Integration von Risiken in Geschäftsprozessmodelle zur Gestaltung eines betrieblichen Informationssystems

DISSERTATION

zur Erlangung des akademischen Grades eines

Doktors der Wirtschaftswissenschaften

der

Fakultät Wirtschaftswissenschaften

der

Technischen Universität Dortmund

vorgelegt von

Diplom-Ökonom Tobias Thomas Anton

aus Bochum

Dortmund, August 2018

Danksagung

Die vorliegende Arbeit entstand im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik der Wirtschaftswissenschaftlichen Fakultät der Technischen Universität Dortmund.

Mein besonderer Dank gilt meinem Doktorvater Prof. Dr. Richard Lackes für die Betreuung dieser Arbeit und die wertvollen wissenschaftlichen Diskussionen, die dieses Werk mitgeprägt haben. Prof. Dr. Andreas Hoffjan danke ich sehr für die Übernahme des Zweitgutachtens und Prof. Dr. Johannes Weyer für die Mitarbeit in der Promotionskommission.

Meinen ehemaligen Kolleginnen und Kollegen des Lehrstuhls danke ich für das sehr kollegiale Verhältnis. Erik Frank danke ich für die spannenden und bereichernden Diskussionen rund um Start-ups und Unternehmertum, die stets eine willkommene Ablenkung boten. Besonderer Dank gilt Dr. Markus Siepermann für die häufig mehrstündigen wissenschaftlichen Diskussionen, die fast immer zu einem Erkenntnisgewinn führten.

Mein größter Dank gilt meiner Familie. Meinen Eltern danke ich für ihre Unterstützung aller meiner Vorhaben: Abitur, Unternehmensgründungen und Studium. Sie haben mit ihrem Beitrag den Grundstein für diese Arbeit gelegt. Meiner Frau Seena gebührt der allergrößte Dank, da sie mir auf der langen Zielgeraden den Rücken freigehalten hat, damit ich dieses Projekt abschließen konnte. Meinem Sohn Ajay danke ich dafür, dass er es mir anscheinend nicht übel nimmt, dass ich die ersten Monate seines Lebens fast jede freie Minute in die Fertigstellung der Dissertation investiert habe.

Bochum, im Sommer 2018 Tobias Anton

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
BCM	Business Continuity Management
BILReG	Bilanzrechtsreformgesetz
BPMN	Business Process Model and Notation
BRMS	Business Rule Management System
CDME	Conceptual Domain Model of the Extension
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CVaR	Conditional Value at Risk
DRS	Deutsche Rechnungslegung Standards
EPK	Ereignisgesteuerte Prozesskette
ERM	Enterprise Risk Management / Entity Relationship Model
ERP	Enterprise Resource Planning
ES	Expected Shortfall
ETA	Event Tree Analysis
FCM	Fuzzy-Cognitive Map
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
RMIS	Risikomanagement-Informationssystem
ROPN	Risikoorientierte Prozessnotation
ROPM	Risikoorientiertes Prozessmodell
RPN	Risikoprioritätsnummer
RUWK	Risiko-Ursache-Wirkungskette
SOX	Sarbanes-Oxley Act
UML	Unified Modelling Language
URL	Uniform Resource Locator
VaR	Value at Risk
WfMS	Workflow Managementsystem
XML	Extensible Markup Language

Symbolverzeichnis

G	Betriebswirtschaftliche Größe
I	Istwert
P	Planwert
R	Risikowert
S	Schaden
t, t’	Größe zum Zeitpunkt t bzw. t’
T	Größe in Periode T, die in Zeitpunkt t beginnt und in Zeitpunkt t’ endet: T=[t, t’]
Z	Systemzustand zum Zeitpunkt t
ΔZ_t	Differenzvektor zwischen Zustand Z_t und Z_{t+1}
α	Konfidenzniveau
σ	Standardabweichung

Teil I: Grundlagen des Risiko- und Prozessmanagements

1. Einführung

1.1. Motivation

Die Koordinierung der Wertschöpfungsaktivitäten vieler Unternehmen erfolgt heutzutage häufig in einer geschäftsprozessorientierten Vorgehensweise. Geschäftsprozessmanagementsysteme zur Steuerung der Prozesse haben sich daher als ein Führungsinstrument etabliert.[1] Sie zielen insbesondere darauf ab, Kosten zu reduzieren und Prozessverbesserungen zu erreichen.[2] Die Betrachtung von Unsicherheiten in den betrieblichen Abläufen wird von diesen Systemen jedoch vernachlässigt.[3] Eine Reihe von Beispielen macht allerdings deutlich, wie sehr betriebliche Prozesse vielfältigen Risiken ausgesetzt sind. Die UBS Bank musste zum Beispiel 2011 einen Verlust von über 2 Milliarden US-Dollar hinnehmen, da einzelne Bankmitarbeiter über Jahre bewusst Kontrollen im Handelsprozess mit ETF Fonds umgehen konnten. 2017 standen die Produktionsanlagen in drei BMW Werken für mehrere Tage still, da ein kleines Bauteil vom Zulieferer Bosch nicht geliefert werden konnte. Nicht zuletzt aufgrund solcher Negativbeispiele verlangen gesetzliche Vorgaben von Unternehmen ein systematisches Risikomanagement, welches Risiken dokumentiert und offenlegt, um Anteilseigner und Geschäftspartner über die Risikosituation eines Unternehmens zu informieren.[4] Darüber hinaus wird ein aktives und umfassendes Risikomanagement im Rahmen einer wertorientierten Unternehmensführung als notwendig angesehen.[5] Die aufgeführten Beispiele zeigen, dass eine abstrakte Risikobetrachtung auf strategischer Planungsebene nicht ausreicht. Die Analyse der Risiken muss vielmehr auf Geschäftsprozessebene erfolgen. Entsprechend verlangen regulatorische Vorgaben bereits explizit eine Fokussierung auf die Geschäftsprozesse.[6] Zum anderen bedingt ein umfassendes Risikomanagement die Einbeziehung der Geschäftsprozesse,[7] da sie das Zusammenspiel der beteiligten Ressourcen im Rahmen der Wertschöpfung vollständig beschreiben und Risiken in ihnen entstehen und wirksam werden.[8]

---

[1] Vgl. Scheer und Klueckmann 2009, S. 15.
[2] Vgl. Searle 2011.
[3] Vgl. Suriadi 2014, S. 934.
[4] Vgl. Lundqvist 2014, S. 393 ff.
[5] Vgl. Beasley et al. 2005, S. 523.
[6] Vgl. Hampel et al. 2004, S. 116; Karagiannis et al., 2007, S. 316 f.; Rieke 2009, S. 4; IDW 2017.
[7] Vgl. Jallow et al. 2007, S. 168.
[8] Vgl. Wolf und Runzheimer 2009, S. 111; Diederichs und Imhof 2011, S. 175; Suriadi et al. 2014, S. 935.

Als Konsequenz werden verstärkt Möglichkeiten gesucht das Prozess- und das Risikomanagement zu verbinden.[9] Trotz der offensichtlichen Notwendigkeit beide Disziplinen zu verknüpfen, existieren jedoch kaum Handlungsanweisungen, wie ein engeres Zusammenspiel beider erfolgen kann.[10] In der wissenschaftlichen Auseinandersetzung werden beide Disziplinen überwiegend getrennt voneinander betrachtet, obwohl eine Integration aus den genannten Gründen sinnvoll erscheint. In der betrieblichen Praxis werden die Aufgaben beider in der Regel durch unterschiedliche Abteilungen verantwortet, so dass eine engere Verzahnung bereits organisatorisch erschwert wird.

Zahlreiche Untersuchungen der letzten Jahre stellen entsprechend Ansätze vor, um beide Disziplinen methodisch zu verbinden.[11] Bei näherer Betrachtung der vorgeschlagenen Ansätze fallen jedoch mehrere Mängel auf. Vielfach erfolgt aus Sicht des Risikomanagements keine systematische Herleitung der Anforderungen. So werden häufig nur einzelne Aspekte wie z. B. die Modellierung von Einzelrisikos innerhalb eines Geschäftsprozessmodells als ausreichend angesehen. Eine weitergehende Betrachtung komplexer Risikophänomene innerhalb eines Prozesses wird meist vernachlässigt. Zusätzlich fehlt bei den vorgeschlagenen Konzepten vielfach eine formale Beschreibung des Ansatzes, wodurch die Zusammenhänge zwischen den Risikophänomenen untereinander und zu den Geschäftsprozesselementen nicht eindeutig spezifiziert werden. Darüber hinaus betrachtet der Großteil der Konzepte nur eine Verbindung zwischen einzelnen Phasen des Risiko- und Prozessmanagements, so dass es an einer phasenübergreifenden Integration mangelt.

[9] Vgl. Rikhardsson et al. 2006; Diederichs und Imhof 2011; Weiß und Winkelmann 2011.
[10] Vgl. Conforti et al. 2013, S. 2939.
[11] Vgl. im Folgenden Suriadi et al. 2014.

1.2. Ziel der Arbeit

Diese Arbeit thematisiert die zuvor genannten Defizite, indem sie das Ziel verfolgt, eine Notation zur Modellierung von Risikophänomenen in Geschäftsprozessmodellen zu entwickeln, welche dazu beiträgt die genannten Mängel zu überwinden. Konkret werden dabei die folgenden Forschungsfragen adressiert:

> **Forschungsfrage 1**: *Welche Anforderungen bestehen an eine Notation zur Modellierung von Risiken in Geschäftsprozessmodellen?*
> **Forschungsfrage 2**: *Welche Ansätze zur Integration von Risiken in Geschäftsprozesse existieren derzeit und durch welche Limitationen sind diese gekennzeichnet?*
> **Forschungsfrage 3**: *Wie ist eine Notation konkret zu gestalten, um die Modellierung von Risikophänomenen in Geschäftsprozessmodellen zu ermöglichen?*

Eine Risikoanalyse auf Geschäftsprozessebene und ein damit einhergehendes unternehmensweites Risikomanagement bedingen die Verarbeitung vieler Informationen, die nur IT-gestützt zufriedenstellend realisiert werden kann. Zusätzlich erfordert die mit den Risikophänomenen einhergehende Komplexität, z. B. durch Risiko-Ursache-Wirkungsketten und Risikokorrelationen, den Einsatz adäquater Software, um die Informationsverarbeitung zu unterstützen.[12] Entsprechend stellt sich die Frage, inwiefern bestehende Risikomanagement-Informationssysteme eine Verarbeitung von Risikophänomenen auf Geschäftsprozessebene unterstützen und wie eine solche generell realisiert werden kann. Daraus ergeben sich folgende weitere Forschungsfragen:

> **Forschungsfrage 4**: *Welche Anforderungen sollten Risikomanagement-Informationssysteme erfüllen?*
> **Forschungsfrage 5**: *Welchen Funktionsumfang bieten aktuelle Risikomanagement-Informationssysteme?*
> **Forschungsfrage 6**: *Wie ist ein Risikomanagement-Informationssystem zu gestalten, welches das Management von Risiken auf Geschäftsprozessebene ermöglicht?*

[12] Vgl. Reichmann und Kißler 2013, S. 201; Zhao et al. 2014, S. 922.

1.3. Gang der Untersuchung

Die vorliegende Arbeit gliedert sich in drei Teile auf. Im ersten Teil werden die Grundlagen des Risiko- und des Prozessmanagements behandelt. Im zweiten und dritten Kapitel werden dazu die Begriffe des Risikos und des Risikomanagements definiert und erörtert, um für die weitere Arbeit ein einheitliches Verständnis zu schaffen. In Kapitel Vier wird das Phasenmodell des Risikomanagements vorgestellt, welches üblicherweise in Literatur und Praxis genutzt wird, um die Aktivitäten dieser Disziplin zu strukturieren. Dabei werden systematisch für jede Phase die Ziele und die gängigen Methoden präsentiert. Kapitel Fünf beschäftigt sich mit den Vorteilen des Geschäftsprozessmanagements, dem Aufbau des üblichen Phasenmodels dieses Führungsinstruments und den gängigen Modellierungsmethoden zur Darstellung von Geschäftsprozessen.

