskreis „Prüfungsfragen und betriebswirtschaftliche Fragen zu Governance, Risk und Compliance“ (GRC). Verabschiedet vom Hauptfachausschuss (HFA) am 03.03.2017.

1. Vorbemerkungen

1 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) verdeutlicht in diesem *IDW Prüfungsstandard* den Inhalt freiwilliger Prüfungen (vgl. Tz. 16) von Risikomanagementsystemen und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit derartige Aufträge planen und durchführen sowie darüber Bericht erstatten.

2 § 107 Abs. 3 Satz 2 AktG sieht vor, dass der Aufsichtsrat aus seiner Mitte einen Prüfungsausschuss bestellen kann, der sich neben der Überwachung der Abschlussprüfung befasst mit

- der Überwachung des Rechnungslegungsprozesses,
- der Wirksamkeit
  - des internen Kontrollsystems,
  - des Risikomanagementsystems und
  - des Internen Revisionssystems.

In der Gesetzesbegründung zum BilMoG wird ausgeführt, dass die in § 107 Abs. 3 Satz 2 AktG – der zunächst lediglich die innere Ordnung des Aufsichtsrats betrifft – genannten Bereiche als eine Konkretisierung der allgemeinen Überwachungsaufgabe des Aufsichtsrats aus § 111 Abs. 1 AktG anzusehen sind (vgl. Tz. A1). Zudem wird in der Gesetzesbegründung klargestellt, dass der Aufsichtsrat die genannten Aufgaben selbst wahrzunehmen hat, wenn er keinen Prüfungsausschuss einrichtet.[2]

3 Die Überwachungsaufgaben des Aufsichtsrats umfassen auch die Maßnahmen des Vorstands, die sich auf die Begrenzung der Risiken aus möglichen Verstößen gegen gesetzliche Vorschriften und interne Richtlinien (Compliance) beziehen. Dem trägt Ziffer 5.3.2 des Deutschen Corporate Governance Kodex (DCGK) Rechnung, der zu den Aufgaben des Prüfungsausschusses ausführt, dass sich der Prüfungsausschuss – falls kein anderer Ausschuss damit betraut ist – auch mit der Compliance des Unternehmens befasst.

4 Während die Befassung durch den Aufsichtsrat und den Prüfungsausschuss voraussetzt, dass die entsprechenden Systeme vorhanden sind, ist – ungeachtet der Pflichten nach § 91 Abs. 2 AktG – die Einrichtung, Ausgestaltung und Überwachung der Systeme eine im Orga-

[2] Vgl. BT-Drucks. 16/10067, S. 102.

nisationsermessen des Vorstands stehende unternehmerische Entscheidung, durch die der Vorstand vor dem Hintergrund der unternehmensindividuellen Gegebenheiten seinen allgemeinen Organisations- und Sorgfaltspflichten nachkommt (vgl. Tz. A2). Die konkrete Ausgestaltung ist hierbei insb. von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens abhängig (vgl. Tz. 31).

5 Die durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden Corporate Governance Systeme

- internes Kontrollsystem (IKS),
- Risikomanagementsystem (RMS),
- Internes Revisionssystem (IRS) und
- Compliance Management System (CMS)

sind weder im Gesetz noch in der Literatur eindeutig definiert. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme lehnt sich dieser *IDW Prüfungsstandard* an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement[3] an (vgl. Tz. A3).

6 Auch wenn die Überwachungsfunktion höchstpersönlich von den Aufsichtsrats- bzw. Prüfungsausschussmitgliedern wahrzunehmen ist und nicht an Dritte delegiert werden kann, kann es für den Aufsichtsrat von Interesse sein, einen Wirtschaftsprüfer mit der Prüfung einzelner oder mehrerer Corporate Governance Systeme als Grundlage für die eigene Beurteilung zu beauftragen. Auch der Vorstand kann ein Interesse daran haben, einen Wirtschaftsprüfer mit der Prüfung eines oder mehrerer dieser Systeme zu beauftragen. Die Prüfung der Wirksamkeit dieser Systeme durch einen unabhängigen Wirtschaftsprüfer kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten des Vorstands und des Aufsichtsrats dienen.

7 Dieser *IDW Prüfungsstandard* behandelt die Prüfung des Teils des unternehmensweiten Risikomanagements, der sich mit den strategischen Risiken und den operativen Risiken aus der Geschäftstätigkeit (Risiken aus den Leistungserstellungsprozessen) befasst. Die Prüfung i.S. dieses *IDW Prüfungsstandards* (im Folgenden auch: RMS-Prüfung) umfasst stets sämtliche Grundelemente des Risikomanagementsystems (vgl. Tz. 31). Eine isolierte Prüfung einzelner Grundelemente liegt nicht im Anwendungsbereich dieses *IDW Prüfungsstandards* (vgl. Tz. A5).

8 Die Zielsetzung einer nach diesem *IDW Prüfungsstandard* durchgeführten Systemprüfung liegt in der Beurteilung, inwieweit das Unternehmen durch Einrichtung eines RMS Vorsorge getroffen hat, wesentliche strategische und operative Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen. Ziel ist es dagegen nicht, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind. Die Prüfung ist auch nicht darauf ausgerichtet, ein Prüfungsurteil über den Fortbestand des geprüften Unternehmens zu erteilen.

[3] Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk (COSO ERM): https://www.coso.org/Pages/guidance.aspx (Stand: 13.03.2017).

9 Die Prüfung des RMS in Bezug auf operative (betriebliche) Risiken betrifft diejenigen Risiken aus der Geschäftstätigkeit bzw. den Leistungserstellungsprozessen, die dem Erreichen der aus den strategischen Zielen abgeleiteten operativen Ziele entgegenstehen. Für Zwecke der Prüfung des operativen Risikomanagementsystems sieht dieser *IDW Prüfungsstandard* eine Abgrenzung zu prüfender Teilbereiche durch den Auftraggeber vor.

10 Die Prüfung des RMS kann auch auf das Management der strategischen Risiken begrenzt werden. Die strategischen Risiken betreffen diejenigen Risiken, die dem Erreichen der strategischen Unternehmensziele entgegenstehen (vgl. Tz. A6). In Bezug auf den Teil des RMS, der auf das Management der strategischen Risiken ausgerichtet ist, wird grundsätzlich eine unternehmensübergreifende Sichtweise verfolgt. Im Falle der Prüfung des strategischen RMS erfolgt daher i.d.R. keine Eingrenzung auf einzelne Unternehmensprozesse oder Bestandteile der Unternehmensorganisation (vgl. Tz. A7).

11 Die Abgrenzung eines zu prüfenden Teilbereichs i.S. dieses *IDW Prüfungsstandards* bestimmt sich nach einzelnen operativen Risikoarten und/oder Unternehmensprozessen bzw. Organisationseinheiten (z.B. Geschäftsbereichen, Funktionsbereichen, Geschäftsprozessen, Niederlassungen und/oder Regionen) (vgl. Tz. A4).

12 Für die Prüfung des Compliance Management Systems, des internen Kontrollsystems der Unternehmensberichterstattung sowie des Internen Revisionssystems hat das IDW gesonderte *IDW Prüfungsstandards* veröffentlicht.[4] Die Abgrenzung der Prüfungsgegenstände ist dabei nicht notwendigerweise überschneidungsfrei. In Abhängigkeit von den Prüfungszielen und der Festlegung des zu prüfenden Teilbereichs durch die gesetzlichen Vertreter können deshalb mehrere dieser Verlautbarungen bei einem Prüfungsauftrag anwendbar sein.

13 Die Prüfung des RMS nach diesem *IDW Prüfungsstandard* ist von der Prüfung der gemäß § 91 Abs. 2 AktG einzurichtenden Maßnahmen zur frühzeitigen Erkennung von den Fortbestand der Gesellschaft gefährdenden Entwicklungen (sog. „Risikofrüherkennungssystem“) nach § 317 Abs. 4 HGB zu unterscheiden. Für die Prüfung der Maßnahmen nach § 91 Abs. 2 AktG ist *IDW PS 340*[5] anzuwenden.

14 Neben Definitionen (Abschn. 2), Gegenstand, Ziel und Umfang der Prüfung (Abschn. 3) und einer Beschreibung der Grundelemente eines RMS (Abschn. 4) enthält dieser *IDW Prüfungsstandard* in den Abschn. 5 – 10 zu beachtende Prüfungsanforderungen sowie Anwendungshinweise und Erläuterungen (Tz. A1 ff. und Anlagen).[6]

15 Dieser *IDW Prüfungsstandard* behandelt Prüfungsaufträge zur Erlangung hinreichender Sicherheit. Er steht im Einklang mit dem International Standard on Assurance Engagements

[4] Vgl. *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)* (Stand: 11.03.2011), *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)* (Stand: 03.03.2017) und *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983)* (Stand: 03.03.2017).

[5] Vgl. *IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340)* (Stand: 11.09.2000).

[6] Die Anwendungshinweise und sonstigen Erläuterungen (einschließlich der Anlagen) enthalten weiterführende Hinweise zu den Anforderungen dieses *IDW Prüfungsstandards* sowie zu deren Umsetzung. Insbesondere können sie a) genauer erläutern, was eine Anforderung bedeuten oder abdecken soll; b) Beispiele für Prüfungshandlungen enthalten, die unter den gegebenen Umständen geeignet sein können. Obwohl solche erläuternden Hinweise keine Anforderungen darstellen, sind sie für die richtige Anwendung der Anforderungen dieses *IDW Prüfungsstandards* relevant.

(ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ (Stand Dezember 2013).[7]

16 Dieser *IDW Prüfungsstandard* betrifft freiwillige Prüfungen von RMS. Er findet keine Anwendung auf gesetzlich vorgeschriebene Prüfungen von RMS, z.B. Prüfung des RMS für aufsichtsrechtliche Zwecke bei Kreditinstituten nach dem Kreditwesengesetz.

17 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden bei freiwilligen Prüfungen von RMS, die nach dem 30.04.2017 beauftragt werden.

2. Definitionen

18 Für die Zwecke dieses *IDW Prüfungsstandards* gelten die folgenden Begriffsdefinitionen:

a. Risiken – mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen (Risiko im engeren Sinne) oder positiven (Chance) Zielabweichung führen können.

b. Operative (betriebliche) Risiken – mögliche künftige Entwicklungen oder Ereignisse, die im Hinblick auf die Geschäftstätigkeit bzw. die Leistungserstellungsprozesse zu einer für das Unternehmen negativen oder positiven Abweichung von den aus den strategischen Zielen abgeleiteten operativen Ziele führen können.

c. Strategische Risiken – mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen oder positiven Abweichung von den strategischen Zielen führen können.

d. Wesentliches Risiko – Risiko, das – mit einer nicht nur vertretbar geringen Eintrittswahrscheinlichkeit – zu einer für das Unternehmen negativen oder positiven Zielabweichung führen kann, durch die die Unternehmensziele nicht entsprechend der Risikostrategie erreicht werden.

e. Risikomanagement – strukturierter Umgang mit Risiken (i.S.v. positiven und negativen Zielabweichungen) im Unternehmen (vgl. Tz. A9).

f. Risikomanagementsystem – Gesamtheit der Regelungen, die einen strukturierten Umgang mit Risiken (i.S.v. positiven und negativen Zielabweichungen) im Unternehmen sicherstellt (vgl. Tz. 31, Tz. A8 f.).

g. Regelungen – Oberbegriff für Grundsätze, Verfahren und vorgegebene Maßnahmen im Rahmen des Risikomanagements.

h. Aussagen des Unternehmens über das RMS – in einer RMS-Beschreibung explizit oder implizit enthaltene Aussagen der gesetzlichen Vertreter zu den Grundelementen des RMS (Tz. 31, Tz. A21 ff.) sowie zur Angemessenheit, Implementierung und ggf. zur Wirksamkeit des RMS in Übereinstimmung mit den angewandten RMS-Grundsätzen.

i. RMS-Grundsätze – allgemein anerkannte Rahmenkonzepte, andere angemessene Rahmenkonzepte oder vom Unternehmen selbst entwickelte Grundsätze für Risikomanagementsysteme (vgl. Tz. A20).

[7] https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga (Stand: 13.03.2017).

j. Allgemein anerkannte Rahmenkonzepte für RMS – Rahmenkonzepte, die von einer autorisierten oder anerkannten standardsetzenden Organisation im Rahmen eines transparenten Verfahrens entwickelt und verabschiedet oder durch gesetzliche oder andere rechtliche Anforderungen festgelegt werden (vgl. Tz. A11 und Anlage 1).

k. RMS-Beschreibung – Darstellung der Regelungen zu den Grundelementen eines RMS. Die angewandten RMS-Grundsätze werden in der RMS-Beschreibung entweder durch Verweis auf allgemein zugängliche RMS-Grundsätze oder durch Aufzählung der einzelnen Grundsätze dargestellt (vgl. Tz. A12).

l. Prüfungsrisiko – Risiko, dass der RMS-Prüfer ein uneingeschränktes Prüfungsurteil abgibt, wenn die Aussagen in der RMS-Beschreibung einen wesentlichen Fehler aufweisen.

m. Fehler in den Aussagen der RMS-Beschreibung – die RMS-Beschreibung ist unvollständig oder enthält falsche oder irreführende Aussagen (vgl. Tz. A13).

n. Mangel des RMS – Beanstandung hinsichtlich der Angemessenheit bzw. Wirksamkeit der Regelungen zur Identifizierung, Bewertung, Steuerung und Überwachung der Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen.

o. Sachverständiger des RMS-Prüfers – eine natürliche Person oder eine Organisation mit Fachkenntnissen auf einem anderen Gebiet als betriebswirtschaftlichen Prüfungen, deren Arbeit auf diesem Gebiet vom RMS-Prüfer verwertet wird, um den RMS-Prüfer dabei zu unterstützen, ausreichende und angemessene Prüfungsnachweise zu erlangen. Bei einem Sachverständigen des RMS-Prüfers kann es sich entweder um einen internen Sachverständigen handeln (d.h. einen Partner oder fachlichen Mitarbeiter der Praxis des RMS-Prüfers oder eines Mitglieds des Netzwerks der Wirtschaftsprüferpraxis) oder um einen externen Sachverständigen des RMS-Prüfers.

19 Für die Zwecke dieses *IDW Prüfungsstandards* umfasst der Begriff „Unternehmen“ nicht nur Unternehmen im rechtlichen Sinne, sondern auch andere Einheiten (vgl. Tz. A14).

3. Gegenstand, Ziel und Umfang der Prüfung

20 Gegenstand der Prüfung sind die in der RMS-Beschreibung enthaltenen Aussagen des Unternehmens über das RMS.

21 Die Verantwortung für das RMS, d.h. die Konzeption, Implementierung, Aufrechterhaltung und Überwachung eines angemessenen und wirksamen RMS, und die Inhalte der RMS-Beschreibung, einschließlich der Abgrenzung von Teilbereichen, die der Prüfung unterliegen sollen, sowie für die Auswahl bzw. Entwicklung geeigneter RMS-Grundsätze liegt bei den gesetzlichen Vertretern des Unternehmens. Diese Verantwortung umfasst auch die Dokumentation des RMS, um eine konsistente Anwendung und personenunabhängige Funktion des Systems im Zeitablauf zu ermöglichen, sowie ggf. die Organisation der Erstellung der RMS-Beschreibung durch geeignete Personen im Unternehmen, z.B. einen für das Risikomanagementsystem operativ Verantwortlichen (vgl. Tz. A15 f.).

22 Ziel einer Wirksamkeitsprüfung des RMS ist es, dem Prüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die im geprüften Zeitraum implementierten (vgl. Tz. 28) Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt (vgl. Tz. 26) sind,
- die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen
  - während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen, und
  - während des geprüften Zeitraums wirksam (vgl. Tz. 29) waren.

23 Neben einer Prüfung der Wirksamkeit ist auch die Beauftragung einer Prüfung möglich, die sich nur auf die Angemessenheit und Implementierung der in der RMS-Beschreibung dargestellten Regelungen des RMS bezieht *(Angemessenheitsprüfung)*. Eine Wirksamkeitsprüfung umfasst stets auch die Angemessenheitsprüfung.

24 Die *Angemessenheitsprüfung* zielt darauf ab, dem RMS-Prüfer ein Urteil mit hinreichender Sicherheit darüber zu ermöglichen, ob

- die zu einem bestimmten Zeitpunkt implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind,
- die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen
  - geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen, und
  - zu einem bestimmten Zeitpunkt implementiert (vgl. Tz. 28) waren.

25 Für Unternehmen, die ein RMS erstmals einrichten oder erweitern, kann es zweckmäßig sein, im Rahmen einer Angemessenheitsprüfung einen Wirtschaftsprüfer bereits während der Entwicklung, Einführung, Änderung oder Erweiterung des Systems projektbegleitend mit der RMS-Prüfung nach diesem *IDW Prüfungsstandard* zu beauftragen (vgl. Tz. A17).

26 Die in der RMS-Beschreibung enthaltenen Aussagen zu den Regelungen des RMS sind angemessen dargestellt, wenn sie auf sämtliche der in Tz. 31 genannten Grundelemente eines RMS eingehen und keine wesentlichen Fehler (vgl. Tz. 18m.) enthalten.

27 Die Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. Dies umfasst auch die Überwachung durch das RMS, ob die von den gesetzlichen Vertretern implementierten Risikosteuerungsmaßnahmen geeignet sind, mit hinreichender Sicherheit die Risikostrategie umzusetzen und die Ziele des RMS zu erreichen (vgl. Tz. A18).

28 Der Begriff Implementierung bezieht sich auf die Einrichtung der Regelungen des RMS in den Geschäftsprozessen zu einem bestimmten Zeitpunkt.

29 Die Wirksamkeit des RMS ist dann gegeben, wenn die Regelungen in den laufenden Geschäftsprozessen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung in einem bestimmten Zeitraum wie vorgesehen eingehalten werden (vgl. Tz. A19).

30 Es liegt in der Verantwortung des RMS-Prüfers, Prüfungshandlungen durchzuführen, um ausreichende und angemessene Prüfungsnachweise zu erlangen, auf die er sein Urteil zu den in der RMS-Beschreibung enthaltenen Aussagen stützen kann.

4. Grundelemente eines RMS

31 Ein RMS i.S. dieses *IDW Prüfungsstandards* weist die folgenden miteinander in Wechselwirkung stehenden Grundelemente auf, die in die Geschäftsabläufe eingebunden sind (vgl. Tz. 21 ff.). Bei der Konzeption des RMS sind die Wechselwirkungen zwischen den Grundelementen zu berücksichtigen. Die Ausgestaltung des RMS hängt insb. von den festgelegten Zielen des RMS sowie von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens ab:

Risikokultur (vgl. Tz. A21)	Die Risikokultur als Teil der Unternehmenskultur umfasst die grundsätzliche Einstellung und die Verhaltensweisen beim Umgang mit Risikosituationen. Sie beeinflusst maßgeblich das Risikobewusstsein im Unternehmen und bildet die Grundlage für ein wirksames RMS.
Ziele des RMS (vgl. Tz. A22)	Die unternehmenspolitischen Zielsetzungen und insb. die Unternehmensstrategie bilden die Ausgangsbasis für die Ableitung einer Risikostrategie und für ein systematisches Risikomanagement des Unternehmens. In der Risikostrategie wird festgelegt, in welchem Ausmaß unter Berücksichtigung der Risikotragfähigkeit des Unternehmens Risiken eingegangen werden sollen (Risikoappetit), ergänzt durch unternehmerische Vorgaben zum erwünschten Umgang mit Risiken in Form einer Risikopolitik. Die Ziele des RMS sind darauf ausgerichtet sicherzustellen, dass die Unternehmensziele entsprechend der Risikostrategie erreicht werden.
Organisation des RMS (vgl. Tz. A23)	Von entscheidender Bedeutung für das RMS sind eine transparente und eindeutige Aufbauorganisation sowie eine klar definierte Ablauforganisation. Verantwortungsbereiche und Rollen sind klar geregelt, abgegrenzt, kommuniziert und dokumentiert. Die Aufgabenträger erfüllen die erforderlichen persönlichen und fachlichen Voraussetzungen. Es stehen ausreichende Ressourcen für Risikomanagementmaßnahmen zur Verfügung (insb. Personen, Technologie, Hilfsmittel). Die wesentlichen Regelungen zur Aufbau- und Ablauforganisation des Risikomanagements sind dokumentiert und verbindlich vorgegeben.
Risikoidentifikation	Die Risikoidentifikation umfasst die regelmäßige, systematische

(vgl. Tz. A24)	Analyse von internen und externen Entwicklungen und Ereignissen, die zu negativen oder positiven Abweichungen von den festgelegten Zielen des RMS führen können.
Risikobewertung (vgl. Tz. A25)	Risiken werden hinsichtlich ihrer Ursache-Wirkungs-Zusammenhänge systematisch untersucht sowie typischerweise im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Auswirkungen beurteilt. Bewertungsverfahren und -kriterien sind (auch für nicht quantifizierbare Risiken) eindeutig definiert. Dies umfasst die Verwendung einer Bewertungssystematik, die es erlaubt, die Bedeutung und den Wirkungsgrad von Risikosteuerungsmaßnahmen einzuschätzen. Die einzelnen Risikobewertungen werden systematisch aggregiert. Risikointerdependenzen werden dabei analysiert und berücksichtigt.
Risikosteuerung (vgl. Tz. A26)	Auf der Grundlage der identifizierten und bewerteten Risiken trifft die Unternehmensleitung Entscheidungen über Maßnahmen zur Risikosteuerung (Risikovermeidung, Risikoreduktion, Risikoteilung bzw. -transfer sowie Risikoakzeptanz). Als Bezugsrahmen dienen die festgelegten Ziele des RMS.
Risikokommunikation (vgl. Tz. A27)	Die Risikokommunikation gewährleistet einen angemessenen Informationsfluss im RMS. Dies umfasst einen standardisierten Prozess auf der Basis konkreter Zuständigkeiten, Periodizitäten, Schwellenwerte und Berichtsformate. Für eilbedürftige Risikomeldungen ist ein separater Berichtsprozess etabliert, der eine zeitnahe Übermittlung der relevanten Informationen sicherstellt. Für die Risikobeurteilung werden die entscheidungsrelevanten Informationen gesammelt, auf ihre Zuverlässigkeit überprüft und aktualisiert.
Überwachung und Verbesserung des RMS (vgl. Tz. A28)	Die Angemessenheit und Wirksamkeit des RMS werden durch prozessintegrierte und prozessunabhängige Kontrollen überwacht. Voraussetzung für die Überwachung ist eine angemessene Dokumentation des RMS. Die Ergebnisse der Überwachungsmaßnahmen (insb. festgestellte Mängel im RMS) werden in geeigneter Form berichtet und ausgewertet, damit die erforderlichen Maßnahmen zur Verbesserung des Systems und zur Beseitigung von Mängeln ergriffen werden können.

Anforderungen

5. Berufspflichten

32 RMS-Prüfungen i.S. dieses *IDW Prüfungsstandards* sind betriebswirtschaftliche Prüfungen außerhalb der Jahresabschlussprüfung, bei denen der RMS-Prüfer neben den allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit (§§ 17 Abs. 1, 43 Abs. 1 Satz 1, 49 WPO, §§ 1 – 12 BS WP/vBP) auch die besonderen Berufspflichten nach §§ 28 – 44 BS WP/vBP zu beachten hat.

6. Auftragsannahme

33 Vor Auftragsannahme hat sich der Wirtschaftsprüfer zu vergewissern, dass die Regelungen des Qualitätssicherungssystems der WP-Praxis zur Auftragsannahme und Auftragsfortführung eingehalten werden.[8] Ein Auftrag zur Durchführung einer RMS-Prüfung darf nur angenommen werden, wenn davon auszugehen ist, dass die Berufspflichten einschließlich des Unabhängigkeitsgrundsatzes eingehalten werden können. Dies setzt voraus, dass ausreichende Erfahrung und Kompetenz sowie personelle und zeitliche Ressourcen in der WP-Praxis vorhanden sind oder erlangt werden können, um den Auftrag ordnungsgemäß durchführen zu können (§ 4 Abs. 2 BS WP/vBP).

34 Ist der Wirtschaftsprüfer mit der Jahresabschlussprüfung für das Unternehmen beauftragt, steht dies einer Beauftragung des Wirtschaftsprüfers als RMS-Prüfer nicht entgegen.

35 Bei der notwendigen Beurteilung der Auftragsrisiken vor Auftragsannahme hat der Wirtschaftsprüfer festzustellen, ob das vorgesehene Prüfungsteam insgesamt über die für die Durchführung des Auftrags notwendigen Fach- und Branchenkenntnisse verfügt, Erfahrungen mit den einschlägigen rechtlichen Anforderungen vorliegen oder erlangt werden können und erforderlichenfalls Sachverständige (z.B. IT-Spezialisten bei der Beurteilung der Sicherheit von IT-gestützten Geschäftsprozessen im Rahmen der Prüfung des RMS) zur Verfügung stehen.[9] Zudem hat der Wirtschaftsprüfer festzustellen, ob er davon ausgehen kann, dass die erforderlichen Prüfungsnachweise erlangt werden.

36 Im Zusammenhang mit der Entscheidung über die Annahme eines Auftrags zur Durchführung einer RMS-Prüfung hat sich der Wirtschaftsprüfer Informationen über die Ausgestaltung des RMS und der angewandten RMS-Grundsätze zu verschaffen, um die grundsätzliche Eignung des in der RMS-Beschreibung dargestellten Systems als Prüfungsgegenstand zu beurteilen. Diese Beurteilung hat anhand der in Tz. 31 dargestellten Grundelemente eines RMS zu erfolgen (vgl. Tz. A29 ff.).

37 Da die Grundlage der Prüfung eine Beschreibung des im Unternehmen eingerichteten RMS ist, darf der Prüfer den Auftrag nur annehmen, wenn eine RMS-Beschreibung vorliegt bzw. die gesetzlichen Vertreter ihre Bereitschaft erklären, eine RMS-Beschreibung zu erstellen.

38 Der RMS-Prüfer hat mit dem Auftraggeber die Auftragsbedingungen – insb. die Verantwortlichkeiten der gesetzlichen Vertreter und des RMS-Prüfers – schriftlich zu vereinbaren (vgl. Tz. A33 f.).

39 Im Auftragsbestätigungsschreiben ist darauf hinzuweisen, dass keine Prüfungssicherheit darüber erlangt wird, ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf durch das zu prüfende RMS erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll

[8] Vgl. *Entwurf eines IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW EQS 1)* (Stand: 04.10.2016), Tz. 70 ff.

[9] Vgl. *IDW EQS 1*, Tz. 75.

sind, sondern ausschließlich die in der RMS-Beschreibung getroffenen Aussagen zum RMS beurteilt werden (vgl. Tz. 8).

40 Wird dem Wirtschaftsprüfer vor Auftragsannahme ein Prüfungshemmnis bekannt, das nach Einschätzung des Wirtschaftsprüfers zu einer Nicht-Erteilung des Prüfungsurteils führen würde, darf er den Auftrag nicht annehmen.

41 Werden dem RMS-Prüfer nach Auftragsannahme Informationen bekannt, die – wenn sie ihm vorher bekannt geworden wären – zur Ablehnung des Auftrags geführt hätten, hat er über die ggf. erforderlichen Schritte zu entscheiden, z.B. bei Unabhängigkeitsrisiken die Ergreifung von Schutzmaßnahmen i.S.v. § 30 BS WP/vBP oder ggf. die Niederlegung des Mandats.[10]

42 Der RMS-Prüfer darf nach Auftragsannahme einer wesentlichen Änderung der Bedingungen des Prüfungsauftrags nicht zustimmen, wenn es dafür keine vertretbare Begründung gibt (vgl. Tz. A36). Erfolgt eine Änderung der Bedingungen, darf der Prüfer Prüfungsnachweise nicht außer Acht lassen, die vor der Änderung der Auftragsbedingungen erlangt wurden.

7. Prüfungsplanung

7.1. Allgemeine Grundsätze

43 Der RMS-Prüfer hat die Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass sie in sachgerechter Weise durchgeführt werden kann. Hierzu sind Art, zeitliche Einteilung und Umfang der geplanten Prüfungshandlungen festzulegen, die erforderlich sind, um die Prüfungsziele (vgl. Tz. 22 ff.) zu erreichen.

44 Bei der Auswahl der Mitglieder des Prüfungsteams hat der RMS-Prüfer darauf zu achten, dass diese insgesamt über ausreichende praktische Erfahrungen mit Systemprüfungen sowie die notwendigen Branchen- und ggf. Rechtskenntnisse verfügen, um den Auftrag ordnungsgemäß durchzuführen und ein sachgerechtes Prüfungsurteil zu erteilen.[11] Das Prüfungsteam muss über ausreichende Kenntnisse in den relevanten Teilbereichen (vgl. Tz. 11) verfügen, die dem zu prüfenden RMS zugrunde liegen. Der RMS-Prüfer hat sich zu vergewissern, dass das Prüfungsteam bei der Hinzuziehung von Sachverständigen im erforderlichen Umfang in die Tätigkeit des Sachverständigen eingebunden werden kann, um die Verantwortung für sein Prüfungsurteil insgesamt übernehmen zu können.

45 Der RMS-Prüfer muss die Prüfung mit einer kritischen Grundhaltung[12] planen und mit dem Bewusstsein durchführen, dass Umstände bestehen können, die dazu führen, dass das RMS zu dem zu prüfenden Zeitpunkt bzw. in dem zu prüfenden Zeitraum nicht angemessen bzw. wirksam war. Unter Ausübung seines pflichtgemäßen Ermessens hat der Prüfer die Prüfungshandlungen so zu planen und durchzuführen, dass das Prüfungsrisiko (vgl. Tz. 18l.) soweit reduziert wird, um mit hinreichender Sicherheit beurteilen zu können, ob die RMS-Beschreibung wesentliche Fehler (vgl. Tz. 50) enthält.

[10] Vgl. *IDW EQS 1*, Tz. 79.

[11] Vgl. § 38 Abs. 3 BS WP/vBP.

[12] Vgl. § 37 BS WP/vBP; zur kritischen Grundhaltung vgl. auch *IDW Prüfungsstandard: Ziele und allgemeine Grundsätze der Durchführung von Abschlussprüfungen (IDW PS 200)* (Stand: 03.06.2015), Tz. 17.

46 Bei der Bestimmung von Art und Umfang der Prüfungshandlungen hat der RMS-Prüfer die Art des Prüfungsauftrags (Angemessenheits- oder Wirksamkeitsprüfung) und das beurteilte Risiko wesentlicher Fehler in der RMS-Beschreibung (vgl. Abschn. 7.3) zu berücksichtigen, das insb. von den angewandten RMS-Grundsätzen, der Beschreibung des RMS durch die gesetzlichen Vertreter und den in der RMS-Beschreibung dargestellten Teilbereichen des RMS bestimmt wird.

47 Umfasst die Prüfung des RMS mehrere Organisationseinheiten (z.B. rechtlich selbstständige Einheiten oder Niederlassungen), hat der RMS-Prüfer bei der Festlegung von Art und Umfang der Prüfungshandlungen die Bedeutsamkeit der relevanten Risiken in den jeweiligen Organisationseinheiten zu berücksichtigen (vgl. Tz. A37 ff.).

48 Der RMS-Prüfer muss die geplanten Prüfungshandlungen in einem Prüfungsprogramm zusammenfassen, das die Prüfungsanweisungen zur sachlichen und zeitlichen Auftragsabwicklung für die Mitglieder des Prüfungsteams enthält.[13]

49 Zudem hat der RMS-Prüfer die übrigen auftragsbezogenen Qualitätssicherungsmaßnahmen zu planen, sowie die Überwachung der Auftragsabwicklung und die Durchsicht der Prüfungsergebnisse.[14]

7.2. Wesentlichkeit

50 Der RMS-Prüfer hat für Zwecke der Planung und Durchführung der Prüfungshandlungen sowie der Auswertung der Prüfungsergebnisse zu bestimmen, in welchen Fällen ein Fehler in der RMS-Beschreibung bzw. in welchen Fällen ein Mangel des RMS qualitativ oder quantitativ als wesentlich einzustufen ist (vgl. Tz. A40 ff.). Die Bestimmung der Wesentlichkeit liegt im pflichtgemäßen Ermessen des RMS-Prüfers.

7.3. Prüfungshandlungen zur Identifikation und Beurteilung von Risiken wesentlicher Fehler in der RMS-Beschreibung

7.3.1. Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld

51 Der RMS-Prüfer hat ein Verständnis von dem rechtlichen und wirtschaftlichen Umfeld, den Merkmalen des Unternehmens sowie den Unternehmenszielen, -strategien und -risiken zu erlangen, soweit dies für die RMS-Prüfung relevant ist (vgl. Tz. 46 f.).

52 Das zu erlangende Verständnis muss – unter Berücksichtigung der in Abschn. 7.3.2 dargestellten Prüfungshandlungen – ausreichen, um die Risiken wesentlicher Fehler in der RMS-Beschreibung bzw. für wesentliche Mängel des in der RMS-Beschreibung dargestellten RMS (vgl. Tz. A44) festzustellen und zu beurteilen. Das erlangte Verständnis muss zudem eine angemessene Grundlage bilden für die Planung und Durchführung von Prüfungshandlungen als Reaktion auf die festgestellten und beurteilten Risiken und zur Erlangung hinreichender Sicherheit für die Bildung des Prüfungsurteils.

[13] Vgl. § 38 Abs. 1 BS WP/vBP.

[14] Vgl. *IDW EQS 1*, Tz. 107 ff., 133 ff.

7.3.2. Gewinnung eines Verständnisses von dem in der RMS-Beschreibung dargestellten Risikomanagementsystem

53 Der RMS-Prüfer muss ein angemessenes Verständnis von dem in der RMS-Beschreibung dargestellten RMS erlangen. Hierzu gehört, dass sich der RMS-Prüfer u.a. durch Befragungen ein angemessenes Verständnis von den Verantwortlichkeiten sowie über die Prozesse zur Aufstellung der RMS-Beschreibung verschafft. Im Rahmen der Prüfung eines abgegrenzten Teilbereichs des operativen RMS hat sich der Prüfer auch mit dem RMS in Bezug auf strategische Risiken zu befassen (einschließlich der Ableitung der operativen Ziele aus den relevanten strategischen Unternehmenszielen) (vgl. Tz. A47 f.).

54 Der RMS-Prüfer hat Befragungen der gesetzlichen Vertreter sowie weiterer geeigneter Personen im Unternehmen durchzuführen,

- ob diese Personen Kenntnisse über vorliegende, vermutete oder behauptete bewusst falsche Angaben in der RMS-Beschreibung oder über Mängel des RMS haben,
- ob das Unternehmen über eine Interne Revision verfügt; falls eine solche eingerichtet ist, sind weitere Befragungen durchzuführen, um sich ein Verständnis von den Aktivitäten und Feststellungen der Internen Revision in Bezug auf das zu prüfende RMS zu machen (vgl. Tz. 71 f.) und
- ob das Unternehmen Sachverständige bei der Konzeption des RMS oder der Erstellung der RMS-Beschreibung eingesetzt hat (vgl. Tz. 70).

7.3.3. Identifizierung und Beurteilung der Risiken wesentlicher Fehler in der RMS-Beschreibung

55 Der RMS-Prüfer muss auf der Grundlage des gewonnenen Verständnisses von dem Unternehmen und von dessen rechtlichem und wirtschaftlichem Umfeld sowie von dem zu prüfenden RMS die Risiken wesentlicher Fehler in der RMS-Beschreibung identifizieren und beurteilen. Auf dieser Grundlage hat der RMS-Prüfer weitere Prüfungshandlungen zur Prüfung der Angemessenheit und ggf. der Wirksamkeit des RMS zu planen und durchzuführen.

56 Sofern der RMS-Prüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die mit den Prüfungsnachweisen nicht in Einklang stehen, auf die er seine Risikobeurteilung ursprünglich gestützt hat, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren.

8. Prüfungsdurchführung

8.1. Prüfung der Ausgestaltung und Aktualität der RMS-Beschreibung

57 Der RMS-Prüfer hat die Ausgestaltung und Aktualität der der Prüfung zugrunde liegenden RMS-Beschreibung zu beurteilen. Hinsichtlich der Ausgestaltung der RMS-Beschreibung hat der RMS-Prüfer zu beurteilen, ob die von den gesetzlichen Vertretern erstellte RMS-Beschreibung die Regelungen zum Aufbau und zur Funktionsweise des RMS vollständig und richtig sowie in einer für die Adressaten verständlichen Art und Weise darstellt (vgl. Tz. A12). Hierzu zählen auch die bei der Ausgestaltung des RMS angewandten RMS-Grundsätze. Die Prüfung der Vollständigkeit umfasst auch, ob die Aussagen der gesetzlichen Vertreter zu den

Regelungen des RMS auf sämtliche der in Tz. 31 genannten Grundelemente eines RMS eingehen.

58 Hinsichtlich der Aktualität der RMS-Beschreibung ist festzustellen, ob die RMS-Beschreibung dem zu prüfenden Stand des RMS entspricht oder ob zwischenzeitlich Änderungen vorgenommen wurden, die aus Sicht des RMS-Prüfers als wesentlich zu erachten sind. Soweit dies der Fall ist, hat der RMS-Prüfer die gesetzlichen Vertreter aufzufordern, die RMS-Beschreibung entsprechend anzupassen.