In Teil Zwei der Arbeit wird eine Notation zur Modellierung von Risikophänomenen in Geschäftsprozessen konzipiert. Dazu werden in Kapitel Sechs zunächst die Vorteile einer engeren Verzahnung von Risiko- und Geschäftsprozessmanagement herausgestellt. Darauf aufbauend werden in Kapitel Sieben Anforderungen an die Notation abgeleitet, um dann die Standardnotation zur Modellierung von Geschäftsprozessen, die BPMN, um eine Risikosicht zu erweitern.

Der dritte Teil der Arbeit widmet sich der DV-Unterstützung des Risikomanagements. In Kapitel Acht werden Anforderungen an Risikomanagement-Informationssysteme (RMIS) aufgestellt, auf deren Basis eine empirische Analyse des Softwaremarktes für RMIS erfolgt. Hierbei werden Verbesserungspotentiale der Systeme herausgearbeitet. In Kapitel Neun erfolgt die Konzeption eines Risikomanagement-Informationssystems, welches das Management von Risiken auf Geschäftsprozessebene unterstützt. Abschließend werden in Kapitel Zehn die Ergebnisse der Arbeit zusammengefasst, Limitationen aufgeführt und ein Ausblick auf weitere Forschungspotentiale gegeben.

2. Das betriebswirtschaftliche Risiko

2.1. Überblick

Der Begriff des Risikos wird in Forschung und Praxis seit jeher kontrovers diskutiert und unterschiedlich ausgelegt.[13] Daher ist für die vorliegende Untersuchung zunächst eine Definition des zugrunde gelegten Risikobegriffs erforderlich. Je nach Forschungsdisziplin nähern sich die wissenschaftlichen Ausführungen der Definition des Risikos aus unterschiedlichen Blickwinkeln und kommen daher zu nicht einheitlichen Definitionsweisen.[14] Dies gilt auch innerhalb der Disziplinen wie z. B. der betriebswirtschaftlichen Forschung.[15] Damit für die vorliegende Arbeit ein einheitliches Verständnis des Risikos geschaffen werden kann, werden die vorhandenen betriebswirtschaftlichen Auffassungen zum Risikobegriff zunächst genauer betrachtet und eingeordnet.

2.2. Risikoauffassungen in der betriebswirtschaftlichen Literatur

Die bestehenden Auffassungen des betriebswirtschaftlichen Risikos lassen sich in ursachenbezogene und wirkungsbezogene Risikoauffassungen einordnen.[16] Ursachenbezogene Auffassungen stellen die Gründe für eine zukünftige unbekannte Entwicklung in den Mittelpunkt der Risikobetrachtung. Dabei kann ein Risiko aus zwei Gründen entstehen. Zum einen aus einem Mangel an Informationen (informationsorientierte Sicht) und zum anderen aus der Fehlentscheidung eines Entscheidungsträgers (entscheidungsorientierte Sicht). Die informationsorientierte Sicht stellt heraus, dass Entscheidungen in einem Zustand unvollständiger Information getroffen werden und daraus ein Risiko resultiert. Dabei unterscheidet ein Großteil der Autoren zwei Entscheidungszustände der informationsorientierten Sicht:

a) Einen Entscheidungszustand mit bekannten Wahrscheinlichkeiten der Entscheidungsfolgen.
b) Einen Entscheidungszustand mit unbekannten Wahrscheinlichkeiten über die Folgen der Entscheidung.

---

[13] Renn 1998, S. 50; Merkelsen 2011; Aven 2012.
[14] Vgl. Jonen 2006, S. 1 f.; Aven und Renn 2009 .
[15] Vgl. Philipp 1967, S. 34 ff.; Imboden 1983, S. 40 ff.; Schuy 1989, S. 10 f.; Rogler 2002, S. 5 ff.; Schorcht und Brösel 2005, S. 8 f.
[16] Vgl. Braun 1984, S. 22; Siepermann 2008, S. 11; Wolf 2010, S. 110.

Eine Entscheidung mit bekannten Wahrscheinlichkeiten der Ergebnisse wird dabei häufig als Entscheidung unter Risiko und eine Entscheidung mit unbekannten Wahrscheinlichkeiten der Ergebnisse als Entscheidung unter Unsicherheit bezeichnet.[17]

Im Gegensatz zu den Vertretern der informationsorientierten Sicht sehen die Vertreter der entscheidungsorientierten Sicht das Risiko allein als Gefahr der Fehlentscheidung des Entscheidungsträgers an.[18] Hier steht die subjektive Entscheidung des Entscheidungsträgers im Fokus.[19] Für gewöhnlich stehen dem Entscheider zum Zeitpunkt einer Entscheidung mehrere Handlungsalternativen zur Verfügung. Da die zukünftige Entwicklung dieser Alternativen mehrheitlich mit Unsicherheit belegt ist, sehen die Vertreter dieses Risikoverständnisses das Risiko in der mit Unsicherheit behafteten Wahl einer Alternative im Entscheidungszeitpunkt. Eine im Nachhinein als nicht optimal getroffene Wahl wird als Fehlentscheidung angesehen und allein der Wahl einer falschen Alternative durch den Entscheider im Entscheidungszeitpunkt zugerechnet. Das Risiko entsteht nach dieser Ansicht also bereits mit der Entscheidung.[20] Dabei wird nicht berücksichtigt, warum diese Fehlentscheidung entsteht, wie es bei der informationsorientierten Sichtweise explizit (Informationsmangel) getan wird.

Neben den ursachenbezogenen Risikoauffassungen beschreiben die wirkungsbezogenen Risikoauffassungen das Risiko als eine Abweichung von einem geplanten Zielwert oder Zielzustand.[21] Dabei wird davon ausgegangen, dass Erwartungen über Systemzustände bzw. Planwerte für messbare Größen (z. B. Umsatz, Absatzmenge o. ä.) existieren und die tatsächlichen Realisierungen der Zielgrößen von den Erwartungen abweichen.[22] Bei der wirkungsorientierten Sicht wird ein reines und ein spekulatives Risiko unterschieden (siehe Abbildung 1). Das reine Risiko bezeichnet dabei weitestgehend versicherbare Risiken. Es steht somit für Gefahren, die bei einem Eintritt einen direkten Vermögensverlust bewirken (z. B. Maschinen- oder Gebäudeschäden durch Feuer).[23] Nach diesem Verständnis ist ein Risiko also die Möglichkeit eines Schadens. Das Risiko wird als „reines Risiko“ bezeichnet, da es nur negative Auswirkungen berücksichtigt. Positive Abweichungen von einem Zielzustand in Form eines Ge-

[17] Vgl. Streitferdt 1973, S. 6; Imboden 1983, S. 47 ff.; Hermann 1996, S. 11.
[18] Siepermann 2008, S. 13.
[19] Vgl. Schuy 1989, S. 16 f.
[20] Vgl. Schuy 1989, S. 16; Philipp 1967, S. 37 f.
[21] Vgl. Oberparleiter 1955, S. 100; Bussmann 1955, S. 12; Braun 1984, S. 23; Erben 2000, S. 7; Siepermann 2008, S. 13 f.
[22] Vgl. Head 1967, S. 210; Berkau 2007, S. 153.
[23] Vgl. Walther 1953, S. 9; Christians 2006, S. 203; Diederichs 2010, S. 192.

winns werden nicht berücksichtigt.[24] Demgegenüber steht das spekulative Risiko, welches häufig nicht versicherbar ist und aus unternehmerischem Handeln heraus entsteht. Es ist ein Risiko, welches sich durch die mögliche Abweichung von einem geplanten Zielzustand äußert und zunächst wertneutral ist.[25] Die Abweichung kann dabei in Bezug auf einen Planwert bzw. einen erwarteten Zustand sowohl negativ als auch positiv sein und wird in diesem Kontext auch als Risiko im engeren bzw. im weiteren Sinn bezeichnet.[26] Oftmals wird hierbei eine positive Abweichung (Risiko im weiteren Sinn) auch als Chance benannt und bei einer negativen Planabweichung (Risiko im engeren Sinn) bzw. Verlustgefahr vom eigentlichen Risiko gesprochen.[27]

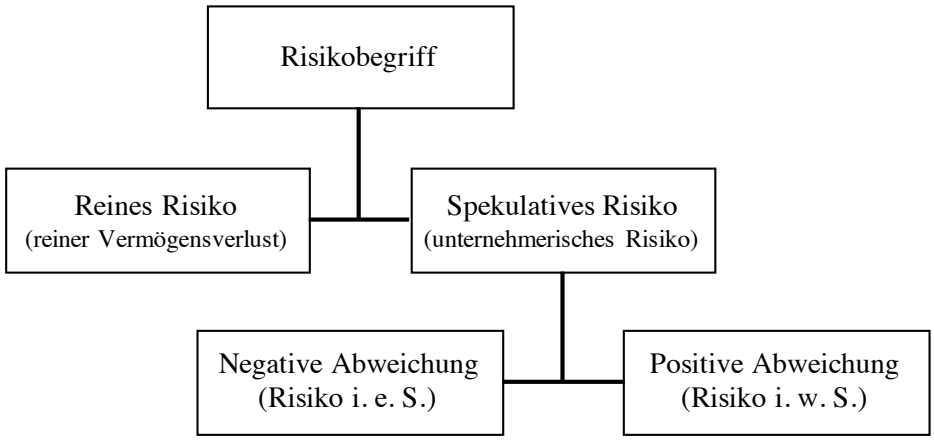


Abbildung 1: Systematik des Risikobegriffs[28]

In der internationalen Literatur wird für die Definition des Risikos vielfach auf das weit verbreitete COSO Enterprise Risk Management (ERM) Rahmenwerk oder den ISO Standard 31000 für Risikomanagement zurückgegriffen.[29] Das COSO ERM definiert Risiko als Möglichkeit, dass ein Ereignis eintritt, welches die gesetzten Ziele negativ beeinflusst. Der Risikomanagement Standard ISO 31000 versteht unter Risiko den „Effekt von Unsicherheit auf Ziele“. Beide folgen somit einer Risikoauffassung, die eine Wirkung auf eine Zielgröße inkludiert, wobei die Ursache (der Eintritt eines Ereignisses) mit Unsicherheit behaftet ist. Das

[24] Vgl. Rosenkranz und Missler-Behr 2005, S. 20.
[25] Vgl. Helten et al. 2000, S. 161 ff.; Scholz et al. 2012, S. 316.
[26] Vgl. Dörner und Bischof 1999, S. 446; Lück 2000, S. 315.
[27] Vgl. Braun 1984, S. 23 f.; Rogler 2002, S. 5; Diederichs 2012, S. 8 f.
[28] Vgl. Lück 2000, S.315.
[29] COSO 2004; ISO 31000 2009.

COSO ERM Rahmenwerk stellt heraus, dass es sich um eine negative Planabweichung handelt, womit diese Definition dem Risiko im engeren Sinn ähnelt. ISO 31000 legt nicht explizit fest wie der Effekt wirkt. Somit kann der Begriff Risiko im Sinne von ISO 31000 als aus Unsicherheit resultierende positive oder negative Zielabweichung verstanden werden. Dies entspricht dem Risiko im weiteren Sinn.