59 Im Falle einer Wirksamkeitsprüfung hat der RMS-Prüfer zu beurteilen, ob die RMS-Beschreibung auf wesentliche Veränderungen im RMS bezogen auf den Betrachtungszeitraum gesondert eingeht.

8.2. Prüfung der in der RMS-Beschreibung enthaltenen Aussagen zur Angemessenheit und Wirksamkeit des RMS

8.2.1. Angemessenheit des RMS

60 Der RMS-Prüfer hat die Ergebnisse seiner Risikobeurteilungen zu analysieren und bei den weiteren Prüfungshandlungen zu berücksichtigen. Wenn dem RMS-Prüfer bereits anlässlich der Prüfungshandlungen zur Gewinnung eines Verständnisses von dem zu prüfenden RMS und der RMS-Beschreibung wesentliche Fehler bzw. Mängel bekannt werden, kann er zu dem Ergebnis gelangen, dass das dargestellte RMS nicht angemessen ausgestaltet ist. In diesem Fall erübrigen sich weitere Prüfungshandlungen zur Angemessenheit und Wirksamkeit des RMS.

61 Im Rahmen der Prüfung der Angemessenheit des RMS hat der RMS-Prüfer zu beurteilen, ob die in der RMS-Beschreibung des Unternehmens dargestellten Regelungen so ausgestaltet und implementiert sind, dass sie in Übereinstimmung mit den angewandten RMS-Grundsätzen geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken rechtzeitig zu identifizieren, zu bewerten und entsprechend den vom Unternehmen festgelegten Zielen des RMS zu steuern und zu überwachen (vgl. Tz. A49).

62 Der RMS-Prüfer hat durch die Kombination von Befragungen mit anderen Prüfungshandlungen, einschließlich Beobachtung sowie Einsichtnahme in Aufzeichnungen und Dokumente, festzustellen, ob das RMS wie beschrieben zu einem bestimmten Zeitpunkt eingerichtet (implementiert) ist (vgl. Tz. A50).

8.2.2. Wirksamkeit des RMS

63 Die Prüfung der Wirksamkeit des RMS zielt zusätzlich auf die Beurteilung ab, ob die in der RMS-Beschreibung dargestellten Regelungen innerhalb des gesamten zu prüfenden Zeitraums wie vorgesehen eingehalten wurden (vgl. Tz. A51 ff.).

64 Die Beurteilung der Kontinuität der Beachtung der in der RMS-Beschreibung dargestellten Regelungen erfordert es, dass die Prüfung der Wirksamkeit einen angemessenen Zeitraum abdeckt, z.B. ein Geschäftsjahr (vgl. Tz. A52).

65 Sofern Prüfungshandlungen zur Beurteilung der Wirksamkeit der in der RMS-Beschreibung dargestellten Regelungen zu einem vorgezogenen Zeitpunkt durchgeführt werden, sind wei-

tere Prüfungsnachweise zur Beurteilung der Wirksamkeit bis zum Ende des zu prüfenden Zeitraums einzuholen.

8.3. Weitere Prüfungshandlungen

8.3.1. Verwertung der Arbeit von Sachverständigen des Prüfers

66 Wenn die Beurteilung bedeutsamer Sachverhalte besondere Sachkenntnisse erfordert, um angemessene und ausreichende Prüfungsnachweise zu erlangen, hat der RMS-Prüfer zu entscheiden, ob Sachverständige hinzuzuziehen sind (vgl. Tz. A62).

67 Beim Einsatz von internen Sachverständigen des Prüfers unterliegen diese dem Qualitätssicherungssystem der WP-Praxis. Der RMS-Prüfer hat die internen Sachverständigen angemessen anzuleiten und zu überwachen.

68 Wenn die Arbeiten eines externen Sachverständigen des Prüfers verwertet werden sollen, hat der Prüfer

- zu beurteilen, ob der Sachverständige über die Kompetenz, die Fähigkeiten und die Objektivität verfügt, die für die Zwecke der RMS-Prüfung notwendig sind. Die Beurteilung der Objektivität des Sachverständigen umfasst u.a. eine Befragung zu möglichen Interessen und Beziehungen, die eine Gefährdung der Objektivität des Sachverständigen hervorrufen können (vgl. Tz. A63),
- ein ausreichendes Verständnis von dem Fachgebiet des Sachverständigen zu erlangen,
- mit dem Sachverständigen Art, Umfang und Ziele der Arbeit für die Zwecke der RMS-Prüfung zu vereinbaren und
- die Angemessenheit der Arbeit des Sachverständigen für die Zwecke der Prüfung des RMS zu beurteilen (vgl. Tz. A64 f.).

8.3.2. Verwertung der Arbeit anderer Wirtschaftsprüfer

69 Plant der RMS-Prüfer die Verwertung der Arbeit eines anderen Wirtschaftsprüfers, hat er zu beurteilen, ob dessen Arbeit für seine Zwecke geeignet ist (vgl. Tz. A66).

8.3.3. Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter

70 Sollen Informationen, die unter Verwendung der Tätigkeit eines Sachverständigen der gesetzlichen Vertreter erstellt wurden, als Prüfungsnachweise verwendet werden, muss der RMS-Prüfer, soweit notwendig, unter Berücksichtigung der Bedeutung der Tätigkeit des Sachverständigen für die Zwecke des RMS-Prüfers (vgl. Tz. 22 ff.)

- die Kompetenz, Fähigkeiten und Objektivität des Sachverständigen beurteilen,
- ein ausreichendes Verständnis von der Tätigkeit des Sachverständigen gewinnen und
- die Angemessenheit der Tätigkeit des Sachverständigen als Prüfungsnachweis beurteilen (vgl. Tz. A66).

8.3.4. Verwendung der Arbeit der Internen Revision

71 Plant der RMS-Prüfer, Arbeiten der Internen Revision zu verwenden, hat er Folgendes zu beurteilen:

- inwieweit die organisatorische Stellung und die Arbeitsweise die notwendige Objektivität der internen Revisoren gewährleisten,
- ob die notwendige fachliche Kompetenz der Internen Revision vorhanden ist,
- ob die Arbeiten der Internen Revision mit einer systematischen Vorgehensweise und mit der notwendigen berufsüblichen Sorgfalt (einschließlich qualitätssichernder Maßnahmen) durchgeführt werden und
- ob die Arbeiten der Internen Revision für Zwecke der Prüfung des RMS angemessen sind (vgl. Tz. A66 f.).

72 Für die Frage, inwieweit sich die Arbeiten der Internen Revision auf die Art, den Umfang und den Zeitpunkt der eigenen Prüfungshandlungen auswirken, hat der Prüfer Folgendes zu berücksichtigen:

- Art und Umfang der Revisionstätigkeiten (sowohl durchgeführte als auch noch durchzuführende)
- Relevanz der Revisionstätigkeit für die eigene Prüfung
- Nachvollziehbarkeit der Revisionsergebnisse
- die Art, den Umfang und die Ergebnisse einer Prüfung nach *IDW PS 983*.

8.3.5. Ereignisse nach dem Beurteilungszeitpunkt/-zeitraum

73 Der RMS-Prüfer hat die Auswirkungen von Ereignissen nach dem Zeitpunkt bzw. Zeitraum, auf den sich die Aussagen in der RMS-Beschreibung beziehen, bis zum Datum des RMS-Prüfungsberichts zu würdigen (vgl. Tz. A68).

74 Der RMS-Prüfer ist nicht verpflichtet, Prüfungshandlungen nach dem Datum des RMS-Prüfungsberichts durchzuführen oder Prüfungshandlungen durchzuführen, um Ereignisse festzustellen, die nicht den Prüfungszeitraum betreffen.

75 Falls dem RMS-Prüfer nach dem Datum des RMS-Prüfungsberichts bis zur Auslieferung des Berichts Sachverhalte bekannt werden, die auf Mängel oder bedeutsame zwischenzeitliche Änderungen im RMS hindeuten, auf die in der RMS-Beschreibung nicht eingegangen wird, hat er auf eine Änderung der RMS-Beschreibung durch das Unternehmen hinzuwirken. Unterbleibt eine Änderung, hat er zu untersuchen, ob weitere Prüfungshandlungen vorzunehmen sind, um festzustellen, ob die betreffenden Sachverhalte eine Auswirkung auf sein Prüfungsurteil haben. Des Weiteren kann es erforderlich sein, die Adressaten der Berichterstattung hierüber zu informieren.

76 Werden dem RMS-Prüfer nach dem Datum der Auslieferung des RMS-Prüfungsberichts Sachverhalte bekannt, die dazu führen, dass das Prüfungsurteil in der erteilten Form nicht hätte abgegeben werden dürfen, hat er angemessene Maßnahmen zu ergreifen, damit die Adressaten hiervon Kenntnis erlangen. Die Einholung rechtlichen Rats kann angezeigt sein.

8.3.6. Sonstige Angaben in der RMS-Beschreibung

77 Enthält die RMS-Beschreibung sonstige Angaben, die nicht Gegenstand der Auftragsvereinbarung (vgl. Tz. A33 ff.) sind (z.B. Angaben in Bezug auf nicht zu prüfende Teilbereiche des RMS oder Angaben zur Wirksamkeit des RMS bei einer Angemessenheitsprüfung), hat der RMS-Prüfer darauf hinzuwirken, dass die gesetzlichen Vertreter diese Angaben in der RMS-Beschreibung unterlassen oder diese Angaben eindeutig von den prüfungsrelevanten Angaben der RMS-Beschreibung abgrenzen.

78 Es liegt im Ermessen des RMS-Prüfers, ob die sonstigen Angaben in die Prüfung einbezogen werden.

79 Der RMS-Prüfer hat die nicht geprüften sonstigen Angaben im RMS-Prüfungsbericht zu benennen und darauf hinzuweisen, dass sie nicht geprüft wurden und sich daher das Prüfungsurteil nicht darauf erstreckt. Nicht in die Prüfung einbezogene sonstige Angaben hat der RMS-Prüfer jedoch kritisch zu lesen, um ggf. bestehende wesentliche Unstimmigkeiten gegenüber den geprüften Aussagen in der RMS-Beschreibung festzustellen.

80 Falls der RMS-Prüfer beim kritischen Lesen der sonstigen Angaben

- eine wesentliche Unstimmigkeit zwischen den sonstigen Angaben und den geprüften Aussagen in der RMS-Beschreibung oder den Aussagen im RMS-Prüfungsbericht feststellt oder
- wesentliche offensichtliche Fehler in den sonstigen Angaben feststellt, die nicht mit den geprüften Aussagen in der RMS-Beschreibung und den Aussagen im RMS-Prüfungsbericht zusammenhängen,

hat er den Sachverhalt mit den gesetzlichen Vertretern zu erörtern und, sofern angebracht, weitere angemessene Maßnahmen zu ergreifen (vgl. Tz. A69).

81 Hat der RMS-Prüfer festgestellt, dass die Klarheit und Übersichtlichkeit der RMS-Beschreibung durch die sonstigen Angaben, die nicht Gegenstand der Prüfung sind, wesentlich beeinträchtigt ist, hat er das Prüfungsurteil einzuschränken oder zu versagen.

8.3.7. Schriftliche Erklärungen

82 Der RMS-Prüfer hat vor Abschluss der Prüfung von den gesetzlichen Vertretern eine Vollständigkeitserklärung einzuholen, in der bestätigt wird, dass die RMS-Beschreibung auf der Grundlage der angewandten RMS-Grundsätze vollständig und richtig ist und dem Prüfer, wie in den Auftragsbedingungen vereinbart, alle relevanten Erklärungen und Nachweise zur Angemessenheit, Implementierung und ggf. Wirksamkeit des RMS erteilt worden sind. Dazu gehört auch die Zusicherung, dass die gesetzlichen Vertreter dem RMS-Prüfer vollständig die folgenden ihnen bekannten Aspekte mitgeteilt haben:

- Mängel in Bezug auf die Angemessenheit des RMS
- Fälle, in denen die Regelungen des RMS nicht, wie in der RMS-Beschreibung dargestellt, durchgeführt wurden
- geplante bedeutsame Änderungen im RMS

- Ereignisse, die nach dem Prüfungszeitraum, aber vor dem Datum des RMS-Prüfungsberichts eingetreten sind und eine erhebliche Auswirkung auf die Aussagen in der RMS-Beschreibung haben können (vgl. Tz. A70).

83 Über die Einholung der Vollständigkeitserklärung hinaus kann es notwendig sein, weitere schriftliche Erklärungen zu erlangen, um andere für die RMS-Beschreibung relevante Prüfungsnachweise zu stützen.

84 Sofern sich einzelne Aspekte der Vollständigkeitserklärung oder weiterer schriftlicher Erklärungen auf Sachverhalte beziehen, die wesentlich für die in der RMS-Beschreibung dargestellten Aussagen sind, muss der RMS-Prüfer

- die Begründetheit dieser Erklärung(en) und deren Konsistenz zu anderen erlangten Nachweisen, einschließlich anderer mündlicher oder schriftlicher Erklärungen der gesetzlichen Vertreter, beurteilen und
- abwägen, ob zu erwarten ist, dass die Personen, welche die schriftlichen Erklärungen abgeben, in Bezug auf die betreffenden Sachverhalte ausreichend informiert sind.

85 Die Vollständigkeitserklärung muss zeitnah zum Datum des RMS-Prüfungsberichts, darf aber nicht nach diesem datiert werden.

86 Weigern sich die gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben, oder bestehen begründete Zweifel in Bezug auf die Kompetenz oder die Integrität der Personen, welche die Vollständigkeitserklärung abgeben, bzw. bestehen andere begründete Zweifel, dass die erteilte Erklärung verlässlich ist, ist darin ein Prüfungshemmnis zu sehen. In diesem Fall hat der RMS-Prüfer im Prüfungsbericht darauf hinzuweisen, dass ein Prüfungsurteil nicht erteilt wird.

Beziehen sich die Zweifel auf andere vom RMS-Prüfer angeforderte schriftliche Erklärungen, hat der RMS-Prüfer den Sachverhalt mit den Verantwortlichen zu erörtern, die Auswirkungen auf die Verlässlichkeit der bereits eingeholten Prüfungsnachweise zu würdigen und, sofern angebracht, weitere Maßnahmen zu ergreifen, einschließlich der Feststellung möglicher Auswirkungen auf das Prüfungsurteil.

8.4. Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils

87 Der RMS-Prüfer muss würdigen, ob ausreichende und angemessene Prüfungsnachweise als Grundlage für die Beurteilung der Aussagen in der RMS-Beschreibung über die Angemessenheit, Implementierung bzw. Wirksamkeit des RMS erlangt wurden. Ist dies der Fall, hat der RMS-Prüfer die Prüfungsfeststellungen auszuwerten und auf dieser Grundlage ein Prüfungsurteil zu treffen.

88 Bei der Bildung des Prüfungsurteils hat der RMS-Prüfer zu würdigen, ob nicht korrigierte Fehler in der RMS-Beschreibung bzw. festgestellte Mängel in dem in der RMS-Beschreibung dargestellten RMS einzeln oder in der Summe wesentlich sind. Hierbei hat der RMS-Prüfer alle relevanten Prüfungsnachweise zu berücksichtigen, unabhängig davon, ob sie dem Anschein nach die Aussagen in der RMS-Beschreibung bestätigen oder ihnen widersprechen (vgl. Tz. A71).

89 Bestehen keine wesentlichen Beanstandungen in Bezug auf die RMS-Beschreibung bzw. die in der RMS-Beschreibung dargestellten Regelungen, hat der RMS-Prüfer ein uneinge-

schränktes Prüfungsurteil abzugeben. Liegen wesentliche Beanstandungen vor, ist das Prüfungsurteil einzuschränken oder zu versagen.

90 Das Prüfungsurteil ist wegen eines Fehlers in der RMS-Beschreibung oder eines Mangels in dem in der RMS-Beschreibung dargestellten RMS einzuschränken, wenn der Fehler bzw. Mangel zwar wesentlich, aber nicht umfassend ist. Sind die Beanstandungen nicht auf bestimmte Teile der in der RMS-Beschreibung enthaltenen Aussagen einzugrenzen, z.B. weil aufgrund von Mängeln bei der Konzeption des RMS oder einer unangemessenen Risikokultur die dargestellten Regelungen des RMS insgesamt als nicht angemessen anzusehen sind, ist das Prüfungsurteil zu versagen.

91 Ist der RMS-Prüfer nicht in der Lage, angemessene und ausreichende Prüfungsnachweise zu erlangen, liegt ein Prüfungshemmnis vor. In diesem Fall ist das Prüfungsurteil einzuschränken, wenn die Auswirkungen des Prüfungshemmnisses zwar die Beurteilung eines wesentlichen Teils der Aussagen in der RMS-Beschreibung ausschließen, eine Beurteilung insgesamt aber noch möglich ist. Kann aufgrund von Prüfungshemmnissen auch nach Ausschöpfung der prüferischen Möglichkeiten ein Urteil nicht abgegeben werden, ist in der Berichterstattung des RMS-Prüfers darauf hinzuweisen, dass ein Prüfungsurteil nicht erteilt wird.

92 Falls sich im Verlauf der Prüfung herausstellt, dass sich die RMS-Beschreibung nicht für eine Prüfung eignet oder sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthält, die eine Irreführung der Berichtsadressaten zur Folge haben können, hat der RMS-Prüfer zunächst auf eine entsprechende Änderung der RMS-Beschreibung hinzuwirken. Unterbleibt eine Änderung, hat er abzuwägen, ob das Prüfungsurteil einzuschränken oder zu versagen ist. Wenn sich im Verlauf der Prüfung herausstellt, dass die zu prüfenden Teilbereiche von den gesetzlichen Vertretern irreführend festgelegt wurden oder die angewandten RMS-Grundsätze nicht geeignet sind, hat der RMS-Prüfer das Prüfungsurteil zu versagen.

93 Einschränkungen, Versagungen oder Nichterteilungen des Prüfungsurteils sind klar durch die Verwendung des Begriffs „Einschränkung“ bzw. „Versagung“ oder „Nichterteilung“ zu kennzeichnen. Die Gründe für die Einschränkung bzw. Versagung oder die Nichterteilung des Prüfungsurteils sind vollständig und eindeutig im RMS-Prüfungsbericht darzustellen.

94 Hält der RMS-Prüfer es für notwendig, die Berichtsadressaten auf einen in der RMS-Beschreibung enthaltenen Sachverhalt aufmerksam zu machen, der nach der Beurteilung des RMS-Prüfers grundlegend für das Verständnis der RMS-Beschreibung durch die Berichtsadressaten ist, muss der RMS-Prüfer einen Hinweis zur Hervorhebung des Sachverhalts in den RMS-Prüfungsbericht aufnehmen. Dieser Hinweis darf sich nur auf in der RMS-Beschreibung angegebene Informationen beziehen.