2.3. Risikoverständnis in der vorliegenden Arbeit

Zur Festlegung einer geeigneten Arbeitsdefinition des Risikobegriffs für die vorliegende Arbeit wird im Folgenden zunächst auf die Kritik an den aufgeführten Definitionen eingegangen. Die ursachenbezogenen Risikoauffassungen stellen Phänomene in den Mittelpunkt der Betrachtung, die als Grund einer ungewünschten Entwicklung ausgemacht werden können. Diese Sichtweise bedingt, dass ein Risiko durch eine unsichere Informationsstruktur oder eine Fehlentscheidung entsteht. Die Fehlentscheidung kann aufgrund der unsicheren Informationsstruktur oder durch unbewusstes Handeln des Entscheiders getroffen werden.[30] Dies ist aber nicht immer der Fall, da z. B. auch aufgrund unvorhersehbarer externer Risikoereignisse wie Umweltkatastrophen ein Risiko entstehen kann.[31]

Die wirkungsbezogenen Risikoauffassungen betrachten die Gefahr der Verfehlung von Planwerten als Risiko. Durch diese ex-post Sicht können Risiken quantifiziert werden, indem die Differenz von Plan- und Istwert als Risikogröße ermittelt wird. Diese Sichtweise wird unter anderem dahingehend kritisiert, dass Planabweichungen bei einer flexiblen Planung bereits berücksichtigt werden. Die Kritik wird an anderer Stelle aber entkräftet, da eine Entscheidung in einem Zeitpunkt t_0 sich an den in diesem Zeitpunkt vorliegenden Zielen und Informationen orientiert. Planungsanpassungen im Rahmen der flexiblen Planung erfolgen aber in einem späteren Zeitpunkt t_1 unter anderen (neuen) Informationsständen und daraus neu justierten Zielvorhaben.[32] Zur Untermauerung der Angemessenheit der wirkungsorientierten Risikoauffassung verweist Schuy auf die Dynamik des Risikobegriffs. Er definiert Risiko als „Gefahr einer negativen Abweichung von einem Ziel […]. Dabei handelt es sich um eine dynamische, im Zeitablauf veränderbare Größe“.[33] Damit geht er insbesondere auf den dynamischen Charakter von Risiken ein. Würde man das Risiko nur gemäß den ursachenorientierten Auffas-

[30] Vgl. Siepermann 2008, S. 13.
[31] Vgl. Rogler 2002, S. 8.
[32] Vgl. Siepermann 2008, S. 17.
[33] Vgl. Schuy 1989, S. 26.

sungen ohne eine Berücksichtigung der Zeitkomponente definieren, würde eine statische Analyse vorliegen. Dies würde bedeuten, dass eine Veränderung der Eintrittswahrscheinlichkeit und des Risikoausmaßes durch diverse Einflüsse niemals eintreten kann.[34] Da diese beiden Komponenten des Risikos sich aber verändern können, z. B. durch Gegensteuerungsmaßnahmen, ist eine dynamische Betrachtung sinnvoll bzw. eine wirkungsbezogene Risikoauffassung begründbar. Damit einher geht die Tatsache, dass Risiken mit subjektiver Zielsetzung verbunden sind.[35] Unterstellt man, dass ein Unternehmen nicht plant bzw. keine Erwartungen hat, so existiert nach dieser Definition für dieses Unternehmen kein Risiko. Als Kardinalziel jedes Unternehmens kann jedoch mindestens der Unternehmenserhalt unterstellt werden.[36] Somit kann bei einer vorherrschenden Inkonsistenz der Planung zumindest von einem impliziten Plan des Unternehmenserhalts ausgegangen werden, so dass auch bei nicht explizit in Fakten ausgedrückter Planung immer ein Risiko besteht.

In der vorliegenden Arbeit wird daher die Auffassung geteilt, dass ein Risiko die Gefahr einer negativen Abweichung einer Ist-Größe vor einer subjektiven Plangröße darstellt, wobei der Plan in einem Zeitpunkt t entstanden ist, in welchem Entscheidungen unter Unsicherheit über zukünftige Ereignisse im Zeitpunkt t' $(t' > t)$ getroffen wurden. Damit einher geht die Auffassung, dass eine positive Abweichung von diesem Plan als Chance zu verstehen ist. In der Literatur hat sich in den letzten Jahren diese Risikodefinition, die sowohl eine ursachenbezogene als auch eine wirkungsbezogenen Komponente enthält, etabliert.[37] Das Risiko entsteht aufgrund von Unsicherheiten im Zeitpunkt der Entscheidung und durch subjektive Erwartungen über einen zukünftigen Zustand. Es stellt die individuelle Gefahr einer negativen Abweichung des tatsächlichen Ist-Zustands vom ursprünglichen Plan-Zustand dar. Dieses Risikoverständnis hebt die Bedeutung objektiv gegebener Unsicherheiten und subjektiver Erwartungen hervor. Es unterstreicht, dass unterschiedliche Entscheider differenzierten Risikosituationen unterliegen und ein Risiko für einen Entscheider A, nicht zwingend ein Risiko für einen Entscheider B bedeuten muss, da sich insbesondere die gegebenen Informationsstände und die davon beeinflussten subjektiven Planzustände unterscheiden.

---

[34] Vgl. Schuy 1989, S. 26.
[35] Vgl. Streitferdt 1973, S. 7 f.; Lübbecke, Anton und Lackes 2013, S. 565.
[36] Vgl. Joos-Sachse 2006, S. 3.
[37] Vgl. Imboden 1983, S. 51; Helten 1994, S. 2; Siepermann 2008, S. 25; Scholz et al. 2012, S. 315.

2.4. Risikokorrelationen und Risiko-Ursache-Wirkungsketten

Ein Unternehmen ist üblicherweise nicht nur einem, sondern mehreren Risiken ausgesetzt,[38] die voneinander abhängig oder unabhängig sein können. Besteht zwischen zwei Risiken eine Abhängigkeit (Dependenz), so lässt sich der Grad des Zusammenhangs über die Korrelation ermitteln. Neben einseitigen Abhängigkeitsbeziehungen, können wechselseitige Abhängigkeiten zwischen Risiken bestehen (Interdependenzen), so dass sich Risiken gegenseitig verstärken oder abschwächen. Es lassen sich drei Arten von Risikobeziehungen unterscheiden:[39]

- Risikokomplementarität
- Risikokonkurrenz
- Risikoindifferenz

Als komplementär bezeichnet man Risiken, die sich durch ihr Zusammenwirken gegenseitig verstärken. Bezogen auf einen Schaden S bedeutet dies, dass der Gesamtschaden bei kumulativem Eintritt der Risiken RI_i größer ist, als die Summe der Schäden der Einzelrisiken RI_i bei isoliertem Risikoeintritt (Risikokomplementarität):[40]

$$S(RI_1 + RI_2) > S(RI_1) + S(RI_2)$$

Demgegenüber können Wechselwirkungen zwischen Risiken bestehen, die bei gleichzeitigem Auftreten zu einer gegenseitigen Abschwächung oder einer (teilweisen) Kompensation führen (Risikokonkurrenz):

$$S(RI_1 + RI_2) < S(RI_1) + S(RI_2)$$

Letztlich können Risiken unabhängig voneinander sein (Risikoindifferenz). Zwischen ihnen besteht keine Korrelation, so dass der kumulierte Gesamtschaden, der Summe der Einzelrisikoschäden entspricht:

---

[38] Vgl. Hempel und Offerhaus 2008, S. 4.
[39] Vgl. Löhr 2010, S. 39.
[40] Vgl. Burger und Buchart 2002, S. 4 f.

$$S(RI_1 + RI_2) = S(RI_1) + S(RI_2)$$

Aus einer Korrelation zwischen Einzelrisiken folgt nicht zwingend ein kausaler Zusammenhang. Ein solcher liegt vor, wenn ein Risiko den Eintritt eines anderen Risikos verursacht. Man spricht dann von einer Risiko-Ursache-Wirkungsbeziehung zwischen dem unabhängigen Risiko (Ursache) und dem kausal abhängigen Risiko (Wirkung).[41] Eine solche Wirkungsbeziehung ist durch einen stabilen Systemzustand Z_t im Zeitpunkt t gekennzeichnet, der durch Parameteränderungen ΔZ_t (Ursache) in einen neuen Systemzustand $Z_{t'}$ (Wirkung) überführt wird ($t' > t$). Die Parameteränderungen resultieren dabei aus unternehmensinternen oder externen Ereignissen. Liegt eine solche Ursache-Wirkungsbeziehung zwischen mehr als zwei Risiken vor, spricht man von einer Risiko-Ursache-Wirkungskette. Tritt z. B. ein ungeplanter Absatzrückgang ein, führt dieses eingetretene Absatzrisiko zu einem Umsatzrückgang, der wiederum ein Liquiditätsrisiko auslöst. Das Liquiditätsrisiko ist in diesem Fall kausal vom Absatzrisiko abhängig. Weitere vom Liquiditätsrisiko kausal abhängige Risiken, wie z. B. ein Beschaffungsrisiko aufgrund nicht bezahlter Rechnungen, können Bestandteil der Risiko-Ursache-Wirkungskette sein. Unternehmensweit können komplexe Beziehungen zwischen den Einzelrisiken die Risikosituation beeinflussen und den Umgang mit Risiken erschweren. Die Kenntnis der Risiko-Ursache-Wirkungsketten und der Risikokorrelationen ist daher von Interesse[42] und insbesondere für die Bestimmung des Gesamtrisikos sowie zur Einleitung adäquater Risikosteuerungsmaßnahmen relevant (siehe Kapitel 4).

2.5. Risikoarten

Aufgrund der Anzahl und Vielfältigkeit von Risiken bietet sich zu ihrer Handhabung eine Kategorisierung nach Risikoarten an. Durch eine angemessene Strukturierung von Risiken kann ein Überblick über die Risikolandschaft erzeugt und ihre Steuerung erleichtert werden.[43] In der Literatur entwickelten sich daher zahlreiche Ansätze der Risikokategorisierung.[44] Die Möglichkeiten der Kategorisierung sind allerdings so vielfältig und komplex wie die Risikophänomene selbst. Eine stets eindeutige Einordung eines Risikos in eine Kategorie kann somit

[41] Vgl. im Folgenden Siepermann 2008, S. 36 ff.
[42] Vgl. Diederichs 2010, S. 58 f.
[43] Vgl. Imboden 1983, S. 65.
[44] Vgl. Kalwait et al. 2008, S. 23; Siepermann 2008, S. 73; Verbano und Venturini 2011; Kaplan und Mikes 2012.

nicht immer überschneidungsfrei erfolgen.[45] So kann z. B. ein Risiko im Produktionsprozess ebenso der Kategorie *Interne Risiken* oder *Operative Risiken* als auch der Kategorie *Produktionsrisiken* zugeordnet werden. Ein Gliederungsvorschlag, der sich an den Dimensionen Entstehungs-/Wirkungsort bzw. -bereich, Zeithorizont, Umfang und Managementebene orientiert, ist in Abbildung 2 aufgeführt. Die internen Risiken entstehen aus dem Unternehmen heraus bzw. in seinem Handlungsfeld und stellen Risiken dar, die durch die Entscheidungen und Aktivitäten des Unternehmens und seiner Akteure ausgelöst werden.[46] Die externen Risiken hingegen stellen Risiken dar, die einen Einfluss auf das Unternehmen haben, jedoch außerhalb seines direkten Einflussbereiches entstehen. Auf ihr Eintreten hat das Unternehmen keinen direkten Einfluss und die Steuerungsmöglichkeiten sind begrenzt. Eine weitere Differenzierungsmöglichkeit mit Bezug zum Entstehungs- bzw. Wirkungsbereich von Risiken, bietet eine Unterscheidung nach finanz- und leistungswirtschaftlichen Risiken.[47] Weiterhin können sie anhand des konkreten Funktionsbereiches, in denen sie entstehen bzw. schlagend werden, kategorisiert werden.[48] Zu der Dimension Zeit lassen sich kurzfristige und langfristige Risiken zählen. Die Fristigkeit bezieht sich hierbei auf das Bestehen der Risiken. Manche Risiken bestehen nur für kurze Momente, z. B. für die Dauer eines Prozessdurchlaufs. Andere Risiken existieren über lange Zeiträume. Risikokategorien, die sich der Dimension Umfang zuordnen lassen, sind solche Kategorien, die sich auf den Grad der Auswirkung eines Risikos beziehen. Einzelrisiken sind Risiken, die sich auf einzelne Phänomene beziehen. Gesamtrisiken stellen aggregierte Einzelrisiken dar.[49] Eine weitere Kategorie innerhalb der Dimension Umfang lässt sich anhand der Bewertung der Risikoauswirkung treffen. So können Risiken z. B. als erfolgsbeeinflussend oder existenzgefährdend bewertet und entsprechend kategorisiert werden.[50] Operative Risiken umfassen alle Risiken, die in den Geschäftsprozessen entstehen bzw. schlagend werden können.[51] Dazu gehören z. B. Produktionsprobleme aufgrund von Lieferschwierigkeiten oder Personalausfällen.