95 Darüber hinaus hat der RMS-Prüfer auf sonstige Sachverhalte hinzuweisen, auch wenn diese nicht in der RMS-Beschreibung dargestellt sind, wenn dies nach der Beurteilung des RMS-Prüfers für die Berichtsadressaten zum Verständnis des Prüfungsauftrags, der Verantwortung des RMS-Prüfers oder zum Verständnis des RMS-Prüfungsberichts erforderlich ist. Ein Hinweis auf sonstige Sachverhalte ist – ebenso wie ein Hinweis zur Hervorhebung eines Sachverhalts nach Tz. 94 – klar zu kennzeichnen und es ist klarzustellen, dass das Prüfungsurteil im Hinblick auf den entsprechenden Sachverhalt nicht eingeschränkt oder versagt wird (vgl. Tz. A72).

9. Dokumentation

96 Der RMS-Prüfer hat die zur Stützung seines Prüfungsurteils dienenden Prüfungsnachweise in angemessener Zeit in den Arbeitspapieren zu dokumentieren.

97 Form und Inhalt der Dokumentation stehen im pflichtgemäßen Ermessen des RMS-Prüfers. Die Arbeitspapiere sind so anzulegen, dass sich ein erfahrener Wirtschaftsprüfer, der nicht mit der Prüfung befasst war, in angemessener Zeit ein Bild über die Abwicklung und Ergebnisse der Prüfung machen kann.

98 Anhand der Dokumentation muss ein erfahrener Wirtschaftsprüfer folgende Punkte in angemessener Zeit nachvollziehen können (vgl. Tz. A73):

- Einhaltung der Berufspflichten (insb. zum Grundsatz der Unabhängigkeit einschließlich möglicher Unabhängigkeitsgefährdungen und deren Lösung)
- Art, Zeitpunkte und Umfang der durchgeführten Prüfungshandlungen
- die Ergebnisse der Prüfungshandlungen und die erlangten Prüfungsnachweise
- bedeutende Sachverhalte, die während der Prüfung aufgetreten sind, sowie daraus resultierende bedeutsame Schlussfolgerungen und Beurteilungen.

99 Im Rahmen der Dokumentation von Art, Umfang und Zeitpunkten der Prüfungshandlungen hat der RMS-Prüfer aufzuzeichnen,

- welche Prüfungsnachweise zur Angemessenheit und Wirksamkeit des RMS erlangt wurden nebst deren eindeutiger Bezeichnung,
- von wem die Prüfungshandlungen durchgeführt und wann sie abgeschlossen wurden,
- von wem und wann die Prüfungshandlungen kontrolliert wurden sowie den Inhalt dieser Überprüfung.

100 Soweit der RMS-Prüfer bestimmte Arbeiten der Internen Revision oder von Sachverständigen verwertet, hat er dies zu dokumentieren. Hiervon umfasst ist die Dokumentation seiner Beurteilungsergebnisse sowie seiner in diesem Zusammenhang durchgeführten Prüfungshandlungen.

101 Erhält der RMS-Prüfer Informationen, die einer zuvor erfolgten abschließenden Beurteilung eines bedeutsamen Prüfungssachverhalts entgegenstehen, hat er die in diesem Zusammenhang ergriffenen Maßnahmen (z.B. die Durchführung zusätzlicher Prüfungshandlungen) zu dokumentieren.

102 Der Abschluss der Auftragsdokumentation hat innerhalb eines angemessenen Zeitraums nach dem Datum des RMS-Prüfungsberichts zu erfolgen. Die Löschung bzw. das Entfernen von Dokumentationen ist nach der abschließenden Zusammenstellung der Arbeitspapiere und finalen Auftragsdokumentation vor dem Ablauf der Aufbewahrungsfrist unzulässig.

103 Für den Fall, dass der RMS-Prüfer es für notwendig erachtet, die Auftragsdokumentation nach der abschließenden Zusammenstellung zu ändern oder zu ergänzen, und dies keine Auswirkungen auf den RMS-Prüfungsbericht hat, ist Folgendes zu dokumentieren:

- Die Gründe für die Änderungen bzw. Ergänzungen und
- von wem sie wann durchgeführt und
- von wem sie wann durchgesehen wurden.

10. Berichterstattung des RMS-Prüfers

10.1. RMS-Prüfungsbericht

104 Der RMS-Prüfer hat einen schriftlichen RMS-Prüfungsbericht zu verfassen, der ein Prüfungsurteil über die in der RMS-Beschreibung getroffenen Aussagen enthält bzw. erforderlichenfalls eine Aussage enthält, dass ein Prüfungsurteil nicht erteilt werden kann.

105 Im RMS-Prüfungsbericht ist das Prüfungsurteil von anderen Informationen und Erläuterungen (z.B. Hervorhebungen und Hinweisen (vgl. Tz. 94 f.) oder von Feststellungen und Empfehlungen zum RMS, die keinen Einfluss auf das Urteil haben), klar zu trennen.

106 Der RMS-Prüfungsbericht muss folgende Bestandteile enthalten:

a. Überschrift: Angabe, dass es sich um den Bericht eines unabhängigen Wirtschaftsprüfers handelt

b. Berichtsadressaten

c. Prüfungsauftrag

d. Beschreibung des zu prüfenden RMS

e. Darstellung der oder Bezugnahme auf die vom Unternehmen angewandten RMS-Grundsätze

f. Gegenstand, Art und Umfang der Prüfung einschließlich einer zusammenfassenden Beschreibung der durchgeführten Prüfungshandlungen (Prüfungshandlungen zur Risikobeurteilung, Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen) einschließlich der Klarstellung, dass es sich um einen Auftrag zur Erlangung hinreichender Sicherheit über die in der RMS-Beschreibung enthaltenen Aussagen über das RMS handelt

g. Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter und des RMS-Prüfers

h. Aussage, dass die Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* durchgeführt wurde; der RMS-Prüfer darf nicht die Einhaltung dieses *IDW Prüfungsstandards* erklären, wenn er nicht sämtliche einschlägigen Anforderungen beachtet hat

i. Aussage, dass bei der Prüfung die Berufspflichten der WPO und der Berufssatzung WP/vBP, einschließlich der Anforderungen an die Unabhängigkeit, eingehalten werden und dass die WP-Praxis die Anforderungen an die Qualitätssicherung anwendet

j. Feststellungen zum RMS und ggf. Empfehlungen

k. falls relevant:
   - Beschreibung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands
   - Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke ausgeschlossen ist
   - ggf. Hinweis auf nicht geprüfte sonstige Angaben in der RMS-Beschreibung (vgl. Tz. 77 ff.)

l. zusammenfassendes Prüfungsurteil

   - Urteil, ob die im geprüften Zeitraum implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des geprüften Zeitraums wirksam waren.
   - sofern sich die Prüfung nur auf die Aussagen zur Angemessenheit und Implementierung des RMS bezieht (Angemessenheitsprüfung): Urteil, ob die zu einem bestimmten Zeitpunkt implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und ob die dargestellten Regelungen in allen wesentlichen Belangen zu einem bestimmten Zeitpunkt implementiert waren.
   - Wird das Prüfungsurteil eingeschränkt oder versagt bzw. nicht erteilt, sind die Gründe für die Einschränkung, Versagung oder Nichterteilung in einem gesonderten Abschnitt des RMS-Prüfungsberichts darzustellen. Gleiches gilt für Hervorhebungen und Hinweise.

m. eine Aussage über die inhärenten Grenzen des RMS und zum Risiko, die Feststellungen zum RMS auf die Zukunft zu übertragen.

n. Datum des RMS-Prüfungsberichts: Das Datum darf nicht vor dem Datum liegen, an dem der RMS-Prüfer ausreichende und angemessene Nachweise als Grundlage für das Prüfungsurteil über das RMS erlangt hat.

o. Unterschrift, Name und Ort des Prüfers.

107 Da die freiwillige Prüfung von RMS keine Vorbehaltsaufgabe i.S.d. § 48 Abs. 1 Satz 1 WPO ist, besteht keine Pflicht zur Führung des Siegels.

108 Wenn der RMS-Prüfer auf die Arbeit eines Sachverständigen des RMS-Prüfers (vgl. Tz. 66 ff.) Bezug nimmt, darf nicht der Eindruck entstehen, dass die Verantwortung des RMS-Prüfers für das Prüfungsurteil durch diese Bezugnahme verringert wird.

109 Die RMS-Beschreibung der gesetzlichen Vertreter ist dem RMS-Prüfungsbericht als Anlage beizufügen. Sind in der Beschreibung auch nicht geprüfte Angaben enthalten, ist dies im RMS-Prüfungsbericht zu verdeutlichen (vgl. Tz. 79).

110 Beispiele für RMS-Prüfungsberichte finden sich in Anlage 2 zu diesem *IDW Prüfungsstandard*.

10.2. Weitere Berichtspflichten

111 Wenn nach der Einschätzung des RMS-Prüfers bestimmte Prüfungsfeststellungen eine unmittelbare Reaktion des Unternehmens erfordern, ist darüber vorab zu berichten.

112 Der RMS-Prüfer muss feststellen, ob ggf. weitere Berichtspflichten bestehen, z.B. gegenüber dem Aufsichtsorgan des Unternehmens. Im Falle einer Berichtspflicht ist diese im RMS-Prüfungsbericht oder in sonstiger geeigneter Weise zu erfüllen (vgl. Tz. A74).

Anwendungshinweise und sonstige Erläuterungen

Vorbemerkungen [Tz. 1 ff.]

A1 Die Vorschriften des § 111 AktG finden nicht nur auf die Aktiengesellschaft und die Kommanditgesellschaft auf Aktien (KGaA) (§ 278 Abs. 3 AktG), sondern nach § 25 Abs. 1 Satz 1 Nr. 2 MitbestG, § 3 Abs. 2 MontanMitbestG, § 3 Abs. 1 MitbestErgG, § 1 Abs. 1 Nr. 3 DrittelbG, § 24 Abs. 2 Satz 2 MgVG auch auf die mitbestimmte GmbH Anwendung. Auf die mitbestimmungsfreie GmbH findet § 111 AktG nach § 52 Abs. 1 GmbHG nur insoweit Anwendung, als im Gesellschaftsvertrag nicht etwas anderes bestimmt ist.

A2 Sollte es an den in Tz. 2 genannten wirksamen Systemen fehlen, obliegt dem Aufsichtsrat bzw. dem von ihm eingerichteten Prüfungsausschuss die Prüfung, ob der Verzicht zur Einrichtung entsprechender Systeme mit den Organisations- und Sorgfaltspflichten des Vorstands nach § 93 Abs. 1 Satz 1 AktG im Einklang steht.

A3 Die in Tz. 5 ausgeführte Systematisierung verschiedener (Teil-)Systeme der Corporate Governance setzt keine separate Aufbau- oder Ablauforganisation der genannten Systeme im Unternehmen voraus. In Abhängigkeit von Art, Umfang und Komplexität der Geschäftstätigkeit werden in der Praxis häufig integrierte Systeme entwickelt (vgl. Tz. A9). Darüber hinaus wird in der Praxis auch das Three-Lines-of-Defense Modell[15] verwendet, um die Rollen und Verantwortlichkeiten sowie die Abgrenzung der Funktionen der jeweiligen Corporate Governance Systeme untereinander zu beschreiben.

A4 Eine mögliche Abgrenzung von Teilbereichen für Zwecke der Prüfung in Bezug auf operative Risiken kann z.B. nach Unternehmensfunktionen oder -prozessen erfolgen:

a. Kategorisiert nach Risiken aus *Unternehmensfunktionen* (funktionale Sicht):
   - Risiken der *Beschaffung* (Supply-Chain)
     - Beschaffung von Produktionsfaktoren (Qualität, Verfügbarkeit)
     - Beschaffungslogistik
   - Risiken der *Produktion* (Produkte/technische Realisation), einschließlich der Sicherstellung der operativen Betriebsfortführung

[15] Das Three-Lines-of-Defense Modell wurde vom Dachverband der europäischen Revisionsinstitute (ECIIA) als Leitfaden zur Umsetzung der Abschlussprüferrichtlinie entwickelt, um die unterschiedlichen Rollen zur internen Steuerung und deren Zusammenspiel zu erklären und darzustellen. Es wurde mit Herausgabe eines umfangreichen Positionspapiers durch das Institute of Internal Auditors im Januar 2013 weltweit in seiner Bedeutung hervorgehoben – vgl. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (Stand: 13.03.2017).

   - Risiken aus der Produktion (z.B. Umwelt-/Gesundheitsgefährdung)
   - Qualitätsrisiken/Gewährleistungsrisiken
   - Wissensmanagement (Warenzeichen, Patente, Know-how)
 - Risiken des *Absatzes*
   - Marketing, Vertrieb, Distributionslogistik
   - Absatzportfoliosteuerung (Produkte, Leistungen)

sowie Risiken aus den Unterstützungsfunktionen: sowie Risiken aus den Unterstützungsfunktionen:

 - Rechnungswesen/Finanzwesen
   - Wachstumssteuerung (Investitionen)
   - Finanzierung (Liquidität, Marktpreis, Kreditsicherheit)
 - Personalwesen
   - Ressourcenplanung (Einstellung, Fluktuation, Ruhestand)
   - Mitarbeiterentwicklung (Ausbildung, Fortbildung, Förderung)
   - Nachfolgeplanung
 - IT-Betrieb
 - Sonstige Funktionen

b. Kategorisiert nach den Risiken aus diversen *Prozessen* (prozessuale Sicht):
   - Kernprozesse
     - Innovationsprozess/F&E
     - Beschaffungsprozess
     - Produktionsprozess
     - Vertriebsprozess
     - Vermarktung
   - Unterstützende Prozesse/Hilfsprozesse
     - Abrechnung
     - Qualitätssicherung
     - Personalprozesse
     - Mahnwesen
     - Investitionen
     - IT/Datenmanagement
     - Mergers & Acquisitions
     - Rechtsbereich/Legal
   - Management Prozesse
     - Qualitäts-, Umwelt- und Sicherheitspolitik
     - Budgetplanung
     - Ressourcenplanung
     - Personalplanung und -entwicklung
     - Projektmanagement (z.B. Management von Großprojekten).

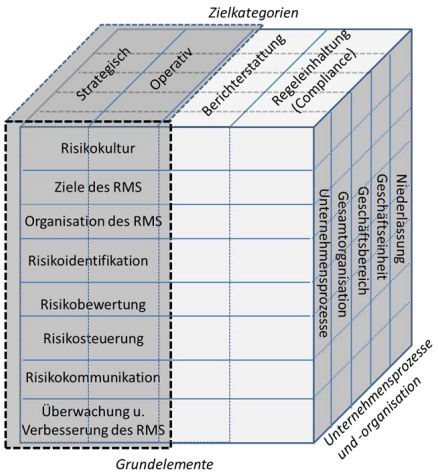

Abb. 1: Abgrenzung der Teilbereiche

A5 Die Prüfung des RMS i.S. dieses *IDW Prüfungsstandards* umfasst stets sämtliche Grundelemente des Risikomanagementprozesses (vgl. Tz. 31). Eine isolierte Prüfung in Bezug auf einzelne Grundelemente (z.B. nur die Prüfung des Grundelements Risikosteuerung, ohne zu berücksichtigen, wie das Unternehmen die Ziele des RMS festlegt oder Risiken identifiziert), liegt nicht im Anwendungsbereich dieses *IDW Prüfungsstandards*.

A6 Die strategischen Risiken stehen im Zusammenhang mit den für das Unternehmen und seine Geschäftsfelder vorhandenen und künftigen Erfolgspotenzialen. Strategische Risiken können z.B. aus falschen Geschäftsentscheidungen, mangelhafter Umsetzung von Entscheidungen oder mangelnder Anpassungsfähigkeit an Veränderungen in der Unternehmensumwelt hervorgehen.

A7 Für Zwecke der Prüfung kann eine Abgrenzung in Teilbereiche im Bereich der strategischen Risiken ausnahmsweise erfolgen, wenn strategische Risiken für einzelne Geschäftsfelder oder -bereiche isoliert und unabhängig von der Gesamtunternehmensstrategie betrachtet werden können. Eine solche Teilbereichsabgrenzung kann z.B. bei stark diversifizierten Unternehmen in Betracht kommen, bei denen eigenständige und daher getrennt zu betrachtende Geschäftsbereiche unter einer Finanzholding zusammengefasst werden.

Definitionen [Tz. 18 f.]

A8 Die in den Grundelementen des RMS zum Ausdruck kommenden Regelungen bilden in ihrer Gesamtheit das Risikomanagementsystem (vgl. Tz. 18f.).

A9 Der Begriff Risikomanagement (vgl. Tz. 18e.) ist unabhängig von der Bezeichnung der einzelnen Abteilungen und Funktionen im Unternehmen zu verstehen.

A10 Das RMS ist integraler Bestandteil der Corporate Governance des Unternehmens. Die Notwendigkeit zur Einrichtung einer eigenständigen Aufbau- und Ablauforganisation für das RMS ist abhängig von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens.

A11 Allgemein anerkannte Rahmenkonzepte i.S.d. Tz. 18j. werden – soweit nicht rechtlich vorgeschrieben – im Rahmen eines transparenten Verfahrens entwickelt, das die Veröffentlichung als Entwurf mit der Möglichkeit der Kommentierung durch Fachkreise und die interessierte Öffentlichkeit beinhaltet. Die in der Anlage 1 nicht abschließend aufgeführten Rahmenkonzepte genügen diesen Anforderungen.

A12 Die RMS-Beschreibung (vgl. Tz. 18k.) stellt die Konzeption des RMS und die implementierten Regelungen des RMS in einer für die Adressaten verständlichen Art und Weise dar. Hierbei werden sowohl hinsichtlich des Umfangs als auch der Konkretisierung die Ziele des RMS sowie Art und Umfang der Geschäftstätigkeit des Unternehmens angemessen berücksichtigt. Regelmäßig wird die RMS-Beschreibung eine Zusammenfassung der relevanten internen Verfahrensbeschreibungen enthalten. Die RMS-Beschreibung wird im Allgemeinen aber nicht den Umfang einer umfassenden Prozessbeschreibung haben (vgl. Tz. 21). Bei Verweisen innerhalb der RMS-Beschreibung auf andere Verfahrensbeschreibungen und Dokumente ist die RMS-Beschreibung aus sich heraus verständlich und enthält alle wesentlichen Regelungen.

A13 Ein Fehler in den Aussagen der RMS-Beschreibung (vgl. Tz. 18m.) kann z.B. vorliegen, wenn die RMS-Beschreibung

- nicht auf sämtliche Grundelemente eingeht,
- einen Mangel in dem in der RMS-Beschreibung dargestellten RMS nicht erkennen lässt oder
- unangemessene Verallgemeinerungen bzw. unausgewogene und verzerrende Darstellungen enthält.