---

[45] Vgl. Löhr 2010, S. 32; Diederichs 2012, S. 55.
[46] Vgl. Bussmann 1955, S. 21; Kalwait et al. 2008, S. 35.
[47] Vgl. Wengert und Schittenhelm 2013, S. 26.
[48] Vgl. Kajüter 2012, S. 20.
[49] Vgl. Kajüter 2012, S. 20.
[50] Vgl. Burger und Buchhart 2002, S.34.
[51] Vgl. Szabo 2012, S. 777.

Bereich/Ort	Internes Risiko / Externes Risiko
	Leistungswirtschaftliches Risiko / Finanzwirtschaftliches Risiko
	Funktionsbereich (Einkaufs-, Produktions-, Lager-, Absatzrisiko etc.)
Zeitbezug	Kurz-, Mittel- und Langfristiges Risiko
Umfang	Einzelrisiko / Gesamtrisiko
	Erfolgsbeeinflussendes / Existenzgefährdendes Risiko
Ebene	Operatives Risiko / Strategisches Risiko

Abbildung 2: Mögliche Kategorisierung von Risiken

Strategische Risiken hingegen umfassen Risikophänomene, die sich aufgrund der gewählten Strategie ergeben. Sie beinhalten solche Risiken, die im Rahmen von langfristig bindenden Entscheidungen entstehen können. Dazu gehören z. B. Risiken aufgrund der Wahl des Produktsortiments, der Wahl der Absatzmärkte und ähnliche Risiken. Ihre Auswirkungen sind bei einem Eintritt meist sehr umfassend, so dass sie länger nachwirken und zudem nicht schnell eingedämmt werden können. Ihr Auftreten ist zudem meist nicht unmittelbar erkennbar.[52] Die Schwierigkeit einer eindeutigen Kategorisierung zeigt sich auch hier. So können z. B. operative Risiken häufig auch den Kategorien *kurzfristige Risiken* oder *erfolgsbeeinflussende Risiken* und strategische Risiken den Kategorien *langfristige Risiken* und *existenzgefährdende Risiken* zugeordnet werden. Dabei soll nicht ausgeschlossen werden, dass auch operative Risiken langfristige Auswirkungen haben oder existenzgefährdend sein können bzw. strategische Risiken kurzfristiger Natur sowie erfolgsbeeinflussend sein können.

[52] Vgl. Diederichs et al. 2004b, S. 190.

3. Risikomanagement

3.1. Ursprung und Entwicklung

Der Begriff des Risikomanagements hat seinen Ursprung in den USA, wo im Rahmen des „Risk Managements“ der Umgang mit versicherbaren Risiken im Mittelpunkt stand.[53] Insbesondere beschäftigte sich das Risk Management anfänglich mit der Optimierung von Versicherungsverträgen.[54] Daher wurden die Begriffe Risk Management, Insurance Management und Insurance Handling in diesem Rahmen häufig synonym verwendet.[55] Im weiteren Verlauf erweiterte sich der Aufgabenbereich des Risk Management von einem reinen Versicherungsmanagement hin zu einem systematischen Umgang mit Risiken, wobei die Beschränkung auf die reinen, versicherbaren Risiken[56] meist beibehalten wurde.[57] Hierbei wurde erstmals ein prozessorientierter Ansatz gewählt, um Risiken zu identifizieren, zu bewerten und zu steuern.[58] Durch die zunehmende Bedeutung der Optimierung von Geschäftsabläufen in den 1990er Jahren und die Fokussierung auf die Steigerung des Unternehmenswertes nahm auch das Risikomanagement eine neue Rolle ein.[59] Globaler Wettbewerb, wachsende Prozesskomplexität und veränderte wirtschaftliche Rahmenbedingungen führten zu neuen Chancen, aber auch zu neuen Risiken, die ein „pro-aktives, systematisches und holistisches Risikomanagement“ erforderten.[60]

Im internationalen Kontext wird letzteres mit dem Begriff des Enterprise Risk Management (ERM) bezeichnet, dessen charakteristische Eigenschaft darin besteht, dass jegliche Unternehmensrisiken systematisch identifiziert, analysiert und gesteuert werden. Besonders herauszustellen ist zudem, dass im Rahmen des ERM auch eine Betrachtung der möglichen Chancen erfolgt. Es fokussiert also insbesondere eine ganzheitliche Betrachtung, indem jegliche Risiken und Chancen analysiert werden. Dabei wird dies nicht nur in einzelnen Abteilungen („Silo-Betrachtung“[61]), sondern unternehmensweit getan.[62] Dies schließt die Notwendigkeit einer

---

[53] Vgl. Braun 1984, S. 27 ff.
[54] Vgl. Braun 1984, S. 27; Siepermann 2008, S. 33.
[55] Vgl. Siepermann 2008, S. 33; Paetzmann 2012, S. 54.
[56] Zur Bedeutung des Begriffs der reinen Risiken siehe Kapitel 2.2.
[57] Vgl. Braun 1984, S. 29.
[58] Vgl. Verbano und Venturini 2011, S. 520.
[59] Vgl. Verbano und Venturini 2011, S. 520.
[60] Vgl. Hasenmüller 2009, S. 11.
[61] Vgl. Liebenberg und Hoyt 2003, S. 37; Arena et al. 2011, S. 783.
[62] Vgl. Harrington et al. 2002, S. 71; Grace et al. 2015, S. 289 f.

bereichsübergreifenden und somit prozessweiten Sicht auf Risiko- und Chancenzusammenhänge ein. Aus diesem Grund wird auch von integriertem, holistischem oder ganzheitlichem Risikomanagement gesprochen.[63] Während die traditionellen Risikomanagementansätze auf das Management versicherbarer Risiken und die Optimierung der dazugehörigen Verträge abzielten, zielt das ERM im Sinne der Ganzheitlichkeit auf die Betrachtung strategischer, finanzieller sowie operativer Risiken und natürlichen Gefährdungen ab.[64] Obwohl weithin unterschiedliche Auslegungen des ERM Begriffs zu finden sind,[65] bildete sich in der jüngeren Vergangenheit ein einheitliches Verständnis über seine Kernbestandteile heraus. Zum einen ist dies die Ansicht, dass Risiken nicht generell als zu vermeidendes Problem angesehen werden, sondern durch ein adäquates Risikomanagement gesteuert werden sollten, um Chancen zu nutzen.[66] Zum anderen fokussiert sich das ERM sowohl auf die Steuerung von strategischen als auch von operativen Risiken. Beide leiten sich aus der Unternehmensplanung ab, da diese die strategischen und operativen Ziele des Unternehmens vorgibt.[67]

Im Rahmen des strategischen Risikomanagements wird das Ziel verfolgt, die Kardinalziele des Erhalts und der Weiterentwicklung des Unternehmens in ihrer Erreichung zu unterstützen.[68] Weiterhin wird das frühzeitige Erkennen von Chancen und Risiken als wichtigste Funktion des strategischen Risikomanagements genannt.[69] Dazu gehören die risikoorientierte Prüfung der Unternehmensgrundsätze und der strategischen Planung, da diese bereits Quellen von Risiken sein können.[70] Als Aufgabe des strategischen Risikomanagements wird auch die Verankerung eines Risikobewusstseins in der Organisation angesehen.[71] Durch die Risikoeinstellung der Unternehmensleitung und die durch sie festgelegten risikobezogenen Rahmenbedingungen und Ziele leiten sich unternehmensweite Maßnahmen und Verhaltensweisen im Umgang mit Risiken ab. Dieses als Risikokultur bezeichnete Bewusstsein ist Bestandteil der Unternehmenskultur und drückt aus, welches Risikobewusstsein im Unternehmen vorherrscht. Die Risikokultur beinhaltet somit die von der Unternehmensleitung vorgelebten

---

[63] Vgl. McShane et al. 2011, S. 644; Verbano und Venturini 2011, S. 520.
[64] Vgl. McShane et al. 2011, S. 644; Schiller und Prpich 2014, S. 999.
[65] Vgl. Bromiley et al. 2015, S. 265 f.
[66] Vgl. Bromiley et al. 2015, S. 268.
[67] Vgl. Braun 1984, S. 43; Rommelfanger 2008, S. 18.
[68] Vgl. Diederichs 2012, S. 10 f.; Zur Diskussion, dass unternehmerisches Handeln stets zielgerichtet ist, vgl. Braun 1984, S. 41 ff.
[69] Vgl. Braun 1984, S. 99.
[70] Vgl. Braun 1984, S. 101.
[71] Vgl. Wengert und Schittenhelm 2013, S. 12 ff.

grundlegenden Normen und Werte im Umgang mit Risiken. Sie legt fest, wie mit Risiken umgegangen wird und wie viel Risiko akzeptabel ist.[72] Ähnlich der Unternehmenskultur bildet sich die Risikokultur aus drei Ebenen heraus.[73] Dies sind nicht direkt sichtbare generelle Basisannahmen, das Normen- und Wertesystem und das Symbolsystem des Unternehmens. Zu den Basisannahmen zählt die grundsätzliche Einstellung der Unternehmensmitglieder gegenüber Risiken.[74] Das Normen- und Wertegerüst beinhaltet konkrete Verhaltensregeln, die innerhalb der Organisation üblich sind. Das Symbolsystem umfasst alle konkret sichtbaren Elemente der Risikokultur, wie z. B. ein Risikohandbuch.[75] Eine gute Risikokultur ist geprägt durch gegenseitiges Vertrauen und einem gemeinsamen Verständnis für die Bedeutung des Risikomanagements.[76] Die Risikokultur kann bereits durch die organisatorische Einbindung des Risikomanagements in die Aufbauorganisation gefördert werden.[77] Weiterhin werden folgende Aspekte als förderlich angesehen:[78]

- Einbindung aller Beteiligten in allen Phasen des Risikomanagementprozesses
- Lernen aus vergangenen Risikosteuerungsmaßnahmen und Risikoereignissen
- Klare Verantwortlichkeiten und Rechenschaftspflicht
- Eine offene Kommunikation von Risikoaspekten und Erkenntnissen

Neben der Unterstützung des Aufbaus einer Risikokultur im Sinne des Unternehmens, ist die Implementierung geeigneter Instrumente zum Umgang mit Risiken eine weitere Aufgabe des strategischen Risikomanagements.[79] Ein wesentliches Instrument dabei ist ein Risikohandbuch, welches die grundsätzlichen Eigenschaften des Risikomanagements der Unternehmung beschreibt. Hierin wird z. B. der Aufbau des Risikomanagementsystems erläutert, relevante Begriffe definiert und die Ziele des Risikomanagements aufgeführt. Es liefert die Vorgaben für den Ablauf des operativen Risikomanagements. Dazu gehören die Festlegung der Metho-

[72] Vgl. Hoitsch et al. 2005, S. 126.
[73] Vgl. Bungartz 2006, S. 171 f.
[74] Vgl. Rossiter 2001, S. 45.
[75] Vgl. Bungartz 2006, S. 171.
[76] Vgl. Hopkin 2015, S. 110.
[77] Vgl. Wengert und Schittenhelm 2013, S. 13 ff.
[78] Vgl. Hopkin 2015, S. 110 f.
[79] Vgl. Wengert und Schittenhelm 2013, S. 15.

den zur Risikoidentifizierung, Risikoquantifizierung, Risikobeurteilung, Risikosteuerung und Risikoüberwachung.[80]

Gegenstand des operativen Risikomanagements[81] ist die tatsächliche Ausgestaltung des Risikomanagements im Unternehmensalltag. Es hat die Aufgabe operative Risiken zu identifizieren, zu quantifizieren, zu bewerten, mittels Maßnahmen zu steuern und zu überwachen. Zu den operativen Risiken gehören im Allgemeinen alle Risiken, die von internen Prozessen, Personen, Systemen und externen Ereignissen ausgehen.[82] Es zielt daher insbesondere auf den Umgang mit Risiken in den Geschäftsprozessen ab.[83] In welchem Umfang dies geschieht leitet sich individuell aus den Vorgaben des strategischen Risikomanagements ab.

3.2. Gesetzliche und regulatorische Bedeutung

3.2.1. Gesetzliche und regulatorische Vorgaben

Diverse Unternehmensskandale, internationale Finanz- und Wirtschaftskrisen und eine zunehmende Anzahl an Firmeninsolvenzen haben Gesetzgeber weltweit dazu bewegt, regulatorische Maßnahmen durchzuführen, um Unternehmen zu einem risikobewussten Handeln zu verpflichten. Für den US-amerikanischen Wirtschaftsraum ist hierbei insbesondere der Sarbanes-Oxley Act[84] (SOX) und für Deutschland das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zu nennen.[85] Beide Gesetzestexte verpflichten Kapitalgesellschaften zu Risikomanagementmaßnahmen. Unternehmen dieser Gesellschaftsform waren insbesondere von Bilanzfälschungen und Zusammenbrüchen in den 1990er Jahren betroffen. Prominente Beispiele sind Enron, Worldcom,[86] die Barings Bank[87] und der Kirch Konzern[88]. In den USA führten insbesondere Betrugsskandale bezüglich der Finanzlage von Firmen zur Einführung des SOX. Sein Ziel ist es sicherzustellen, dass an US-Börsen gelistete Unternehmen akkurate Informationen über ihre Finanzlage veröffentlichen.[89] In diesem Rahmen fordert der Act konkret, dass der Vorstandsvorsitzende und der Finanzvorstand in jedem Quar-

[80] Vgl. Ebert 2013, S.21; Wengert und Schittenhelm 2013, S. 16 ff.
[81] Im angelsächsischen Raum wird von „operational risk“ gesprochen. Vgl. Boatright 2011, S. 153.
[82] Vgl. Basel Committee on Banking Supervision 2001, S. 2.
[83] Vgl. Brink 2007, S.182.
[84] Vgl. United States of America 2002.
[85] Vgl. Bundesrepublik Deutschland 1998.
[86] Vgl. Zhao et al. 2014, S. 816.
[87] Vgl. Engels und Cluse 2007, S. 21.
[88] Vgl. Erben 2007, S. 45 ff.
[89] Vgl. Hopkin 2015, S. 366.

tals- oder Jahresabschlussbericht per Unterschrift versichern, dass nach bestem Wissen nur wahrheitsgemäße Aussagen in den Berichten veröffentlicht werden.[90] Weiterhin verpflichtet das Gesetz alle unterzeichnenden Vorstände zur Einrichtung und zum Betrieb eines internen Kontrollsystems. Unregelmäßigkeiten sind dem Wirtschaftsprüfer und dem Audit Komitee mitzuteilen.[91] Insgesamt erhielten neben den Vorständen auch die Wirtschaftsprüfer mehr Verantwortung. Sie sind unter anderem dazu verpflichtet das interne Kontrollsystem des geprüften Unternehmens am Ende des Fiskaljahres zu bewerten.[92] Der SOX gibt vor, dass ein erprobtes Risikomanagement Rahmenwerk verwendet werden soll, um Risiken in der Finanzberichterstattung aufzudecken.[93] Konkret wird auf das COSO Internal Control Framework (COSO-IC) verwiesen[94], welches Empfehlungen zum Umgang mit Risiken enthält.[95] Somit besteht hier ein direkter Zusammenhang zum Risikomanagement, obwohl das SOX sich auf interne Kontrollsysteme mit dem Fokus auf finanzielle Auskünfte bezieht. Die enge Verbindung von internen Kontrollsystemen und Risikomanagementsystemen schlägt sich insbesondere in dem 2004 vorgestellten COSO Enterprise Risk Management Framework (COSO ERM) nieder, welches das COSO-IC integriert und um Elemente des Risikomanagements ergänzt.[96]

In Deutschland wurde 1998 im Zuge der Häufung von Unternehmensinsolvenzen das KonTraG verabschiedet. Es ist ein Artikelgesetz, welches Änderungen an bestehenden Vorschriften vornahm. Dabei wurden insbesondere Regelungen aus dem Handelsgesetzbuch und dem Aktiengesetz geändert. Ziel der Gesetzesänderungen war es, die Unternehmen dazu zu verpflichten, ein System einzuführen, welches hilft, frühzeitig bestandsgefährdende Entwicklungen erkennen zu können.[97] Weiterhin sollten die Interessen von Anteilseignern verstärkt berücksichtigt werden.[98] Mit diesen Maßnahmen war die Hoffnung verbunden, dass ein frühzeitiges Aufdecken von Risiken dazu führt, dass die Erfolgsaussichten unternehmerischer Aktivitäten besser bewertet werden können und dass Anleger rechtzeitig über die Entwicklung des

[90] Vgl. Sarbanes-Oxley Act 2002, Section 302.
[91] Vgl. Sarbanes-Oxley Act 2002, Section 302; Hempel und Offerhaus 2008, S.9.
[92] Vgl. Sarbanes-Oxley Act 2002, Section 404.
[93] Vgl. Hopkin 2015, S. 366.
[94] Vgl. U.S. SEC Final Rule 2003.
[95] Für eine detaillierte Beschreibung von Rahmenwerken zum Risikomanagement siehe Kapitel 3.2.2.
[96] Vgl. Ruud und Sommer 2006, S. 130.
[97] Vgl. Hommelhoff und Mattheus 2000, S. 8.
[98] Vgl. Henschel 2010, S. 5.

Unternehmens informiert sind, um gegebenenfalls ihre Investmententscheidung überdenken zu können und sich vor Verlusten zu schützen.[99] Das KonTraG verlangt konkret, dass der Vorstand von Aktiengesellschaften geeignete Maßnahmen zu treffen hat, „damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden".[100] Das reine Erkennen von Risiken impliziert, dass über diese im Falle einer Gefährdung auch an die Kontrollgremien zu berichten ist. Das KonTraG fordert somit indirekt eine Risikoberichterstattung.[101] Sobald über Risiken berichtet wird, ist wiederum davon auszugehen, dass vom Aufsichtsrat geeignete Maßnahmen gefordert werden, um die Risiken zu handhaben. Aus der Forderung nach der Einführung eines Risikofrüherkennungssystems ergibt sich somit bereits indirekt die Notwendigkeit der Einführung einzelner Bestandteile eines Risikomanagementsystems, auch wenn ein solches im Allgemeinen umfassender gestaltet ist. Neben den Anforderungen an die Vorstände verpflichtet das KonTraG explizit die bestellten Wirtschaftsprüfer zur Prüfung und Bescheinigung der Funktionsfähigkeit und Eignung des vom Vorstand implementierten Risikofrüherkennungssystems. So muss gemäß des im KonTraG erneuerten § 317 Absatz 4 des Handelsgesetzbuches der Abschlussprüfer beurteilen, ob der Vorstand die Maßnahmen zur frühzeitigen Erkennung von gefährdenden Entwicklungen umgesetzt hat und diese geeignet sind.[102] Daher enthalten gängige Wirtschaftsprüfungsstandards entsprechende Anforderungen an das im KonTraG geforderte Risikofrüherkennungssystem. Die zuvor erwähnten indirekt geforderten Bestandteile schlagen sich in diesen Prüfungsstandards nieder. So fordert der deutsche Prüfungsstandard IDW PS 340, dass geprüft werden soll, ob alle „wesentlichen Risiken […] frühzeitig erfasst, bewertet und kommuniziert werden".[103] Weiter muss in der Prüfung beurteilt werden, ob die getroffenen organisatorischen Maßnahmen das Risikobewusstsein der Mitarbeiter schärfen und gleichzeitig so unmissverständlich sind, dass sie als Handlungsanweisungen (Risikosteuerungsmaßnahmen) „verstanden und umgesetzt werden können".[104] Somit wird hier verlangt, dass im Rahmen des Risikomanagements eine Risikoidentifizierung, eine Risikobeurteilung und eine Risikokommunikation stattfinden. Die Kommunikation muss dabei so gestaltet werden, dass eine Risikokultur in der Organisation herrscht, die

[99] Vgl. Hommelhoff und Mattheus 2000, S. 8.
[100] Vgl. KonTraG 1998, Artikel 1, Absatz 9.
[101] Vgl. Engels und Cluse 2007, S. 25.
[102] Vgl. KonTraG 1998, Artikel 2 Absatz 6.
[103] Vgl. IDW PS 340 (27), S. 10.
[104] Vgl. IDW PS 340 (28), S. 10.

ein risikobewusstes Handeln fördert und das allen Beteiligten bewusst ist, welche Maßnahmen im Rahmen der Risikosteuerung zu treffen sind. Das KonTraG bezieht sich bei den wesentlichen risikobezogenen Änderungen explizit auf Aktiengesellschaften, aber in der Begründung zum Gesetz verdeutlicht der Gesetzgeber, dass er von einer „Ausstrahlungswirkung“ auf andere Kapitalgesellschaften ausgeht, die sich in ihrer Struktur und Größe nicht sonderlich von einer Aktiengesellschaft unterscheiden.[105] Hierdurch und durch die aus dem KonTraG abgeleiteten Prüfungsstandards ist das KonTraG auch für andere Kapitalgesellschaften von Relevanz.