A14 Unternehmen (vgl. Tz. 19) i.S. dieses *IDW Prüfungsstandards* können neben Unternehmen im rechtlichen Sinne auch Gesellschaften bürgerlichen Rechts, rechtsfähige bzw. nicht rechtsfähige Vereine, Stiftungen, Gebietskörperschaften, sonstige Körperschaften, Eigenbetriebe, Anstalten des öffentlichen Rechts, Gemeinschaften, natürliche Personen oder sonstige wirtschaftlich abgegrenzte Geschäftstätigkeiten (z.B. Standorte, selbstständige Teilbetriebe, Sparten) oder Gruppen dieser Einheiten sein.

Gegenstand, Ziel und Umfang der Prüfung [Tz. 20 ff.]

A15 Art und Umfang der gemäß Tz. 21 in der Verantwortung der gesetzlichen Vertreter liegenden Dokumentation des RMS sind abhängig von den Zielen und der Ausgestaltung des RMS,

dem rechtlichen und wirtschaftlichen Umfeld des Unternehmens und den mit der Dokumentation im Einzelnen verfolgten Zielen (z.B. Dokumentation zum Nachweis der Wirksamkeit des RMS gegenüber Dritten).

A16 Bei der Beurteilung, ob ein angemessen dokumentiertes RMS vorliegt, ist zu berücksichtigen, dass eine fehlende oder unvollständige Dokumentation des RMS zu Zweifeln an der dauerhaften Funktionsfähigkeit der eingerichteten Regelungen führen kann. Zum Nachweis der kontinuierlichen Anwendung der Regelungen empfiehlt es sich, auch die laufenden Unterlagen über die Feststellung von Risiken, deren Bewertung und Analyse sowie deren Kommunikation, die Einführung und Kommunikation der Regelungen zur Steuerung der Risiken und die Regelungen zur Überwachung und Verbesserung des Systems unbeschadet anderer Aufbewahrungspflichten über einen ausreichend langen Zeitraum aufzubewahren.

A17 Eine „projektbegleitende" RMS-Prüfung i.S.d. Tz. 25 stellt keine Mitwirkung an der Entwicklung oder Einrichtung eines RMS dar, durch die der RMS-Prüfer aufgrund der Unabhängigkeitsvorschriften von einer späteren Prüfung der Wirksamkeit des RMS ausgeschlossen wäre. Werden bei der Prüfungsdurchführung wesentliche Mängel in dem in der RMS-Beschreibung dargestellten RMS erkannt, ist es mit der Stellung eines RMS-Prüfers vereinbar, Entscheidungsempfehlungen über notwendige Regelungen zur Ausgestaltung eines angemessenen RMS zu geben. Die Entscheidung über deren Annahme verbleibt beim Unternehmen. Entscheidungen über deren Umsetzung dürfen nicht vom RMS-Prüfer veranlasst werden.

A18 Hinreichende Sicherheit bedeutet nicht absolute Sicherheit: Auch ein wirksames RMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, auftreten können, ohne systemseitig rechtzeitig erkannt und entsprechend den vom Unternehmen festgelegten Zielen des RMS gesteuert zu werden. Diese systemimmanenten Grenzen ergeben sich u.a. aus menschlichen Fehlleistungen (bspw. infolge von Nachlässigkeit, Ablenkungen, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen), Missbrauch oder Vernachlässigung der Verantwortung durch für bestimmte Maßnahmen verantwortliche Personen, der Umgehung oder Außerkraftsetzung von Kontrollen durch Zusammenwirken zweier oder mehrerer Personen oder dem Verzicht des Managements auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen.

A19 Gemäß Tz. 29 ist die Wirksamkeit des RMS dann gegeben, wenn die Regelungen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung in einem bestimmten Zeitraum wie vorgesehen eingehalten wurden. Der Kreis der „Betroffenen" ist nicht notwendigerweise auf die vom Unternehmen beschäftigten Mitarbeiter begrenzt (z.B. bei ausgelagerten Dienstleistungen oder Geschäftsprozessen).

Grundelemente eines RMS [Tz. 31]

A20 Während die Grundelemente den Prozess für die Einrichtung eines RMS allgemein (als Referenzrahmen) beschreiben, werden durch die RMS-Grundsätze (vgl. Tz. 18i.) konkrete inhaltliche Anforderungen an das System definiert, die bei der Einrichtung zugrunde gelegt werden.

Risikokultur

A21 Die Risikokultur wird geprägt von der grundsätzlichen Einstellung und den Verhaltensweisen beim Umgang mit Chancen- und Risikosituationen sowohl im täglichen Geschäft als auch bei bedeutsamen unternehmerischen Entscheidungen.

Im Unternehmen wird die Risikokultur z.B. durch folgende Merkmale beeinflusst:

- Vorgaben durch die Unternehmensleitung in Form von Verhaltensgrundsätzen/Code of Conduct, ergänzt durch einen regelmäßig zum Ausdruck gebrachten „tone from the top" sowie konsequente Ausrichtung der persönlichen Verhaltensweisen an den vorgegebenen Prinzipien
- Förderung eines umfassenden Risikobewusstseins über die Gesamtorganisation hinweg sowie einer offenen Kommunikation von erkannten Risikoentwicklungen
- Gelebtes Verhalten der Unternehmensleitung durch Berücksichtigung von Risiken (einschließlich deren Zusammenhängen und Auswirkungen) bei unternehmerischen Entscheidungen sowie bei Eintritt kritischer Risikosituationen, wie bspw. Krisenereignissen oder wirtschaftlichen Problemen
- Differenzierung der Risikobereitschaft unter Berücksichtigung der Erwartungen der Stakeholder und der externen Rahmenbedingungen, bspw. „zero tolerance" bei der Beachtung von Integrität und ethischen Werten vs. höhere Risikobereitschaft beim Eintritt in neue Märkte oder bei der Einführung innovativer Produkte und Technologien – gepaart mit entsprechenden Maßnahmen zur Risikosteuerung
- Verankerung in den Regelungen zur Zusammenarbeit von Unternehmensleitung und Aufsichtsgremien, bspw. durch die Definition von zustimmungspflichtigen Geschäften und regelmäßigen Informationen an das Aufsichtsgremium
- Verknüpfung mit Anreiz-, Leistungsbeurteilungs- und Mitarbeiterentwicklungssystemen zur Förderung einer positiven Risikokultur und Sanktionierung von unerwünschtem Verhalten.

Ziele des RMS

A22 Aus der Risikokultur, der Unternehmensstrategie und den Unternehmenszielen werden die Ziele des RMS abgeleitet und in einer Risikostrategie formuliert. Diese umfasst bspw. die folgenden Bestandteile:

„*Risikoappetit*" beschreibt die grundsätzliche Bereitschaft, zur Erreichung angestrebter Ziele und Wertsteigerungen damit verbundene Risiken einzugehen. Aus dem Risikoappetit wird – unter Beachtung der Unternehmensstrategie – für das RMS eine „*Risikotoleranz*" festgelegt. Die Risikotoleranz ist die maximal tolerierte Abweichung in Bezug auf die angestrebte Zielsetzung. Diese wird i.d.R. in Form konkreter quantitativer Wesentlichkeitsgrenzen oder auch qualitativer Kriterien umgesetzt, welche meist mit dem gleichen Maßstab wie die Zielerreichung gemessen werden.

Die Ziele des RMS werden in Verbindung mit dem Strategie- und Planungsprozess des Unternehmens auf die jeweiligen Hierarchieebenen heruntergebrochen, bspw. in Form einer quantitativen Risikostrategie mit Limits bei Finanzrisiken im Treasury oder durch die Kopplung an Budgetbegrenzungen und schrittweise Freigaben bei Investitionen oder Entwicklungsprojekten.

Ausgangspunkt für die Bemessung des Risikoappetits sowie der Risikotoleranz des RMS ist die *Risikotragfähigkeit* des Unternehmens. Die Risikotragfähigkeit beschreibt das maximale Risikoausmaß, welches das Unternehmen ohne Gefährdung seines Fortbestands tragen kann. Die Bestandsgefährdung kann dabei aus der finanziellen Situation (Überschuldung, (drohende) Zahlungsunfähigkeit), aber auch aus anderen regulatorischen oder geschäftlichen Anforderungen resultieren (bspw. Verlust der Zulassung wichtiger Produkte, Patentschutz, Wegfall des Zugangs zu wichtigen Märkten, langfristige Betriebsunterbrechung).

In Form einer Risikopolitik werden die unternehmerischen Vorgaben zum erwünschten Umgang mit Risiken durch die Unternehmensleitung formuliert und im Unternehmen kommuniziert, um die aus Unternehmenssicht definierten Ziele in Bezug auf den Risikoappetit und die Risikotoleranz für den jeweiligen Unternehmensbereich zu operationalisieren.

Organisation des RMS

A23 Merkmale der Organisation des RMS sind u.a.

- die klare Festlegung von Rollen und Verantwortlichkeiten im RMS. Hierzu gehören die Festlegung der Verantwortlichkeit für die Koordination und Steuerung des RMS sowie die Festlegung der Aufgaben und der hierarchischen Stellung bzw. der organisatorischen Einordnung und der Berichtslinien. Diese Aufgabe kann durch eine Stelle/Abteilung oder durch ein Gremium (z.B. Risikokomitee) ausgeführt werden. Die Festlegung der Rollen und Verantwortlichkeiten wird in der Praxis zum Teil anhand des „Three-lines-of-Defense Modells“ vorgenommen.[16]
- die Festlegung der Ablauforganisation, insb. für die Risikoerkennung, Risikosteuerung, Kommunikation und Überwachung. Hierzu gehört auch die Festlegung von Rahmenvorgaben zu Methoden des Risikomanagements sowie der Verzahnung mit weiteren Corporate Governance Systemen und Steuerungsinstrumenten. Die Ablauforganisation wird in Form von Handbüchern oder Regelwerken dokumentiert und kommuniziert. Es können unterschiedliche Stellen oder Abteilungen mit Risikomanagementaufgaben befasst sein, unabhängig davon, ob diese als „Risikomanagement“ bezeichnet werden (z.B. Risikomanagementaktivitäten im Controlling, im Treasury, im Qualitätsmanagement oder in der strategischen Planung). In kleineren Unternehmen werden Aufgaben des Risikomanagements zum Teil zentral von der Geschäftsführung selbst wahrgenommen.
- Einsatz technischer Hilfsmittel und erforderlichenfalls einer angemessenen IT-Unterstützung in den einzelnen RMS-Grundelementen (z.B. web-basierte Abfragesysteme und Controllingsysteme).

Risikoidentifikation

A24 Die Regelmäßigkeit der Analyse der Ereignisse und Entwicklungen richtet sich nach der Dynamik der betrachteten Risiken. Sehr dynamische Risiken, wie Entwicklungen an Güter- und Finanzmärkten, werden kontinuierlich bzw. mit hoher Frequenz betrachtet. Für im Zeitablauf weniger dynamische Risiken, wie z.B. Betriebsunterbrechungen, kann dagegen eine

[16] Vgl. *IDW PS 983*, Tz. 10.

detaillierte Analyse im Ein- oder Mehrjahresrhythmus bzw. anlässlich wesentlicher Änderungen an Organisation, Prozessen oder Geschäftsmodell ausreichend sein.

Eine systematische Risikoidentifikation sollte unter Einbezug der verschiedenen Ebenen und Funktionen des Unternehmens erfolgen und umfasst u.a. die folgenden Merkmale:

- eine (vollständige) Betrachtung der Ursachen und Faktoren wesentlicher Risiken für das zu prüfende RMS sowohl innerhalb des Unternehmens als auch im Umfeld, bspw. unterstützt durch themen- bzw. branchenspezifische Risikokataloge
- eine systematische Analyse von Frühwarnindikatoren und Kennzahlen, aus deren Beobachtung frühzeitig mögliche kritische Entwicklungen erkannt werden können. Diese können sowohl aus vorausschauenden Indikatoren und Prognosewerten bestehen (Früherkennung) als auch der Aufdeckung von Schadensfällen und der Analyse von Trends dienen.
- Analyse sowohl aus Sicht der Unternehmensleitung (Top Down) als auch aus Sicht der operativ mit der Erkennung und Steuerung von Risiken befassten Bereiche (Bottom Up)
- Erfassung und Kommunikation von als kritisch erkannten Entwicklungen an die für die nachfolgende Risikobewertung und -steuerung zuständigen Bereiche
- eine vollständige und nachvollziehbare Dokumentation der Risikoidentifikation.

Risikobewertung

A25 Die Bewertung der Risiken erfolgt transparent, nachvollziehbar und nach einer konsistent angewandten Systematik, die es erlaubt, die Bedeutung und den Wirkungsgrad von Risikosteuerungsmaßnahmen einzuschätzen. Die Ermittlung der Auswirkung (d.h. die Höhe der Zielabweichungen) kann für verschiedene Szenarien (z.B. best case/worst case) bestimmt werden. Der Zeithorizont, der für die Bewertung der Risiken zugrunde gelegt wird, sollte konsistent zu dem Zeithorizont der mit den Risiken im Zusammenhang stehenden Ziele sein. In Abhängigkeit des jeweiligen Unternehmensbereichs bzw. der Branche und des Geschäftsmodells des Unternehmens kann der genaue Betrachtungszeitraum variieren.

Die Eintrittswahrscheinlichkeit kann qualitativ (z.B. hoch, mittel oder niedrig), quantitativ (z.B. durch Angabe von Prozentwerten oder Bandbreiten) sowie durch Angabe einer Häufigkeit bezogen auf einen Zeitraum bestimmt werden.

Die Auswirkung strategischer, längerfristiger Risiken wird, wenn möglich, ebenfalls quantitativ bewertet. Sofern operative oder strategische Risiken nicht objektiv nach-vollziehbar bewertet werden können (wie bspw. das Risiko eines Imageverlustes), erfolgt eine qualitative Bewertung. Hierbei sollte aber auch eine Abschätzung der Risikotragweite nach festgelegten Kriterien (bspw. über eine Bandbreitenzuordnung oder der Klassifizierung bspw. als „high priority risk“) erfolgen.

Die Bewertungsergebnisse sind Grundlage für die weitere Verwendung zu Steuerungs-/Überwachungszwecken im RMS. Hierbei kann bspw. eine quantitative Auswertung und Aggregation entsprechende Bewertungsmethoden erfordern; qualitativ bewertete Risiken können in zuvor definierte Wertklassen eingeordnet werden. Die Beurteilung der Wesentlichkeit erfolgt auf der Grundlage der festgelegten Ziele des RMS, insb. der Risikostrategie und des Risikoappetits. Auf dieser Basis kann auf übergeordneter Ebene in regelmäßigen Abständen

eine Aggregation der ermittelten Einzelrisiken für einzelne Risikofelder erfolgen. Hierbei werden Korrelationen berücksichtigt.

Zur qualitativen Unterstützung der Risikobewertung kann es u.U. sachgerecht sein, Verfahren der Risikosimulation einzusetzen. Auf dieser Basis kann dann eine aggregierte Gesamtrisikoposition für die betrachtete Organisationseinheit ermittelt werden.

Der Prozess der Risikobewertung wird nachvollziehbar dokumentiert (z.B. als Prozessbeschreibung in einer Risikorichtlinie, einem RM-Handbuch oder einer bereichs- oder funktionsbezogenen Verfahrensanweisung).

Risikosteuerung

A26 Die Entscheidungen zur Risikosteuerung werden für wesentliche Einzelrisiken festgelegt und nachvollziehbar erläutert und dokumentiert. Gegebenenfalls können regulatorische Anforderungen an die inhaltliche Ausgestaltung der Risikosteuerung bestehen; ebenso können vertragliche Verpflichtungen (bspw. bei Versicherungsverträgen) Vorgaben zum Risikoappetit oder Wirtschaftlichkeitsüberlegungen explizite Maßnahmen zur Risikosteuerung erfordern.

Die Überwachung der Risikosteuerungsmaßnahmen kann dezentral im Verantwortungsbereich der Risikoverantwortlichen oder zentral erfolgen. Der Fokus der Überwachung von Risikosteuerungsmaßnahmen wird hierbei auf die grundsätzliche Umsetzung und die Wirksamkeit eingeleiteter Risikosteuerungsmaßnahmen gerichtet.

Für ein effektives Management der Risikosteuerungsmaßnahmen empfiehlt es sich, den Maßnahmenstatus nach bestimmten Kriterien zu systematisieren. Es können z.B. Maßnahmen hinsichtlich ihres Umsetzungsstandes („in Planung" vs. „initiiert" vs. „bereits effektiv umgesetzt") beurteilt werden.

Die in das RMS involvierten Personen werden im Hinblick auf die Ziele des RMS, den RM-Prozess und die eingesetzten Verfahren und Tools angemessen geschult.

Risikokommunikation

A27 Die Risikokommunikation umfasst u.a. die folgenden Elemente:

- Kommunikation der Regelungen des RMS und von relevanten Risikobereichen an die betroffenen Personen
- Festlegung der Berichtspflichten (Anlässe und Zeitpunkte) und der Berichtswege für die Kommunikation von Risiken an die zuständigen Stellen im Unternehmen einschließlich Unternehmensleitung und Aufsichtsgremien
- Sicherstellung aktueller, zutreffender entscheidungsrelevanter Informationen.

Der Prozess der Risikokommunikation ist nachvollziehbar festgelegt und dokumentiert (z.B. Terminvorgaben, Berichtsformate und Kommunikationswege). Die Kommunikation der Regeln des RMS kann z.B. in Form von Mitarbeiterbriefen, RMS-Handbüchern oder Schulungsveranstaltungen erfolgen.

Das Format und die Struktur der Berichterstattung sind adressatengerecht und aussagefähig ausgestaltet. Die übersichtliche Darstellung der Risikosituation erfolgt bspw. in einem regelmäßigen Risikobericht in standardisierter Form. Hierin kann eine Clusterung der Risiken nach ihrer Wesentlichkeit erfolgen, sodass eine Priorisierung der Risiken für Steuerungs-/

Überwachungszwecke möglich ist. Die hierzu festzulegenden Grenzbereiche werden maßgeblich durch die jeweils gewählte Risikostrategie bestimmt. Eskalationsstufen können auf der Basis angemessener Schwellenwerte eingerichtet werden.

Für eilbedürftige Risikomeldungen ist ein Verfahren zur ad hoc-Risikoberichterstattung etabliert. Dieses sieht vor, dass auf Grundlage von definierten Wesentlichkeitskriterien eine direkte, dokumentierte Weiterleitung von Risikosachverhalten bis zur Unternehmensleitung erfolgt. Die Risikomeldung erfolgt hierbei initial durch die jeweils betroffene Berichtseinheit.

Voraussetzung für eine angemessene Risikokommunikation ist, dass entscheidungsrelevante Informationen so aus internen und externen Quellen gesammelt, aufbereitet, geprüft und aktualisiert werden, wie sie nach wirtschaftlichem Ermessen für die Risikoidentifikation und Risikobewertung von den hierfür Verantwortlichen benötigt werden.