In den Folgejahren unterstrichen weitere Gesetze und Prüfungsstandards die Bedeutung des Risikomanagements für unterschiedliche unternehmerische Zielgruppen. Mit dem Gesetz zur Einführung internationaler Rechnungslegungsstandards und zur Sicherung der Qualität der Abschlussprüfung (Bilanzrechtsreformgesetz – BilReG) von 2004 wird das Handelsgesetzbuch (HGB) so geändert, dass der Gesetzgeber mittelgroße und große Kapitalgesellschaften zur klaren Ausweisung von Chancen und Risiken im Lagebericht unter Angabe der getroffenen Annahmen verpflichtet.[106] Weiterhin wird in HGB § 289 festgelegt, dass auf die Risikomanagementziele und -methoden eingegangen werden muss.[107]

Durch die vom Baseler Ausschuss für Bankenaufsicht formulierten Anforderungen an die Kreditvergabe (Basel I, II und III) werden Banken dazu verpflichtet, die Vergabe von Krediten an Unternehmen mit höheren Eigenkapitalrücklagen abzusichern, damit sie bei ausfallenden Krediten nicht in eine Schieflage geraten. Daraus resultieren für die kreditanfragenden Unternehmen höhere Anforderungen bezüglich des Nachweises ihrer Kreditwürdigkeit. Diese Anforderungen äußern sich wiederum in der Notwendigkeit ein Risikomanagementsystem einzuführen, um der prüfenden Bank bei der Kreditwürdigkeitsprüfung relevante Informationen zur Risikolage zur Verfügung stellen zu können.[108]

---

[105] Vgl. Deutscher Bundestag 1998, S. 15.
[106] Vgl. Diederichs 2012, S. 24.
[107] Vgl. HGB § 289 (2).
[108] Vgl. Reichling 2003, S.17.

3.2.2. Rahmenwerke des Risikomanagements

3.2.2.1. Überblick

Die Implementierung eines Risikomanagementsystems stellt für eine Organisation eine große Herausforderung dar. Mit der Entscheidung bzw. der gesetzlichen Verpflichtung ein Risikomanagementsystem einzuführen steht die Geschäftsleitung vor der Aufgabe, das System in die Organisation zu integrieren und für Akzeptanz sowie einen ordnungsgemäßen Ablauf des Risikomanagements zu sorgen. Dazu muss neben der organisatorischen Verankerung auch organisationsweit ein gemeinsames Grundverständnis hinsichtlich der Zielsetzung, dem strukturellen Aufbau und der verwendeten Begrifflichkeit, z. B. mittels Leitlinien, geschaffen werden.[109] Vielfach wird darauf verwiesen, dass ein Risikomanagementsystem nur vernünftig funktionieren kann, wenn es von allen Beteiligten akzeptiert und „gelebt" wird.[110] Ebenso häufig wird die Bedeutung der Akzeptanz durch das Management hervorgehoben. Sie hat eine unternehmensweite Ausstrahlungswirkung und wird daher als Voraussetzung angesehen, um auch in der Belegschaft Akzeptanz für das Risikomanagement zu schaffen. Nur so kann sich langfristig eine Risikokultur verbreiten, die in ihrer Ausgestaltung im Sinne der Geschäftsleitung ist.[111] Zur Unterstützung bei der Umsetzung und dem Betrieb eines Risikomanagementsystems existieren unterschiedliche Rahmenwerke sowie normative Risikomanagementgrundlagen mit Richtliniencharakter. Sie sollen helfen ein strukturiertes Vorgehen bei der Einführung und dem Betrieb des Systems einzuhalten, die Etablierung einer Risikokultur zu fördern und ein gemeinsames Grundverständnis zu schaffen.[112] Zum einen existieren auf spezielle Anwendungsfälle ausgerichtete Standards (z.B. ISO 14971 „Anwendung des Risikomanagements auf Medizinprodukte"), welche nur für einzelne Branchen Vorgaben und eine grobe Orientierung bieten. Zum anderen lassen sich allgemeingültig aufgebaute Rahmenwerke von jedem Unternehmen als Vorlage verwenden. Sie stellen dazu zunächst ein einheitliches Begriffsverständnis her, indem die wesentlichen Elemente des Risikomanagements definiert werden. Weiterhin geben sie einen strukturellen Rahmen vor, der eingrenzt, welche Aspekte zu beachten sind. Letztlich geben sie Handlungsempfehlungen auf Basis von „Best Practices", um die Unternehmen methodisch zu unterstützen.

---

[109] Vgl. Institute of Management Accountants 2011, S. 25 f.; Diederichs 2012, S. 14 f.
[110] Vgl. Ebert 2013, S. 163.
[111] Vgl. Bosetti 2015, S.86; Rochette 2009, S. 403.
[112] Vgl. Frigo und Anderson 2014, S. 50.

Von besonderer Relevanz sind die weithin bekannten und weltweit verbreiteten Rahmenwerke ISO Standard 31000 und das COSO ERM Framework.[113] Weitere allgemeine Rahmenwerke stellen vielfach nationale Adaptionen der beiden aufgeführten Rahmenwerke dar oder weisen nur geringe unterschiedliche Inhalte auf, so dass sie sich von ihren Kernaussagen her kaum unterscheiden (siehe Abbildung 3).[114] Teilweise sind Inhalte aus Vorgängern der aufgeführten Standards wie z. B. Vorversionen des AZN oder ONR in den internationalen ISO Standard eingeflossen. Mittlerweile beziehen sich die aktuellen Versionen dieser nationalen Standards allerdings auf den ISO Standard 31000.[115]

[113] Vgl. COSO 2004; ISO 2009.
[114] Vgl. Ale et al. 2009, S. 426; Gjerdrum und Peter 2011, S. 11.
[115] Vgl. Gjerdrum und Peter 2011, S. 8; Bosetti 2015, S. 82.

Standard / Rahmenwerk / Richtlinie[116]	Ziele / Inhalte	Zielgruppe	Autoren / Hrsg.	Anmerkungen
AMF Reference Framework	• Vermittlung von allgemeinen Prinzipien der internen Kontrolle und des Risikomanagements • Enthält Fragebögen zur internen Kontrolle und zum Risikomanagement, um bei der Berichterstellung zu unterstützen.	Insbesondere börsennotierte Unternehmen in Frankreich, jedoch auch kleine und mittelständische Unternehmen Frankreichs	Autorité des Marchés Financiers (AMF)	• Erstveröffentlichung 2010 • Orientiert sich an nationalen Regulierungsvorschriften, Empfehlungen aus Corporate Governance Berichten, europäischen Richtlinien und Inhalten von COSO ERM und ISO 31000.
Australian/New Zealand Standard 4360 – Risk Management	• Zielt auf die Vermittlung von grundlegenden Prinzipien und eines einheitlichen Prozesses für das Risikomanagement ab.	Jegliche Organisation in Australien und Neuseeland	Standards Australia and Standards New Zealand Technical Committee OB-007	• Erstveröffentlichung 2009 • Nationaler Fokus • Vorgängerversion war Vorläufer des ISO 31000[117] • Lokale Spezifikation des ISO 31000
A Risk Management Standard by FERMA	• Schaffung einheitlicher Terminologie bezüglich der verwendeten Begriffe • Prozess zur Durchführung des Risikomanagements und Leitfaden zur Schaffung einer Organisationsstruktur für das Risikomanagement	Jegliche (europäische) Organisationen	Federation of European Risk Management Association (FERMA)	• Erstveröffentlichung 2002 • Internationaler Fokus • Orientiert sich am Risk Management Standard (ARMS) der führenden Risikomanagement Organisationen Großbritanniens. • Nutzt das Vokabular des ISO/IEC Guide 73.
COSO's Enterprise Risk Management – Integrated Framework (COSO ERM)	• Schaffung eines einheitlichen Begriffsverständnisses und Leitfaden zur Umsetzung eines umfassenden Risikomanagementprozesses • Zielt darauf ab, durch Risikomanagement Werte zu schaffen.	Jegliche Organisation. Ursprünglich US-amerikanische Unternehmen.	Committee of Sponsoring Organizations of the Treadway Commission (COSO)	• Erstveröffentlichung 2004 • Ursprünglich nationaler Fokus, allerdings vielfach international adaptiert. • Hervorgegangen aus COSO IC Standard • Überarbeitung 2014 angestoßen

[116] Vgl. Autorité des Marchés Financiers (AMF) 2010; Standards Australia and Standards New Zealand Technical Committee OB-007 2009; Federation of European Risk Management Association 2002; Committee of Sponsoring Organizations of the Treadway Commission 2004; United Kingdom Financial Reporting Council 2014; International Organization for Standardization 2009; Institute of Directors in Southern Africa 2002; Austrian Standards Institute 2004 (exemplarische Auswahl ohne Anspruch auf Vollständigkeit).
[117] Vgl. Gjerdrum und Peter 2011, S. 8.

Standard / Rahmenwerk / Richtlinie[116]	Ziele / Inhalte	Zielgruppe	Autoren / Hrsg.	Anmerkungen
FRC Guidance	• Vermittlung von Best Practices im Risikomanagement • Anleitungen für Vorstände, was im Kontext des Risikomanagements zu beachten ist bzw. erwartet wird.	Primär Unternehmen, die an der Londoner Börse gelistet sind. Sekundär andere interessierte Unternehmen.	United Kingdom Financial Reporting Council (FRC)	• Erstveröffentlichung 2014 • Ersetzt unter anderem die Turnbull Guidance.
ISO 31000	• Allgemein gehaltene Norm mit groben Strukturierungs- und Umsetzungsvorgaben für das Risikomanagement[118] • Vorgabe eines prozessorientierten Vorgehens	Jegliche Organisationen	International Standards Organization (ISO)	• Erstveröffentlichung 2009 • Internationaler Fokus • Erstellt von hunderten Risikomanagementexperten weltweit.[119] • Ursprungsversion basiert auf AS/NSZ 4360.[120] • Nicht für externe Zertifizierung ausgelegt.[121]
King III Report	• Rahmenwerk für Corporate Governance und Risikomanagement • Risikomanagement sollte einem Prozess folgen. • Management ist verantwortlich für die Steuerung des Risikomanagements.	Südafrikanische Unternehmen	Institute of Directors in Southern Africa (IoDSA)	• Erstveröffentlichung 2002 • Nationaler Fokus • Unternehmen, die an der Börse Johannesburg gelistet sind, müssen erklären, inwiefern sie den Forderungen nachkommen.
ONR 49000	• konkrete Anleitungen zur Ausgestaltung des Risikomanagements auf Basis von ISO 31000	Organisationen aus Österreich und der Schweiz	Austrian Standards Institute	• Erstveröffentlichung 2004 • Nationaler Fokus • Heute österreichische Spezifikation der ISO 31000 mit Erweiterungen

Abbildung 3: Standards, Rahmenwerke und Richtlinien des Risikomanagements

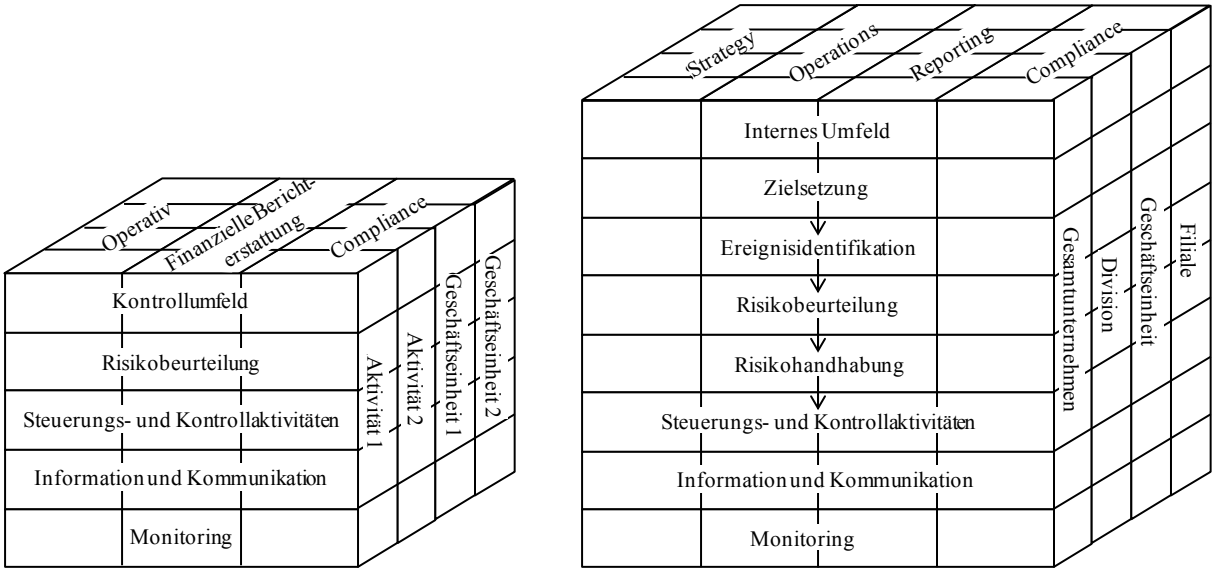
[118] Vgl. Brühwiler 2016, S. 163.
[119] Vgl. Purdy 2010, S. 881.
[120] Vgl. Bosetti 2015, S. 82; Gjerdrum und Peter 2011, S. 8.
[121] Vgl. Bosetti 2015, S. 82.

Aufgrund ihrer Bedeutung werden im Folgenden das COSO ERM und der ISO Standard 31000 näher vorgestellt. Ihre Rahmenvorgaben sind für die Betrachtung der im weiteren Verlauf dieser Arbeit analysierten Anforderungen an die Integration von Risiken in Prozessmodelle (siehe Kapitel 7) und an Risikomanagement-Informationssysteme (siehe Kapitel 8.2) relevant.

3.2.2.2. COSO ERM

Das im Jahr 2004 vorgestellte COSO Enterprise Risk Management – Integrated Framework (COSO ERM) wurde von PriceWaterhouseCoopers im Auftrag des Committee of Sponsoring Organizations of the Treadway Commission (COSO) entwickelt. Es sollte aufbauend auf dem existierenden Rahmenwerk für die Gestaltung interner Kontrollsysteme „COSO Internal Control – Integrated Framework“ als eigenständige Richtlinie für die immer mehr an Bedeutung erlangende Disziplin des Risikomanagements dienen. Ziel des COSO ERM ist die Bereitstellung eines Rahmens zur Identifizierung, Bewertung und Steuerung von Risiken für die Unternehmensführung. Bis zur Einführung von COSO ERM wurden insbesondere nur finanzielle und versicherbare Risiken in die Risikobetrachtung mit einbezogen. Mit der Einführung eines eigenständigen Rahmenwerks wurde auch der Umfang der Risikobetrachtung ausgeweitet, so dass COSO ERM einen ganzheitlichen, unternehmensweiten Ansatz des Risikomanagements verfolgt. Das COSO ERM Framework besteht aus acht Komponenten, die aufeinander aufbauen. Die acht Elemente des COSO ERM Rahmenwerks werden von COSO in einem dreidimensionalen Würfel dargestellt (siehe Abbildung 4). Auf diese Weise wird dem Risikomanagement nach COSO eine Struktur gegeben. Der Aufbau soll es einerseits erleichtern auf die Gesamtheit der Risikosituation zu blicken, es andererseits aber auch ermöglichen, den Fokus auf einzelne Aspekte wie z. B. auf die Betrachtung der Risikolage einer bestimmten Unternehmenseinheit zu richten. Neben den aufeinander aufbauenden Komponenten werden durch die Würfeldarstellung die Zielkategorien Strategie, Operations, Reporting und Compliance herausgestellt. Diese Kategorien legen die Bereiche fest, in denen Ziele formuliert werden sollen. Die dritte Achse legt fest, auf welchen Unternehmensbereich die Ziele sich beziehen. Die acht Komponenten beinhalten Vorgehensweisen und Methoden, die bei der Erreichung der Ziele unterstützen sollen. Die Komponente *Internes Umfeld* (*Internal Environment*) beschreibt dabei den Rahmen der Risikomanagementaktivitäten für die anwendende Organisation. Hier wird unter anderem festgelegt, welche Risikomanagementphilosophie im Unterneh-

men vorherrschen soll, wie risikoaffin bzw. risikoavers das Unternehmen ist und welchen Ansprüchen ein Kontrollgremium, wie ein Aufsichtsrat, genügen muss. Letzterer sollte über eine hohe fachliche Expertise verfügen und aktiv die Entscheidungen des Managements hinterfragen und kontrollieren. Weiterhin sollte er mindestens mehrheitlich bzw. bestenfalls überwiegend mit unternehmensexternen Personen besetzt werden, um möglichst unabhängig vom Management zu sein.



COSO Internal Control – Integrated Framework (1992)

COSO Enterprise Risk Management – Integrated Framework (2004)

Abbildung 4: COSO IC und ERM-Würfel[122]

COSO ERM definiert Risiko als die Möglichkeit, dass ein Ereignis auftritt, welches das Erreichen von Zielen nachteilig beeinträchtigt. Diese Definition beinhaltet indirekt die Annahme, dass Risiken auf den spezifischen Zielen einer Organisation beruhen. Somit ist es notwendig konkrete Ziele zu setzen, um Risiken überhaupt identifizieren, bewerten und steuern zu können. Gemäß COSO ERM müssen die festgelegten Ziele sich an den in der Komponente „Internes Kontrollsystem“ definierten Rahmenbedingungen orientieren. Dieses Festlegen der Ziele ist Bestandteil der Komponente „Zielsetzung“. Ausgehend von den strategischen Zielen sollen anschließend Operative-, Reporting- und Compliance-Ziele festgelegt werden. Daraus leiten sich jeweils Unterziele auf Geschäftseinheiten- und Aktivitätsebene ab. Diese müssen

[122] In Anlehnung an Ruud und Sommer 2006, S. 127.

mittels geeigneter Kennzahlen messbar sein und den Mitarbeitern müssen die Ziele und der jeweilige Zielerreichungsgrad bekannt sein. Auf Basis der Zielsetzung folgen im COSO ERM Elemente der klassischen Risikomanagementphasen. Die Komponenten Ereignisidentifizierung, Risikobeurteilung, Risikohandhabung sowie Steuerungs- und Kontrollaktivitäten spiegeln diese Phasen wider. Aufbauend auf den jeweiligen Zielsetzungen müssen zunächst im Rahmen der Ereignisidentifizierung, die Ereignisse ausfindig gemacht werden, welche die Zielerreichung unerwünscht beeinflussen könnten. Dazu nennt COSO ERM konkret Methoden zur Unterstützung bei der Ereignisidentifizierung. Dies sind z. B. Workshops und Interviews sowie Geschäftsprozessanalysen. Wie sich der Einfluss eines potentiellen positiven oder negativen Ereignisses konkret ausgestaltet, soll im Rahmen der Risikobeurteilung festgelegt werden. Zur Beurteilung der Risiken ist zunächst deren Quantifizierung notwendig (siehe Kapitel 4.3). COSO ERM nennt die Möglichkeiten einer quantitativen oder qualitativen Bemessung. Bei Kenntnissen über die Eintrittswahrscheinlichkeit und das Schadensausmaß ist eine quantitative Bemessung anzustreben. Da vielfach diese Kenntnis in der Praxis nicht vorliegt, solle in diesen Fällen eine qualitative Einschätzung vorgenommen werden. Bei Vorliegen von Vergangenheitsdaten können diese für die Quantifizierung verwendet werden, jedoch sollte mit Prognosen auf Basis von Vergangenheitsdaten vorsichtig umgegangen werden, da die Risikoeinflussfaktoren einem stetigen Wandel unterliegen. Insbesondere wird die Bedeutung der Bemessung und Bewertung von Risikointerdependenzen und Risiko-Ursache-Wirkungsketten von COSO ERM hervorgehoben. Dort wo Risiken nacheinander oder in Kombination auftreten, müssen sie zusammen betrachtet werden und ihre Quantifizierung und Bewertung bzw. die gemeinsame Eintrittswahrscheinlichkeit und das verbundene Schadensausmaß bestimmt werden, da sich durch eine zusammengefasste Betrachtung eine höhere Bedeutung ergeben kann als bei einer Einzelbetrachtung der Risiken.

Im Rahmen der Risikohandhabung sollen Maßnahmen zur Steuerung der identifizierten und bewerteten Risiken festgelegt werden. Dabei nennt COSO ERM die aus den Risikomanagementphasen bekannten Alternativen (siehe Kapitel 4.5). Im Rahmen der Maßnahmenfestlegung sollen insbesondere auch die Auswirkungen der Maßnahmen berücksichtigt, eine Kosten-Nutzen-Betrachtung durchgeführt und mögliche Alternativen der Zielerreichung, welche das Risiko umgehen, gesucht werden. Mittels Kontrollaktivitäten soll die ordnungsgemäße Durchführung der vom Management festgelegten Maßnahmen überprüft werden. Dazu sollen

Richtlinien und verbindliche Maßnahmen festgelegt und dokumentiert werden. Insbesondere wird auf die Bedeutung der Kontrolle von informationstechnischen Systemen hingewiesen, da diese die unternehmenskritischen Daten bereitstellen.

Die Framework-Komponente *Information und Kommunikation* geht auf die Bedeutung von dauerhaft aktueller Informationsbereitstellung ein, damit die Verantwortlichen ihren Pflichten im Rahmen des Risikomanagements nachkommen können. Dazu ist ein Risikomanagement-Informationssystem (RMIS) zu betreiben, welches aus diversen internen und externen Quellen Daten beziehen und aufbereiten kann. Insbesondere hebt COSO ERM hierbei die Bedeutung der Integration des RMIS mit bestehenden betrieblichen Informationssystemen wie z. B. einem ERP-System hervor, da diese bereits im Sinne des ganzheitlichen Ansatzes des Rahmenwerks unternehmensweit integriert sind und entsprechend Daten mit Bezug zur Wertschöpfungskette liefern können. Als weiterer Bestandteil der Komponente wird die Wichtigkeit der internen und externen Kommunikation im Rahmen des Risikomanagements aufgeführt. Intern muss das Management demnach die Ziele, die Risikoeinstellung, das gemeinsame Risikoverständnis und die Verantwortlichkeiten klar an alle Mitarbeiter kommunizieren. Im Rahmen der externen Risikokommunikation wird auf die Bedeutung einer angemessenen Kommunikation mit allen Stakeholdern verwiesen. Einerseits sollen das eigene Risikoverständnis und die Risikolage diesen vermittelt werden. Andererseits soll insbesondere Kunden und Zulieferern die Möglichkeit gegeben werden, risikobezogene Meldungen dem Unternehmen zukommen zu lassen, um daraus Implikationen zu schließen und Verbesserungen einzuleiten. Im Rahmen der Risikoberichterstattung an Prüfinstanzen und andere externe Parteien, sollen die Berichte entsprechend dem Informationsbedarf der Empfänger gestaltet sein. Die letzte Komponente im COSO ERM Framework bildet das Monitoring. Durch ständige Überwachungsaktivitäten oder punktuelle Auswertungen sollen vornehmlich bereits eingeleitete Risikosteuerungsmaßnahmen und Kontrollen auf ihre Wirksamkeit und möglichen Anpassungsbedarf hin überprüft werden. Die Prüfungen werden dabei z. B. durch die jeweiligen Funktions- oder Linienverantwortlichen oder durch interne Prüfer durchgeführt. COSO ERM listet Methoden zur Durchführung der Prüfungen auf, verweist auf die Bedeutung einer ordnungsgemäßen Dokumentation der Prüfaktivitäten und stellt fest, worüber und an wen die Ergebnisse der Überwachungsaktivitäten berichtet werden sollen.