Überwachung und Verbesserung des RMS

A28 Es existieren schriftliche Vorgaben für die prozessintegrierte Überwachung des RMS als Prozessbeschreibung (bspw. in einer Risikorichtlinie bzw. einem RM-Handbuch oder einer Verfahrensanweisung der jeweiligen Organisationseinheit). Eine systematische prozessintegrierte Überwachung ist implementiert. Eine regelmäßige Prüfung der Aktualität und Angemessenheit des Risikomanagements wird vorgenommen. Die Durchführung der prozessintegrierten Überwachung ist nachvollziehbar dokumentiert (z.B. Protokolle, Checklisten).

Eine wichtige Funktion im Bereich der prozessintegrierten Überwachung des RMS bilden die speziell für dessen Ablaufprozesse etablierten Kontrollen, z.B. Überwachung der Risikoidentifikation und -bewertung durch einen Risikobeauftragten. Diese werden auf Ebene sämtlicher in das RMS einbezogenen Organisationseinheiten (bspw. Zentralbereiche wie Treasury, Einkauf etc., operative Einheiten) implementiert und in Abhängigkeit von Komplexität und Bedeutung der jeweiligen RMS-Prozesse ausgestaltet. Sie dienen der Vermeidung bzw. Begrenzung ablauforganisatorischer Risiken innerhalb des RMS.

Das RMS ist Bestandteil regelmäßiger prozessunabhängiger Überwachung (z.B. durch die Interne Revision). Die Überwachung beinhaltet auch regelmäßige Beurteilungen des RMS, die sowohl auf die Angemessenheit als auch auf dessen Wirksamkeit gerichtet sind.

Gegenstand einer prozessunabhängigen Überwachung können u.a. folgende Aspekte sein:

- Vollständige Erfassung aller Risikofelder des Unternehmens
- Angemessenheit der eingerichteten Regelungen zur Risikoerfassung und Risikokommunikation
- Angemessenheit und kontinuierliche Anwendung der Risikosteuerungsmaßnahmen vor dem Hintergrund der gewählten Risikostrategie und der Ziele des RMS
- mögliche beabsichtigte Umgehungen eingerichteter Prozesse und Kontrollen.

Die Ergebnisse von Überwachungsmaßnahmen werden zwecks Ursachenanalyse und Entwicklung von Maßnahmen zur Verbesserung des RMS im Unternehmen kommuniziert.

Ergeben sich im Rahmen der Überwachung oder bei sonstigen Maßnahmen des RMS Hinweise auf Mängel des RMS, werden als Bestandteil der Durchsetzung des RMS Maßnahmen zur Verbesserung des RMS (z.B. Schulungen, Änderung von Berichtslinien und -frequenzen sowie -inhalten, Sanktionen etc.) getroffen. Stand und Verbesserungspotenzial

des RMS werden z.B. anhand von Best Practices, Benchmarking oder Reifegradmodellen beurteilt.

Auftragsannahme [Tz. 33 ff.]

A29 Folgende Aspekte haben bei der Beurteilung der Eignung des in der RMS-Beschreibung dargestellten Systems als Prüfungsgegenstand eine besondere Bedeutung:

- Übernehmen die gesetzlichen Vertreter Verantwortung für die Einrichtung, Aufrechterhaltung, Überwachung und Durchsetzung des RMS?
- Ist das RMS in einer Weise dokumentiert, dass ein sachverständiger Dritter in angemessener Zeit einen Überblick über das RMS erhalten kann?
- Sind die zu prüfenden Teilbereiche des RMS klar abgegrenzt?
- Hat das Unternehmen bei der Konzeption des RMS ein strukturiertes Vorgehen gewählt und werden geeignete RMS-Grundsätze verwendet (vgl. Tz. 18i.) und Anlage 1)?
- Sind die zur Anwendung kommenden RMS-Grundsätze den beabsichtigten Berichtsadressaten zugänglich?

A30 Die grundsätzliche Eignung des dargestellten Systems kann auch dadurch beeinträchtigt werden, dass eine von den gesetzlichen Vertretern festgelegte Abgrenzung der zu prüfenden Teilbereiche nicht hinreichend klar bzw. irreführend ist.

A31 Im Rahmen der Prüfung der Eignung der zugrunde gelegten RMS-Grundsätze ist von Bedeutung, ob die in der RMS-Beschreibung dargestellten RMS-Grundsätze gesetzlich vorgeschrieben sind oder ob sie auf einschlägigen, allgemein anerkannten Rahmenkonzepten oder auf anderen themen-, branchen- oder industriespezifischen Rahmenkonzepten beruhen (vgl. Anlage 1). Sofern solche Rahmenkonzepte nicht existieren oder nicht ausreichend konkret sind, können auch entsprechende Grundsätze durch das Unternehmen selbst entwickelt oder ergänzt werden. Vom Unternehmen selbst entwickelte und verwendete RMS-Grundsätze sind stets vom Prüfer auf Eignung zu beurteilen.

A32 Geeignete RMS-Grundsätze i.S. dieses *IDW Prüfungsstandards* erfüllen die folgenden Anforderungen:

- *Relevanz*: Relevante RMS-Grundsätze führen zu Informationen, die die Entscheidungsfindung der Adressaten der RMS-Beschreibung unterstützen.
- *Vollständigkeit*: RMS-Grundsätze sind vollständig, wenn die nach diesen Grundsätzen erstellten Informationen keine relevanten Gesichtspunkte ausklammern, von denen angenommen werden kann, dass sie die Entscheidungsfindung der Adressaten beeinflussen würden.
- *Verlässlichkeit*: Verlässliche RMS-Grundsätze führen bei der Anwendung in vergleichbaren Fällen zu einer hinreichend konsistenten Beurteilung des RMS.
- *Neutralität*: Neutrale RMS-Grundsätze führen zu Informationen, die frei von irreführenden Darstellungen sind.
- *Verständlichkeit*: Verständliche RMS-Grundsätze führen zu Informationen, die den Adressaten der RMS-Beschreibung klare Schlussfolgerungen ermöglichen und Fehlinterpretationen verhindern.

A33 Folgende Aspekte werden im Allgemeinen mit dem Auftraggeber schriftlich vereinbart (vgl. Tz. 38):

- Ziel und Gegenstand der RMS-Prüfung (vgl. Tz. 20 ff.)
- die Verantwortung der gesetzlichen Vertreter für das RMS sowie für die Inhalte der RMS-Beschreibung
- die vom Unternehmen angewandten RMS-Grundsätze
- Art und Umfang der Prüfung des RMS und der Berichterstattung einschließlich einer Bezugnahme auf diesen *IDW Prüfungsstandard*; dies bezieht sich auch auf eine etwaige Berichtspflicht gegenüber Dritten (vgl. Tz. 112)
- die Tatsache, dass die Prüfung der Aussagen in der RMS-Beschreibung risikoorientiert erfolgt und keine Vollprüfung, sondern eine Prüfung in einer Auswahl vorgenommen wird und deshalb ein unvermeidbares Risiko besteht, dass selbst wesentliche falsche Aussagen in der RMS-Beschreibung bzw. wesentliche Mängel im RMS unentdeckt bleiben
- ein Hinweis auf die systemimmanenten Grenzen des RMS und darauf, dass die Prüfung nicht darauf ausgerichtet ist festzustellen, ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind
- bei einer Angemessenheitsprüfung: Zeitpunkt, auf den sich die Prüfung der Angemessenheit beziehen soll
- bei einer Wirksamkeitsprüfung: Zeitraum, auf den sich die Prüfung der Wirksamkeit des RMS beziehen soll
- Hinweise auf die Verwertung von Arbeiten der Internen Revision, anderer Wirtschaftsprüfer sowie von Sachverständigen
- das Erfordernis eines unbeschränkten Zugangs des Prüfers zu den für die Prüfung erforderlichen Informationen und der Bereitschaft der gesetzlichen Vertreter, Auskünfte in dem erforderlichen Umfang vollständig und richtig zu erteilen
- die Grundlagen der Honorarabrechnung und für den Auslagenersatz
- Haftungsbeschränkungen
- die Verpflichtung der gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben
- ggf. Verwendungsvorbehalt des RMS-Prüfungsberichts sowie
- ggf. Hinweis auf Berichtspflichten gegenüber dem Aufsichtsorgan.

A34 Wenn der RMS-Prüfer auch mit anderen Dienstleistungen (z.B. der Jahresabschlussprüfung oder der Prüfung des Compliance Management Systems) beauftragt war und er in deren Rahmen für die Beurteilung der Aussagen in der RMS-Beschreibung evtl. relevante Informationen erlangt hat, empfiehlt es sich, zu vereinbaren, dass er das Ergebnis dieser Tätigkeiten bei der Prüfung des RMS berücksichtigt.

A35 Es kann sinnvoll sein, im Rahmen der Auftragsannahme eine Vereinbarung mit dem Unternehmen über die Einbeziehung von sonstigen Angaben (vgl. Tz. 77) in die RMS-Prüfung zu schließen.

A36 Beispiele für wesentliche Änderungen der Bedingungen des Prüfungsauftrags (vgl. Tz. 42) sind:

- Änderungen des in der RMS-Beschreibung dargestellten Umfangs des RMS (z.B. durch Ausklammerung bestimmter Regionen oder Länder).
- Anstelle einer Wirksamkeitsprüfung soll nur die Angemessenheit des RMS geprüft werden.

Prüfungsplanung

Allgemeine Grundsätze [Tz. 43 ff.]

A37 Die Bedeutsamkeit der relevanten Risiken einer Organisationseinheit (Tz. 47) kann sich nach quantitativen oder qualitativen Faktoren bemessen. Ausgangsbasis für die Einschätzung des RMS-Prüfers ist die vom Unternehmen selbst vorzunehmende Einschätzung. Quantitative Faktoren stellen insb. auf die wirtschaftliche Bedeutung der jeweiligen Einheit ab. Qualitative Faktoren beziehen sich z.B. auf die Art und/oder die Höhe der jeweils für das RMS relevanten Risiken.

A38 Beispiele für quantitative Faktoren sind:

- Anteil am Gesamtumsatz
- Verhältnis der Ergebnisbeiträge
- Netto-Investitionssumme
- Angestrebte/geplante Rendite.

A39 Beispiele für qualitative Faktoren sind:

- Dezentraler Autonomiegrad des Managements
- Komplexität des Geschäftsmodells
- Grad der Regulierung/Anfälligkeit für Regelverstöße
- Standardisierungsgrad von Prozessen
- Zentralisierung von Prozessen und Funktionen
- Standardisierung wesentlicher Entscheidungen
- Marktstrukturen und Veränderungsdynamik des Marktes.

Wesentlichkeit [Tz. 50]

A40 Der RMS-Prüfer berücksichtigt seine Überlegungen zur Wesentlichkeit (vgl. Tz. 50)

- bei der Planung und Durchführung der Prüfung, einschließlich der Bestimmung von Art, Umfang und zeitlicher Einteilung der Prüfungshandlungen, und
- bei der Auswertung von Prüfungsfeststellungen, d.h. bei der Beurteilung, ob die Aussagen in der RMS-Beschreibung (vgl. Tz. 18h.) wesentliche Fehler enthalten.

A41 Ein wesentlicher Fehler in den Aussagen der RMS-Beschreibung liegt z.B. dann vor, wenn

- sie einen vorhandenen wesentlichen Mangel des RMS nicht erkennen lassen,

- sie falsche Angaben enthalten oder Angaben fehlen, die – einzeln oder in der Summe – für die Adressaten der RMS-Beschreibung entscheidungsrelevant sein können, oder
- sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthalten, die eine Irreführung der Adressaten der RMS-Beschreibung zur Folge haben können.

A42 Ein wesentlicher Mangel des RMS liegt dann vor, wenn das in der RMS-Beschreibung dargestellte RMS nicht geeignet oder nicht wirksam ist, mit hinreichender Sicherheit wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen. Ein wesentlicher Mangel des RMS kann auch bei einer Kumulation von nicht rechtzeitig identifizierten und nicht entsprechend den festgelegten Zielen des RMS gesteuerten Risiken vorliegen, die einzeln betrachtet, nicht wesentlich sind.

A43 Bei der Bestimmung der Wesentlichkeit von Mängeln des in der RMS-Beschreibung dargestellten RMS sind insb. folgende Fragestellungen von Bedeutung:

- *Art des Mangels*: Ist ein nicht rechtzeitig erkanntes, unzutreffend beurteiltes und/oder nicht zielgerichtet gesteuertes Risiko auf eine systemimmanente Schwachstelle zurückzuführen oder handelt es sich um eine einmalige Durchbrechung des Systems? Wurden in der RMS-Beschreibung dargestellte Regelungen des RMS durch die gesetzlichen Vertreter oder durch andere Mitglieder des Managements außer Kraft gesetzt oder umgangen?
- *Bedeutung des vom RMS adressierten Risikos*: Können die möglichen Mängel zu wesentlichen Fehlsteuerungen oder Verfehlungen hinsichtlich der RMS-Ziele führen? In welchem Umfang sind einzelne Unternehmenseinheiten/-prozesse oder die Gesamtorganisation von dem mit dem Mangel verbundenen Risiko betroffen?
- *(Potenzielles) Schadensausmaß*: Welcher finanzielle oder sonstige Schaden ist mit einem nicht rechtzeitig erkannten, unzutreffend beurteilten und/oder nicht zielgerichtet gesteuerten strategischen oder operativen Risiko (i.S. einer negativen Zielabweichung) für die Unternehmensorganisation verbunden? Welche Auswirkungen können sich unter Berücksichtigung der Risikotragfähigkeit und des Risikoappetits aus dem Mangel auf die Gesamtorganisation bzw. einzelne Organisationseinheiten oder Prozesse ergeben?
- *Bestandsgefährdende Risiken*: Können die (möglichen) Mängel den Fortbestand der Unternehmensorganisation gefährden?
- *Ursache für den Mangel*: Beruht ein nicht rechtzeitig erkanntes, beurteiltes und/oder gesteuertes Risiko auf beabsichtigtem oder irrtümlichem Handeln oder Unterlassen?

Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld [Tz. 51 f.]

A44 Anhaltspunkte für wesentliche Mängel des in der RMS-Beschreibung dargestellten RMS können sich u.a. aus den folgenden Umständen ergeben:

- Es werden keine geeigneten RMS-Grundsätze verwendet (vgl. Tz. A31 f.).

- Die Konzeption des RMS weist Lücken auf, die dazu führen können, dass nicht alle relevanten wesentlichen Risiken berücksichtigt werden.
- Der Prozess zur systematischen Erfassung und Analyse von wesentlichen Risiken weist Schwachstellen auf, z.B. werden im Rahmen der Prüfung wesentliche Risiken erkannt, die vom RMS zuvor nicht erfasst und analysiert worden sind.
- Es gibt Nachweise dafür, dass die implementierten Regelungen der Steuerung von wesentlichen Risiken nicht geeignet oder unwirksam sind.
- Die Regelungen des RMS werden nicht regelmäßig auf Anpassungsbedarf wegen geänderter Rahmenbedingungen überprüft und ggf. geändert.
- Im RMS werden keine ausreichenden Ressourcen eingesetzt.
- Das RMS wird im Unternehmen nicht ausreichend kommuniziert und überwacht.
- Das RMS wird nicht konsequent durchgesetzt, z.B. werden bei identifizierten Mängeln keine angemessenen Maßnahmen zur Beseitigung und künftigen Verhinderung der Mängel ergriffen.

A45 Sofern es sich bei dem RMS-Prüfer um den Abschlussprüfer des Unternehmens handelt, wird das erforderliche Verständnis von dem rechtlichen und wirtschaftlichen Umfeld des Unternehmens und dem RMS teilweise bereits vorhanden sein – insb. dann, wenn auch die Maßnahmen nach § 91 Abs. 2 AktG geprüft wurden (vgl. Tz. 13).[17] Die Abschlussprüfung hat im Unterschied zur RMS-Prüfung allerdings das Ziel, die Ordnungsmäßigkeit der Rechnungslegung zu beurteilen. Der Abschlussprüfer richtet seine Risikobeurteilungen daher auf die Feststellung wesentlicher falscher Angaben in der Rechnungslegung aus. Die in diesem Zusammenhang erworbenen Kenntnisse über das Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld werden für Zwecke der RMS-Prüfung im Allgemeinen nicht ausreichend sein.

A46 Besprechungen zwischen dem auftragsverantwortlichen Wirtschaftsprüfer und anderen Mitgliedern des Prüfungsteams sowie ggf. mit Sachverständigen des RMS-Prüfers sollen die Mitglieder für das mögliche Vorhandensein wesentlicher Fehler in der RMS-Beschreibung bzw. wesentliche Mängel im RMS sensibilisieren und ihr Verständnis für die Auswirkungen der Ergebnisse ihrer Prüfungshandlungen auf andere Aspekte der RMS-Prüfung fördern.

Gewinnung eines Verständnisses von dem in der RMS-Beschreibung dargestellten Risikomanagementsystem [Tz. 53 f.]

A47 Im Rahmen der Ausgestaltung des RMS entscheiden die gesetzlichen Vertreter u.a., welche RMS-Grundsätze angewendet werden sollen. Hierbei kommen die in Anlage 1 genannten allgemein anerkannten Rahmenkonzepte, andere geeignete Rahmenkonzepte oder individuell entwickelte geeignete RMS-Grundsätze in Betracht. Bei der individuellen Entwicklung von RMS-Grundsätzen können die gesetzlichen Vertreter auch entscheiden, sich an verfügbaren Informationen über die Praxis anderer Unternehmen zu orientieren. Sofern das angewandte

[17] Vgl. *IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n.F.)* (Stand: 13.03.2013) und *IDW Prüfungsstandard: Kenntnisse über die Geschäftstätigkeit sowie das wirtschaftliche und rechtliche Umfeld des zu prüfenden Unternehmens im Rahmen der Abschlussprüfung (IDW PS 230)* (Stand: 08.12.2005) sowie *IDW PS 340*.

Rahmenkonzept nicht alle RMS-Grundelemente (vgl. Tz. 31) abdeckt, bietet sich eine Ergänzung durch andere Grundsätze an, die individuell entwickelt, im Rahmen von Vergleichen mit der Praxis anderer Unternehmen festgestellt oder einem anderen Rahmenkonzept entnommen werden können.

A48 Das vom RMS-Prüfer zu erlangende Detailverständnis von dem RMS umfasst z.B. folgende Aspekte:

- Die Unternehmensziele und die daraus abgeleiteten RMS-Ziele
- die Risikostrategie und Risikopolitik des Unternehmens
- die Ausprägung des Risikobewusstseins der Mitarbeiter
- die Aufbau- und Ablauforganisation des RMS
- die Regelungen zur Identifikation, Bewertung, Kommunikation und Steuerung der wesentlichen Risiken
- die Regelungen zur Überwachung und Verbesserung des RMS.

Prüfungsdurchführung [Tz. 57 ff.]

Prüfung der in der RMS-Beschreibung enthaltenen Aussagen zur Angemessenheit und Wirksamkeit des RMS [Tz. 60 ff.]

A49 Bei der Festlegung der Prüfungshandlungen kann der Prüfer bei wiederkehrenden Aufträgen Ergebnisse früherer RMS-Prüfungen verwerten. Dies gilt vor allem für die Beurteilung der Angemessenheit des RMS, die sich bei Folgeprüfungen vor allem auf Veränderungen des RMS erstrecken wird. In Bezug auf die Beurteilung der Wirksamkeit des RMS im Prüfungszeitraum können sich die Erkenntnisse aus früheren Prüfungen im Wesentlichen auf die Risikoeinschätzung des RMS-Prüfers und den Umfang der Prüfungen der Wirksamkeit auswirken. Prüfungsnachweise aus früheren Prüfungen stellen aber für sich genommen keinen Nachweis über die Wirksamkeit des RMS im zu prüfenden Zeitraum dar.

A50 Im Rahmen der Prüfung der Angemessenheit (vgl. Tz. 61 f.) kommen insb. die folgenden Prüfungshandlungen in Betracht:

- Befragungen der gesetzlichen Vertreter, anderer Mitglieder des Managements und von Mitgliedern des Aufsichtsorgans (z.B. zur Konzeption des RMS, zur Durchsetzung des RMS und zu bekannten Schwachstellen im RMS).
- Befragungen von Personen, die für die Konzeption und/oder Weiterentwicklung, die Überwachung des RMS und die Koordination von Aktivitäten im Zusammenhang mit dem RMS zuständig sind, um deren Aufgabenstellung, Kompetenz und Erfahrung, Stellung innerhalb der Unternehmenshierarchie und Kenntnisse über mögliche Schwachstellen im RMS und festgestellte Verstöße sowie die Reaktionen des Unternehmens auf solche Feststellungen in Erfahrung zu bringen (z.B. Risikomanager oder Mitarbeiter der Internen Revision).
- Durchsicht von Dokumentationen des RMS (z.B. Organisations-, Risikomanagementhandbücher, Verfahrensgrundsätze)
- Durchsicht von Unterlagen, die im Zusammenhang mit dem RMS generiert werden (z.B. Berichte der Internen Revision, Risikoberichte)

- Beobachtung von Aktivitäten und Arbeitsabläufen im Unternehmen, die mit dem RMS in Verbindung stehen.

A51 Die Prüfung der Wirksamkeit (vgl. Tz. 63) umfasst die kontinuierliche Anwendung der im RMS verankerten Regelungen in dem von der Prüfung abgedeckten Zeitraum. Es wird geprüft, ob die Regelungen wie vorgesehen von den dafür bestimmten Personen beachtet bzw. durchgeführt wurden und diesen die für die Wahrnehmung der Aufgaben erforderlichen Hilfsmittel und Informationen zur Verfügung standen.

A52 Sofern der Zeitraum (vgl. Tz. 64) weniger als ein Geschäftsjahr abdeckt, kann es angebracht sein, im Prüfungsbericht die Gründe für einen kürzeren Zeitraum darzustellen. Gründe, die ggf. zu einem kürzeren Zeitraum führen, können z.B. vorliegen, wenn das System weniger als ein Geschäftsjahr operativ war oder wenn es im Falle von wesentlichen Änderungen des Systems nicht praktikabel ist, entweder einen Zeitraum von einem Geschäftsjahr abzuwarten oder einen Prüfungsbericht zu erstellen, der sowohl den Zeitraum vor als auch nach den vorgenommenen Änderungen umfasst. Ein kürzerer Zeitraum kann ebenfalls dann angemessen sein, wenn der Vorstand oder der Aufsichtsrat bei der Beurteilung der Angemessenheit oder der Wirksamkeit des RMS abweichende Zyklen zugrunde legt, z.B. einzelne Quartale.

A53 Folgende Prüfungshandlungen kommen im Rahmen der Prüfung der Wirksamkeit des RMS in Betracht:

- Befragung der von den Regelungen betroffenen Personen (gesetzliche Vertreter, Mitarbeiter im RMS, Mitarbeiter der Internen Revision und andere relevante Mitarbeiter)
- Durchsicht und Auswertung der RMS-Dokumentation hinsichtlich der kontinuierlichen Anwendung der Regelungen, z.B. Protokolle von Aufsichtsratssitzungen, Risikoinventaren, Checklisten, Fragebögen, Kontrollbeschreibungen, Berichte der Internen Revision
- Beobachtung der Einhaltung von Grundsätzen bzw. der Durchführung von Verfahren und Maßnahmen im RMS (z.B. Risk Assessment Diskussionen, Überwachungsmaßnahmen der Internen Revision)
- Nachvollziehen von für das RMS relevanten Kontrollen
- IT-gestützte Prüfungshandlungen (z.B. Datenanalysen im Zusammenhang mit systemtechnisch abgebildeten Berechtigungs- und Freigabekonzepten).

A54 Befragungen allein reichen für die Erzielung der erforderlichen Urteilssicherheit über die Wirksamkeit des RMS nicht aus. Sie werden für eine Verwertbarkeit als Prüfungsnachweis mit einer oder mehreren zusätzlichen Arten von Prüfungshandlungen kombiniert. Eigene Beobachtungen sind i.d.R. aussagekräftiger als die Verwertung von Aussagen Dritter. Allerdings beziehen sich solche Beobachtungsergebnisse immer nur auf den Zeitpunkt der Prüfung. In diesen Fällen kann es daher erforderlich sein, weitere Prüfungshandlungen in Erwägung zu ziehen, um die kontinuierliche Anwendung der Regelungen des RMS zu prüfen.

A55 Art, Umfang und Zeitpunkt der im Rahmen der Prüfung der Angemessenheit und Wirksamkeit durchzuführenden Prüfungshandlungen sind u.a. abhängig von

- den angewandten RMS-Grundsätzen,
- den Inhalten der RMS-Beschreibung,

- den bisherigen Erfahrungen des Prüfers mit dem Unternehmen,
- den Ergebnissen der Risikobeurteilungen,
- der Ausgestaltung des RMS und dessen Dokumentation,
- der verwendeten IT-Unterstützung,
- der Art und Weise der Überwachung des RMS, z.B. durch die Interne Revision oder andere unternehmensinterne Funktionen sowie
- Wesentlichkeitsüberlegungen.

A56 Bei der Prüfung der Regelungen zur *Risikokultur* können die einzelnen Merkmale der Risikokultur (vgl. Tz. A21) sowohl durch die Durchsicht von Regelwerken und dokumentierten Verhaltensgrundsätzen, die Befragung von gesetzlichen Vertretern und Mitarbeitern bzw. Mitgliedern des Aufsichtsorgans als auch durch Beobachtung und Nachvollziehen des gelebten Verhaltens der Unternehmensmitglieder und deren Umgang mit Risikosituationen festgestellt werden. In diesem Zusammenhang ist nicht nur das formale Bestehen von Regelungen, sondern auch deren tatsächliche Umsetzung im Unternehmen von Bedeutung.

A57 Die Prüfung der Regelungen zur *Risikoidentifikation* kann z.B. eine Analyse umfassen, ob geeignete Regelungen zur rechtzeitigen Risikoerkennung für die identifizierten Risikobereiche existieren und ob diese permanent i.S. eines Soll-/Ist-Vergleichs durch das Unternehmen verfolgt werden. Neben einem ausgeprägten Risikobewusstsein der Mitarbeiter sind die Existenz und der fortwährende Einsatz von geeigneten Regelungen entscheidend für die Vollständigkeit der Risikoidentifikation, die Risikobewertung und die hieran anschließende zeitgerechte Risikokommunikation. Das erlangte Verständnis von dem Unternehmen und seinem Umfeld sowie von dem zu prüfenden RMS spielt eine wichtige Rolle bei der Prüfung der Vollständigkeit der Risikoidentifikation durch den RMS-Prüfer. Hierbei ist auch von Bedeutung, inwieweit sich der Vorgang der Risikoidentifikation an den Unternehmenszielen bzw. den RMS-Zielen orientiert. Eine Verknüpfung mit den Zielen und der Unternehmensplanung ermöglicht es dem RMS-Prüfer, die systematische Ableitung der Risiken und deren Bewertung nachzuvollziehen.

Hinsichtlich der Verwendung von Risikoindikatoren sollten ggf. auch Berichtswege außerhalb des formalen Risikoreportings in die Betrachtung einbezogen werden. Allerdings wird die Vollständigkeit der Risikoidentifikation aufgrund der unvollkommenen Voraussicht ex ante nicht mit hundertprozentiger Sicherheit beurteilt werden können.

A58 Die Prüfung der vom Unternehmen eingerichteten Regelungen zur Risikobewertung setzt voraus, dass dem Prüfer die der Bewertung zugrunde gelegten Prämissen und die hierauf basierenden Planungsrechnungen, Sensitivitätsanalysen, Szenariorechnungen o.Ä. vom Unternehmen offengelegt werden. Hierbei ist von Bedeutung, ob das jeweils verwendete Prognosemodell sachgerecht und richtig gehandhabt worden ist, ob alle verfügbaren relevanten Informationen verwendet wurden und Interdependenzen Rechnung getragen wurde. Zu berücksichtigen ist, dass trotz aller ggf. eingesetzten Hilfsmittel die Bewertung der Risiken stark durch das subjektive Urteil des Bewerters bestimmt wird. Deshalb ist es wichtig, dass sich der Prüfer davon überzeugt, dass die Bewertung vom Unternehmen willkürfrei und im Zeitablauf konsistent vorgenommen wurde. Dieses Nachvollziehen wird, insb. bei möglichen Szenariobetrachtungen, dadurch erleichtert, dass die Kernprämissen zur Risikobewertung durch das Unternehmen dokumentiert werden. Eine konsistente Risikobewertung kommt auch dadurch zum Ausdruck, dass unternehmens- bzw. konzernweit einheitliche Bewer-

tungsverfahren zum Einsatz kommen und je nach Bedeutung der jeweiligen Risiken die unternehmensindividuell festgelegten Wesentlichkeitsgrenzen eingehalten werden. Es ist jedoch nicht die Aufgabe des Prüfers, die Schätzung der Unternehmensleitung durch seine eigene Schätzung zu ersetzen.

Hinsichtlich der Maßgabe einer sachgerechten Abbildung der Gesamtrisikosituation im Unternehmen/Konzern bzw. im zu prüfenden Teilbereich ist es aus Prüfersicht wichtig zu analysieren, ob Abläufe etabliert sind, die die Aggregation von Risiken innerhalb des gesamten Unternehmens/Konzernverbunds bzw. innerhalb der zu prüfenden Teilbereiche einschließlich der Berücksichtigung von Interdependenzen sicherstellen.

A59 Die Prüfung der Risikosteuerung umfasst die Analyse und Beurteilung der Ausgestaltung und wirksamen Umsetzung von dokumentierten Risikosteuerungsmaßnahmen. Für die Prüfung der Ausgestaltung ist z.B. eine Analyse der Beschreibung der Risikosteuerung dahingehend von Bedeutung, ob diese für sachkundige Dritte nachvollziehbar ist, ob die Beschreibung hinreichende Inhalte (insb. Risikobezug, Wirkungsweise der Regelungen, Hinweise zur Wirksamkeit, Kontrollmaßnahmen, Verantwortlichkeiten) umschließt und unternehmensweit konsistent erfolgt. Weiterhin ist von Bedeutung, ob einerseits die beschriebenen Risikosteuerungsmaßnahmen im Einklang mit der Risikostrategie stehen und ob andererseits die Maßnahmen vor dem Hintergrund des jeweils zugrunde liegenden Risikos nach pflichtgemäßem Ermessen des RMS-Prüfers inhaltlich geeignet sind, mit hinreichender Sicherheit die Ziele des RMS umzusetzen. Im Hinblick auf die Umsetzung der Maßnahmen ist von Bedeutung, ob ausreichende und angemessene Prüfungsnachweise zur tatsächlichen Implementierung vorliegen und ob die Maßnahmen auch tatsächlich in der vorgesehenen Weise ausgeführt werden. Eine explizite Aussage zur Angemessenheit und Wirksamkeit von einzelnen Risikosteuerungsmaßnahmen ist nicht Gegenstand der Prüfung, ebenso nicht Aussagen zur Wirtschaftlichkeit getroffener Maßnahmen.

A60 Die Prüfung der Regelungen zur Risikokommunikation umfasst die Beurteilung, ob die entsprechenden aufbau- und ablauforganisatorischen Vorkehrungen im Unternehmen so getroffen wurden, dass alle relevanten Risiken vollständig und so frühzeitig an die jeweils zuständigen Entscheidungsträger kommuniziert werden, um wirksame Maßnahmen zur Risikobewältigung einleiten zu können. Zu diesem Zweck können z.B. die Kommunikationswege und -prozesse im üblichen Geschäftsreporting sowie im Risikoreporting analysiert werden. Hierbei ist insb. von Bedeutung, ob geeignete Eskalationskriterien für die Risikokommunikation festgelegt sind, die Berichtsperiodizitäten der Bedeutung des jeweiligen Risikos angemessen sind und ob geeignete Regelungen hinsichtlich einer ggf. erforderlichen Ad-hoc-Berichterstattung existieren. Ein wesentlicher Aspekt ist auch hier die Nachvollziehbarkeit der Risikokommunikation.

A61 Die Angemessenheit und Wirksamkeit des RMS werden ferner dadurch bestimmt, dass die Anwendung der definierten Regelungen des RMS fortwährend sichergestellt ist. Da dies auf Unternehmensebene durch Überwachungsaktivitäten gewährleistet werden soll, wird der Prüfer auch die entsprechenden Prozesse der Risikoüberwachung analysieren. Die Prüfung umfasst u.a. die Beurteilung, ob die personelle und qualitative Ausstattung der Internen Revision ausreichend ist und die ihr zugewiesenen Aufgaben zur Überwachung des RMS angemessen sind (vgl. Tz. 71 f.). Von Bedeutung kann daher die Analyse des Prüfprogramms der Internen Revision daraufhin sein, ob und inwieweit Aspekte der RMS-Überwachung Be-

rücksichtigung fanden. Schließlich umfasst die Prüfung ergänzend auch die Beurteilung der integrierten Kontrollen und sonstigen Maßnahmen (Managementkontrollen) zur Überwachung des RMS, um ein Gesamtbild von den Überwachungsprozessen zu gewinnen und hierauf basierend zu einem Urteil über deren Wirksamkeit zu gelangen.

Verwertung der Arbeit von Sachverständigen des Prüfers [Tz. 66 ff.]

A62 Eine Verwertung der Arbeit von Sachverständigen (vgl. Tz. 66) kann z.B. geboten sein bei

- der Beurteilung von Maßnahmen der Risikoquantifizierung des Unternehmens, wenn dieses in speziellen Branchen tätig ist, (z.B. im Rohstoff- oder Immobiliensektor),
- der Interpretation spezifischer Anforderungen der angewandten RMS-Grundsätze,
- der Beurteilung von IT-gestützten Bestandteilen des RMS,
- der Würdigung von Sachverhalten, die auf besondere (z.B. bestandsgefährdende) Risiken hindeuten, und der Würdigung von Maßnahmen des Unternehmens zur Begegnung dieser Risiken.

A63 Informationen zu Kompetenz, Fähigkeiten und Objektivität eines externen Sachverständigen (vgl. Tz. 68) können aus unterschiedlichen Quellen stammen, bspw. aus

- persönlicher Erfahrung mit der bisherigen Tätigkeit des Sachverständigen,
- Gesprächen mit dem Sachverständigen,
- Gesprächen mit anderen Wirtschaftsprüfern oder anderen Personen, die mit der Arbeit des Sachverständigen vertraut sind,
- Kenntnissen über die Qualifikationen des Sachverständigen (Feststellung einer Berufszulassung bzw. Mitgliedschaft in einer Berufs- oder Branchenorganisation),
- veröffentlichten Publikationen des Sachverständigen.

A64 Die folgenden Aspekte können bei der Beurteilung der Arbeiten externer Sachverständiger (vgl. Tz. 68) für die Zwecke des RMS-Prüfers relevant sein:

- Die Relevanz und Vertretbarkeit der Feststellungen und Schlussfolgerungen des Sachverständigen und ob diese mit anderen Prüfungsnachweisen im Einklang stehen;
- wenn den Arbeiten des Sachverständigen wesentliche Annahmen und Methoden zugrunde liegen, die Relevanz, Vollständigkeit und Vertretbarkeit dieser Annahmen und Methoden unter den gegebenen Umständen und
- wenn die Tätigkeit des Sachverständigen in der Verwendung von Ausgangsdaten besteht, die Relevanz, Vollständigkeit und Richtigkeit dieser Ausgangsdaten.

A65 Die Beurteilung der Arbeit von externen Sachverständigen kann z.B. durch Befragungen oder die Durchsicht der Berichterstattung bzw. der Arbeitspapiere des externen Sachverständigen erfolgen.

Verwertung der Arbeit anderer Wirtschaftsprüfer sowie Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter und der Internen Revision [Tz. 69 ff.]

A66 Die in Tz. A62 ff. dargestellten Anwendungshinweise können sinngemäß auch auf die Verwertung der Arbeit eines anderen Wirtschaftsprüfers bzw. auf die Verwendung der Arbeit von Sachverständigen der gesetzlichen Vertreter und auf die Verwendung der Arbeit der Internen Revision angewandt werden.

A67 Bei der Beurteilung der Arbeit der Internen Revision ist auch von Bedeutung, inwieweit die Anforderungen aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des IIA (The Institute of Internal Auditors)[18] sowie der DIIR Revisionsstandards, insb. des DIIR Revisionsstandards Nr. 2 zur Prüfung des Risikomanagements durch die Interne Revision, berücksichtigt wurden.

Ereignisse nach dem Beurteilungszeitpunkt/-zeitraum [Tz. 73 ff.]

A68 Als Prüfungshandlungen zur Feststellung von Ereignissen nach dem in der RMS-Beschreibung genannten Zeitpunkt bzw. Zeitraum, auf den sich die Aussagen der gesetzlichen Vertreter beziehen (vgl. Tz. 73), kommen z.B. in Betracht:

- Kritisches Lesen von Protokollen über in diesem Zeitraum stattgefundene Sitzungen der Verwaltungsorgane
- kritisches Lesen von unternehmensinternen Berichten, wie z.B. Berichte der Internen Revision, sowie
- Befragungen von für das Risikomanagement operativ verantwortlichen Personen und erforderlichenfalls der gesetzlichen Vertreter und des Aufsichtsorgans.

Sonstige Angaben in der RMS-Beschreibung [Tz. 77 ff.]

A69 Als weitere angemessene Maßnahme kann der RMS-Prüfer z.B. einen Hinweis (vgl. Tz. 95) in den RMS-Prüfungsbericht aufnehmen und darin die wesentliche Unstimmigkeit bzw. den wesentlichen offensichtlichen Fehler erläutern.

Schriftliche Erklärungen [Tz. 82 ff.]

A70 Schriftliche Erklärungen sind kein Ersatz für andere nach diesem *IDW Prüfungsstandard* vorgesehene Prüfungshandlungen.

Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils [Tz. 87 ff.]

A71 Stellt der Wirtschaftsprüfer eine Abweichung von den in der RMS-Beschreibung dargestellten Regelungen des RMS fest, wird er i.d.R. durch weitere Prüfungshandlungen klären, ob

[18] The Institute of Internal Auditors (IIA): Weltweite Organisation der nationalen Berufsverbände für Interne Revision.

es sich um einen Einzelfall handelt, der die Angemessenheit und Wirksamkeit des RMS nicht berührt oder ob ein Mangel im RMS vorliegt. Als mögliche Prüfungshandlungen kommen hierbei bspw. in Betracht:

- Befragung der gesetzlichen Vertreter zur eigenen Einschätzung der Ursache der festgestellten Abweichung
- Würdigung des Umgangs des Unternehmens mit der festgestellten Abweichung
- Prüfung, ob mit der Überwachung des RMS beauftragte Personen vergleichbare Abweichungen identifiziert haben und welche Maßnahmen daraufhin veranlasst wurden.

A72 Der RMS-Prüfer kann z.B. einen Hinweis nach Tz. 95 für das Verständnis des Prüfungsauftrags durch die Berichtsadressaten für erforderlich halten, um klarzustellen, dass die Prüfung nicht auf die Einhaltung der sich aus § 91 Abs. 2 AktG ergebenden Anforderungen ausgerichtet war.

Dokumentation [Tz. 96 ff.]

A73 Durch die Arbeitspapiere wird gleichzeitig nachgewiesen, dass die RMS-Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* geplant und durchgeführt wurde.

Weitere Berichtspflichten [Tz. 111 f.]

A74 Im Zusammenhang mit der RMS-Prüfung kann sich für den Wirtschaftsprüfer aus der Treuepflicht eine Pflicht zur Information des Auftraggebers über Sachverhalte ergeben, die anlässlich der RMS-Prüfung festgestellt werden. Hierbei kann es sich z.B. handeln um

- beabsichtigte oder unbeabsichtigte Verstöße der gesetzlichen Vertreter oder der Mitarbeiter des Unternehmens gegen Gesetze und andere Vorschriften,
- Hinweise, dass einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder umgesetzte Risikomanagementmaßnahmen offensichtlich nicht geeignet sind.

Anlagen

1. Allgemein anerkannte RMS-Rahmenkonzepte

Name	Organisation	Anwendungsbereich
1. Allgemeine Rahmenkonzepte		
Enterprise Risk Management – Integrated Framework (2004) (COSO ERM)[19]	Committee of Sponsoring Organization of the Tread-way Commission, Jersey City, USA	Umfassendes Modell eines unternehmensweiten Risikomanagements
DIN ISO 31000 Risk management: 2009[20]	International Organization for Standardization	Norm zur Einrichtung eines Integrierten Risikomanagements für Organisationen
ONR 49000 ff: Risikomanagement für Organisationen und Systeme (2014)[21]	Österreichisches Normungs-institut	Generischer, universell anwendbarer und branchenunabhängiger Rahmen für das Risikomanagement von Organisationen und Systemen (einschließlich Checklisten, Prozessbeschreibungen etc.)
1. Spezifische Rahmenkonzepte		
ISO 22301: Business Continuity Management[22]	International Organization for Standardization	Norm für die Erstellung und den Umgang mit dem Business Continuity Management System
IT-Grundschutz-Standards:[23] • BSI-Standard 100-1: Managementsysteme für Informationssicherheit • BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise • BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz • BSI-Standard 100-4: Notfallmanagement	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-Standards enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit.
DIN EN ISO 14971 – Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte[24]	International Organization for Standardization	Norm für das wirksame Management der mit der Anwendung von Medizinprodukten im Gesundheitswesen verbundenen Risiken durch den Hersteller.
BS-6079-3:2000 Project Management, Guide to the management of business related project risk (GB 2000)[25]	British Standards Institution	Hinweise zur Identifikation und Steuerung von Projektrisiken in Organisationen (primär für das RM von Projekten gedacht)

[19] COSO (2004): Enterprise Risk Management (ERM), Executive Summary, 2004. Das Rahmenkonzept wird aktuell überarbeitet.

[20] https://www.iso.org/iso-31000-risk-management.html (Stand: 13.03.2017).

[21] https://shop.austrian-standards.at, Rubrik: Produkte und Leistungen (Stand: 13.03.2017).

[22] http://www.beuth.de/de/norm/din-en-iso-22301/215741063 (Stand: 13.03.2017).

[23] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (Stand: 13.03.2017).

2. Berichterstattung über RMS-Prüfungen

Formulierungsbeispiele für RMS-Prüfungsberichte

2.1. Wirksamkeitsprüfung

Bericht des unabhängigen Wirtschaftsprüfers

Prüfung der Angemessenheit, Implementierung und Wirksamkeit des Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten RMS-Beschreibung der Angemessenheit, Implementierung und Wirksamkeit ihres Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS] durchzuführen.

Unter einem Risikomanagementsystem (RMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (Regelungen) zu verstehen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt. Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit, Implementierung und Wirksamkeit der in der als Anlage 1 beigefügten RMS-Beschreibung aufgeführten Regelungen für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS].

[24] http://www.beuth.de/de/norm/din-en-iso-14971/170088031 (Stand: 13.03.2017).

[25] http://shop.bsigroup.com/ProductDetail?pid=000000000019994545 (Stand: 13.03.2017).

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die [Gesellschaft] zur Verwendung [für interne Zwecke] gerichtet ist.

[*alternativ: Wir erstellen diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.*]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten RMS-Beschreibung enthaltenen Aussagen über ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS]. Bei der Einrichtung des RMS wurden [Bezeichnung der RMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das RMS einschließlich der Dokumentation des RMS und für die Inhalte der RMS-Beschreibung liegt bei den gesetzlichen Vertretern der [Gesellschaft].

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der RMS-Beschreibung enthaltenen Aussagen zur Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS] abzugeben. Die Zielsetzung der Prüfung liegt als Systemprüfung nicht darin, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind.

Die in der RMS-Beschreibung für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] dargestellten Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. Dies umfasst auch die Überwachung durch das RMS, ob die von den gesetzlichen Vertretern implementierten Risikosteuerungsmaßnahmen geeignet sind, mit hinreichender Sicherheit die Risikostrategie umzusetzen und die Ziele des RMS zu erreichen.

Die Wirksamkeit des RMS ist dann gegeben, wenn die Regelungen in den laufenden Geschäftsprozessen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortlichkeit in einem bestimmten Zeitraum wie vorgesehen eingehalten werden. Auch ein wirksames RMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, auftreten können, ohne systemseitig rechtzeitig erkannt und entsprechend den vom Unternehmen festgelegten Zielen des RMS gesteuert zu werden.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des Entwurfs *eines IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW EQS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die im geprüften Zeitraum implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] wirksam waren.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld sowie über das Risikoprofil und die Risikomanagementorganisation des Unternehmens berücksichtigt. Wir haben die in der RMS-Beschreibung dargestellten Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und angemessen sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der RMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des RMS sowie zur Angemessenheit, Implementierung und Wirksamkeit des RMS schriftlich bestätigt.

C. Feststellungen zum Risikomanagementsystem

I. Konzeption des RMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[u.a. Beschreibung der angewandten RMS-Grundsätze]

Ausführungen zu den einzelnen RMS-Grundelementen:

- Risikokultur
- Ziele des RMS

- Organisation des RMS
- Risikoidentifikation
- Risikobewertung
- Risikosteuerung
- Risikokommunikation
- Überwachung und Verbesserung des RMS.

II. Feststellungen [und Empfehlungen]

[a. Feststellungen, die zu einer Einschränkung, Versagung oder Nichterteilung des Prüfungsurteils geführt haben

b. sonstige Feststellungen

c. ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d. ggf. Hinweis auf nicht geprüfte sonstige Angaben in der RMS-Beschreibung

e. Empfehlungen]

D. Zusammenfassendes Prüfungsurteil

Sofern das RMS in Bezug auf strategische Risiken Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten strategischen Unternehmensziele entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Sofern das operative RMS Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,

- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Sofern das RMS sowohl in Bezug auf strategische Risiken als auch auf abgegrenzte Teilbereiche in Bezug auf operative Risiken Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS und [Beschreibung des oder der abgegrenzten Teilbereiche(s) des RMS] in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der strategischen Unternehmensziele und der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung des oder der abgegrenzten Teilbereiche(s) des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die RMS-Beschreibung des für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] bei der Gesellschaft wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Regelungen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des RMS falsche Schlussfolgerungen gezogen werden.

Auch ein wirksames RMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, auftreten können, ohne systemseitig rechtzeitig erkannt und entsprechend den vom Unternehmen festgelegten Zielen des RMS gesteuert zu werden.

Ort, Datum, Unterschrift

Anlagen:

[RMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

2.2. Wirksamkeitsprüfung mit Einschränkung

Bericht des unabhängigen Wirtschaftsprüfers

Prüfung der Angemessenheit, Implementierung und Wirksamkeit des Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten RMS-Beschreibung der Angemessenheit, Implementierung und Wirksamkeit ihres Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS] durchzuführen.

Unter einem Risikomanagementsystem (RMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (Regelungen) zu verstehen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt. Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit, Implementierung und Wirksamkeit der in der als Anlage 1 beigefügten RMS-Beschreibung aufgeführten Regelungen für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS].

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die [Gesellschaft] zur Verwendung [für interne Zwecke] gerichtet ist.

[*alternativ: Wir erstellen diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.*]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten RMS-Beschreibung enthaltenen Aussagen über ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS]. Bei der Einrichtung des RMS wurden [Bezeichnung der RMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das RMS einschließlich der Dokumentation des RMS und für die Inhalte der RMS-Beschreibung liegt bei den gesetzlichen Vertretern der [Gesellschaft].

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der RMS-Beschreibung enthaltenen Aussagen zur Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS] abzugeben. Die Zielsetzung der Prüfung liegt als Systemprüfung nicht darin, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden, und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind.

Die in der RMS-Beschreibung für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] dargestellten Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. Dies umfasst auch die Überwachung durch das RMS, ob die von den gesetzlichen Vertretern implementierten Risikosteuerungsmaßnahmen geeignet sind, mit hinreichender Sicherheit die Risikostrategie umzusetzen und die Ziele des RMS zu erreichen.

Die Wirksamkeit des RMS ist dann gegeben, wenn die Regelungen in den laufenden Geschäftsprozessen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortlichkeit in einem bestimmten Zeitraum wie vorgesehen eingehalten werden. Auch ein wirksames RMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, auftreten können, ohne systemseitig rechtzeitig erkannt und entsprechend den vom Unternehmen festgelegten Zielen des RMS gesteuert zu werden.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *Entwurfs eines IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW EQS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die im geprüften Zeitraum implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen … [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den an-

gewandten RMS-Grundsätzen … [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] wirksam waren.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld sowie über das Risikoprofil und die Risikomanagementorganisation des Unternehmens berücksichtigt. Wir haben die in der RMS-Beschreibung dargestellten Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und angemessen sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der RMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des RMS sowie zur Angemessenheit, Implementierung und Wirksamkeit des RMS schriftlich bestätigt.

C. Feststellungen zum Risikomanagementsystem

I. Konzeption des RMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[u.a. Beschreibung der angewandten RMS-Grundsätze]

Ausführungen zu den einzelnen RMS-Grundelementen:

- Risikokultur
- Ziele des RMS
- Organisation des RMS
- Risikoidentifikation
- Risikobewertung
- Risikosteuerung
- Risikokommunikation
- Überwachung und Verbesserung des RMS.

II. Feststellungen [und Empfehlungen]

a) Feststellungen, die zu einer Einschränkung, Versagung oder Nichterteilung des Prüfungsurteils geführt haben

[Da wir nur unzureichende Unterlagen und anderweitige Nachweise über die eingerichteten Regelungen des RMS für ... [Beschreibung des betreffenden Bereichs] erhalten haben, können wir die Angemessenheit und Wirksamkeit dieser Regelungen nicht beurteilen. Es kann daher nicht ausgeschlossen werden, dass das RMS insoweit nicht geeignet ist, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen.]

[b) sonstige Feststellungen

c) ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d) ggf. Hinweis auf nicht geprüfte sonstige Angaben in der RMS-Beschreibung

e) Empfehlungen].

D. Zusammenfassendes Prüfungsurteil

Unsere Prüfung hat zu der unter Abschn. C. II. dargestellten Einschränkung geführt.

Sofern das RMS in Bezug auf strategische Risiken Gegenstand des Prüfungsauftrags ist:

Mit dieser Einschränkung sind nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten strategischen Unternehmensziele entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Sofern das operative RMS Gegenstand des Prüfungsauftrags ist:

Mit dieser Einschränkung sind nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] in der RMS-Beschreibung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen in Übereinstimmung angemessen dargestellt,

- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Sofern das RMS sowohl in Bezug auf strategische Risiken als auch auf abgegrenzte Teilbereiche in Bezug auf operative Risiken Gegenstand des Prüfungsauftrags ist:

Mit dieser Einschränkung sind nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS und [Beschreibung des oder der abgegrenzten Teilbereiche(s) des RMS] in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der strategischen Unternehmensziele und der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung des oder der abgegrenzten Teilbereiche(s) des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die RMS-Beschreibung des für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] bei der Gesellschaft wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Regelungen erstrecken sich auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des RMS falsche Schlussfolgerungen gezogen werden.

Auch ein wirksames RMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, auftreten können, ohne systemseitig rechtzeitig erkannt und entsprechend den vom Unternehmen festgelegten Zielen des RMS gesteuert zu werden.

Ort, Datum, Unterschrift

Anlagen:

[RMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

2.3. Angemessenheitsprüfung

Bericht des unabhängigen Wirtschaftsprüfers

Prüfung der Angemessenheit und Implementierung des Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten RMS-Beschreibung der Angemessenheit und Implementierung ihres Risikomanagementsystems für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des RMS] durchzuführen.

Unter einem Risikomanagementsystem (RMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (Regelungen) zu verstehen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt. Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit und Implementierung der in der als Anlage 1 beigefügten RMS-Beschreibung aufgeführten Regelungen für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS].

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die [Gesellschaft] zur Verwendung [für interne Zwecke] gerichtet ist.

[*alternativ: Wir erstellen diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.*]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten RMS-Beschreibung enthaltenen Aussagen über ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten

Teilbereiche des zu prüfenden RMS]. Bei der Einrichtung des RMS wurden [Bezeichnung der RMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das RMS einschließlich der Dokumentation des RMS und für die Inhalte der RMS-Beschreibung liegt bei den gesetzlichen Vertretern der [Gesellschaft].

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der RMS-Beschreibung enthaltenen Aussagen zur Angemessenheit und Implementierung des ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche des zu prüfenden RMS] abzugeben. Die Zielsetzung der Prüfung liegt als Systemprüfung nicht darin, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden, und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind.

Die in der RMS-Beschreibung für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] dargestellten Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. Dies umfasst auch die Überwachung durch das RMS, ob die von den gesetzlichen Vertretern implementierten Risikosteuerungsmaßnahmen geeignet sind, mit hinreichender Sicherheit die Risikostrategie umzusetzen und die Ziele des RMS zu erreichen.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *Entwurfs eines IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW EQS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten. Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die zum geprüften Zeitpunkt implementierten Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und ob die dargestellten Regelungen in allen wesentlichen Belangen zum Zeitpunkt [Datum] implementiert waren.

Auftragsgemäß umfasste unsere Prüfung nicht die Beurteilung der Wirksamkeit der in der RMS-Beschreibung des Unternehmens dargestellten Regelungen.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld sowie über das Risikoprofil und die Risikomanagementorganisation des Unternehmens berücksichtigt. Wir haben die in der RMS-Beschreibung dargestellten

Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und angemessen sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der RMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des RMS sowie zur Angemessenheit und Implementierung des RMS schriftlich bestätigt.

C. Feststellungen zum Risikomanagementsystem

I. Konzeption des RMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[u.a. Beschreibung der angewandten RMS-Grundsätze]

Ausführungen zu den einzelnen RMS-Grundelementen:

- Risikokultur
- Ziele des RMS
- Organisation des RMS
- Risikoidentifikation
- Risikobewertung
- Risikosteuerung
- Risikokommunikation
- Überwachung und Verbesserung des RMS.

II. Feststellungen [und Empfehlungen]

[a. Feststellungen, die zu einer Einschränkung, Versagung oder Nichterteilung des Prüfungsurteils geführt haben

b. sonstige Feststellungen

c. ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d. ggf. Hinweis auf nicht geprüfte sonstige Angaben in der RMS-Beschreibung

e. Empfehlungen].

D. Zusammenfassendes Prüfungsurteil

Sofern das RMS in Bezug auf strategische Risiken Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die zum [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten strategischen Unternehmensziele entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - zum [Datum] implementiert.

Sofern das operative RMS Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die zum [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung der zu prüfenden abgegrenzten Teilbereiche des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - zum [Datum] implementiert.

Sofern das RMS sowohl in Bezug auf strategische Risiken als auch auf abgegrenzte Teilbereiche in Bezug auf operative Risiken Gegenstand des Prüfungsauftrags ist:

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die zum [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des strategischen RMS und [Beschreibung des oder der abgegrenzten Teilbereiche(s) des RMS] in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,

- waren die in der RMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten RMS-Grundsätzen ... [Bezeichnung der RMS-Grundsätze] in allen wesentlichen Belangen
  - geeignet, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der strategischen Unternehmensziele und der aus den strategischen Unternehmenszielen abgeleiteten operativen Ziele für [Beschreibung der abgegrenzten Teilbereiche des RMS] entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und
  - zum [Datum] implementiert.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die RMS-Beschreibung des für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] bei der Gesellschaft wurde zum [Datum] erstellt. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des RMS falsche Schlussfolgerungen gezogen werden.

Ort, Datum, Unterschrift

Anlagen:

[RMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

A2 - digital: Übersicht & Inhalt Gesetzesänderungen

CD-Pfad: MA_Gräber\Anhang\A2_Übersicht_Gesetzesänderungen

A3 - digital: Detailauswertung der Studien

CD-Pfad: MA_Gräber\Anhang\A3_Auswertung_Studien

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich vorliegende Masterarbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Stellen sind als solche kenntlich gemacht. Die Arbeit wurde bisher weder in gleicher noch in ähnlicher Form einer anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Dornbirn, am 04. Juli 2021 Pia Gräber