Losgelöst vom COSO ERM Würfel liefert das Framework Vorgaben zur Gestaltung der Rollen und Verantwortlichkeiten im Rahmen des Risikomanagements. Demnach hat zunächst jedes Mitglied einer Organisation Verantwortung im Rahmen des Risikomanagements zu tragen. Besondere Aufgaben kommen dem Aufsichtsrat, der Geschäftsleitung, einem etwaig vorhandenen zentralen Risikomanager, dem CFO und der Internen Revision zu. Der Aufsichtsrat trägt die Verantwortung die Risikoberichte der Geschäftsleitung zu prüfen und Richtungsvorgaben für das Risikomanagement zu machen. Durch seinen Einfluss auf die Wahl der Geschäftsführung hat er bereits indirekten Einfluss auf die Gestaltung des Risikomanagements und kann so ausdrücken, welche risikomanagementbezogenen Erwartungen an die Geschäftsleitung gestellt werden. Die Geschäftsführung ist für alle Risikomanagementaktivitäten direkt verantwortlich. Dem CEO kommt dabei eine Schlüsselrolle zu. Er hat dafür zu sorgen, das *Interne Umfeld* im Sinne des Risikomanagementverständnisses der Organisation zu gestalten. Bei Auftreten von unerwünschten Entwicklungen ist es seine Aufgabe Gegenmaßnahmen anzustoßen bzw. die organisatorischen Strukturen dafür zu schaffen. Dazu wird empfohlen einen zentralen Risikomanager (*Chief Risk Officer*) einzusetzen, der die Rahmenbedingungen und Aufgaben des Risikomanagements mit den leitenden Angestellten diskutiert und vorgibt. Neben dem CEO spielt der CFO im Rahmen des Risikomanagements eine zentrale Rolle. Er trägt die Hauptverantwortung für die Finanzberichte und gestaltet die Rahmenbedingungen für die Berichterstattung. COSO ERM hebt die Bedeutung der Prüfer der Internen Revision hervor, da sie eine Schlüsselrolle in der Prüfung der Effektivität des Risikomanagementsystems spielen. Sie erkennen Schwachstellen und geben Vorschläge zur Verbesserung ab. In dieser Funktion unterstützen sie mit objektiven Einschätzungen die Geschäftsleitung und den Aufsichtsrat bei der Gestaltung und Anpassung des Risikomanagementsystems.

3.2.2.3. ISO 31000

Der 2009 verabschiedete internationale Standard für Risikomanagement ISO 31000 gliedert sich in fünf Bereiche. Darin werden zunächst der Umfang und das Ziel des Standards sowie grundlegende Risikomanagementbegriffe und Prinzipien geklärt. Den Kern des Standards bilden die Beschreibung des Aufbaus des Rahmenwerks und die Beschreibung der operativen Umsetzung mittels des dargestellten Risikomanagementprozesses.

ISO 31000 zielt darauf ab, als ein umfassendes Rahmenwerk für das Risikomanagement zu fungieren. Dazu soll unter Anwendung des Standards sichergestellt werden, dass Risiken ef-

fektiv, effizient und unternehmensweit gehandhabt werden können. Zielgruppe des Standards sind jegliche privaten und öffentlichen Organisationen sowie Individuen aus allen Industrien und Branchen. Der Standard definiert das Risiko als einen Effekt von Unsicherheit auf Ziele. Dabei ist unter Effekt eine positive oder negative Abweichung von etwas Erwartetem zu verstehen. Damit das Risikomanagement effektiv ist, wird herausgestellt, dass organisationsweit grundlegende Prinzipien gelten müssen. Dazu gehört unter anderem das Verständnis, dass Risikomanagement dem Erschaffen und Erhalten von Wert dient. Es muss daher ein integraler Bestandteil aller Prozesse und Entscheidungssituationen sein, sowie systematisch und strukturiert erfolgen. Neben diesen grundsätzlichen Prinzipien beschreibt ISO 31000 wie das Rahmenwerk in den operativen Betrieb überführt werden kann. Dazu sind drei Voraussetzungen nötig:

1. Verbindliche Zustimmung zum Risikomanagement durch die Geschäftsführung
2. Anpassung des Rahmenwerks an die individuellen Gegebenheiten
3. Implementierung des Rahmenwerks und des Risikomanagementprozesses.

Zur erfolgreichen Implementierung bedarf es zunächst einer starken Unterstützung seitens des Managements sowie strategischer und rigoroser Planung, um auf allen Organisationsebenen Zustimmung für ein ganzheitliches Risikomanagementsystem zu erlangen. Dies unterstützend müssen klare Ziele definiert, Kennzahlen entwickelt und auf allen Ebenen Verantwortlichkeiten festgelegt werden. Zur Anpassung des Systems sind die internen und externen Gegebenheiten, die einen Einfluss auf das Rahmenwerk haben, zu evaluieren. Dazu gehören z. B. politische, gesetzliche, soziale, finanzielle oder natürliche Einflüsse auf die Organisation. Des Weiteren ist eine Richtlinie zu entwerfen, die alle wichtigen Aspekte bezüglich des Risikomanagementsystems enthält. Darin sind Erklärungen und Regelungen bezüglich

- der Gründe für die Einführung eines Risikomanagementsystems,
- der Verknüpfung mit den Organisationszielen- und -richtlinien,
- der Regelungen von Haftung und Verantwortlichkeiten,
- der Messung der Leistungsstärke
- und der verbindlichen Zusage zur ständigen Anpassung des Rahmenwerks

festzuhalten. Es soll sichergestellt werden, dass bei der Einführung, der Durchführung und der Kontrolle des Risikomanagements jeweils Verantwortliche (Risk Owner) bestimmt werden. Bei der standardkonformen Gestaltung des Risikomanagementsystems muss weiterhin eine Integration in alle Geschäftsprozesse erfolgen. Der Risikomanagementprozess soll Teil aller Prozesse und Planungen sein und nicht separat betrachtet werden. Als Grundvoraussetzung der Einführung und des erfolgreichen Betriebs stellt der Standard weiterhin klar, dass dem Risikomanagement angemessene Ressourcen zugewiesen werden sollen. Dies gilt für Personal, Methoden- sowie Informationssystemunterstützung zur Bewältigung der Aufgaben. Letztlich verweist ISO 31000 darauf, dass im Rahmen der Anpassung interne und externe Kommunikations- und Berichtprozesse definiert werden müssen, um Risikoinformationen zusammenzuführen.

Zur Einbindung des Risikomanagements in die Organisation sind zwei Schritte notwendig: zum einen die Implementierung des organisationsspezifisch angepassten Rahmenwerks und zum anderen die Implementierung des Risikomanagementprozesses. Nach der Implementierung sind die Festlegungen des Rahmenwerks regelmäßig auf ihre Angemessenheit hin zu kontrollieren und gegebenenfalls anzupassen. Gleiches gilt für den Risikomanagementprozess, welcher im Sinne des Standards, nach seiner Implementierung wesentlicher Bestandteil der Unternehmensführung sein soll.

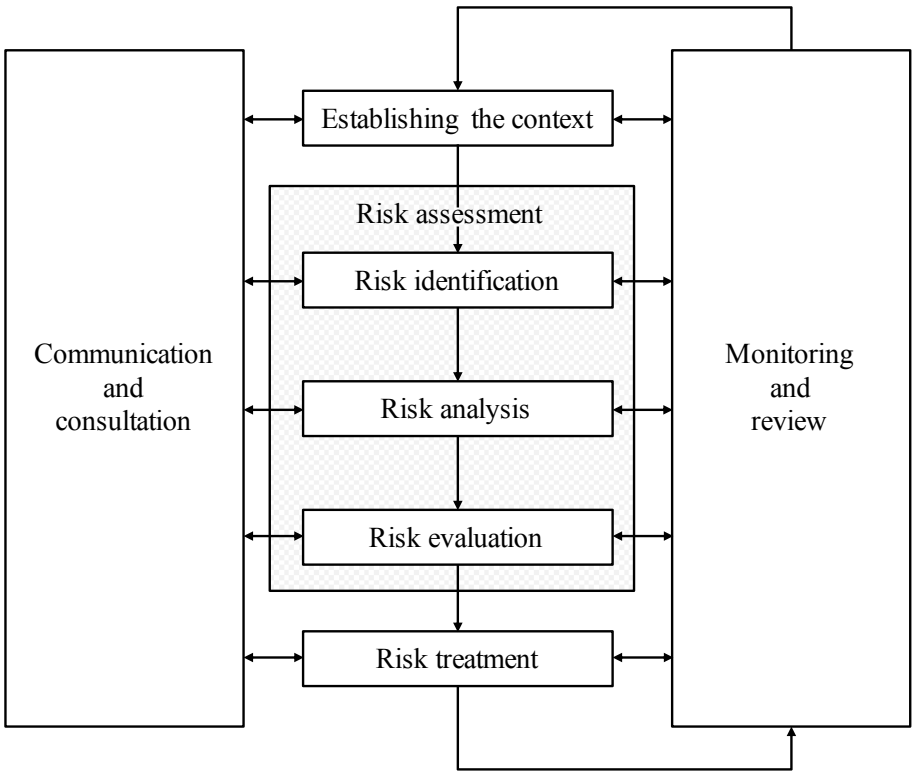


Abbildung 5: Risikomanagementprozess nach ISO 31000[123]

Der Risikomanagementprozess nach ISO 31000 ist in Abbildung 5 dargestellt. Er besteht aus den fünf Phasen:

1. Communication and consultation
2. Establishing the context
3. Risk assessment
4. Risk treatment
5. Monitoring and review.

Der Prozessschritt *Communication and consultation* läuft parallel zu allen anderen Phasen ab und umfasst die dauerhafte Kommunikation bzw. den Austausch zwischen allen internen und externen Stakeholdern. Durch den ständigen Informationsaustausch soll sichergestellt werden, dass in jedem Prozessschritt alle Aufgaben der jeweiligen Phase adäquat durchgeführt werden. Im Rahmen des zweiten Prozessschrittes werden die konkreten Ziele des Risikomanage-

[123] In Anlehnung an ISO 2009.

mentprozesses definiert und wichtige interne und externe Parameter, die zu berücksichtigen sind, festgelegt. Dieser Schritt konkretisiert und operationalisiert die bereits im Rahmen der Anpassung des Rahmenwerks (s. o.) festgelegten Punkte. Unter anderem wird in dieser Phase festgelegt, wie Eintrittswahrscheinlichkeiten zu bestimmen sind und welche Kriterien herangezogen werden, um die Bedeutung eines Risikos zu bestimmen. Der dritte Schritt des ISO 31000 Risikomanagementprozesses gliedert sich in die drei Subprozessschritte *Risk identification*, *Risk analysis* und *Risk evaluation*. Der erste Subprozessschritt behandelt die Identifizierung der Risiken sowie ihrer Ursachen und Wirkungen. Ziel des Prozessschrittes ist das Aufstellen einer Risikoliste, die alle Risiken aufführt, welche das Erreichen von bestimmten Zielen gefährden. Für diese Phase werden im Standard keine konkreten Identifizierungsmethoden aufgeführt, aber es wird auf die Bedeutung relevanter aktueller Informationen verwiesen und dass die Identifizierung mit Einbindung von Experten der jeweiligen Bereiche erfolgen soll. Im Rahmen der *Risk Analysis* werden Ausmaß und Eintrittswahrscheinlichkeit der identifizierten Risiken bestimmt. Auf dieser Basis erfolgt dann im Subprozessschritt *Risk evaluation* die Bewertung der Risiken auf Basis zuvor festgelegter Kriterien. Letztere wurden unter Berücksichtigung der eigenen Risikotoleranz und regulatorischen Vorgaben bestimmt. Im Anschluss an die drei Phasen des *Risk Assessment* folgt der Schritt des *Risk treatment*, welcher auf Basis der Ergebnisse der vorherigen Schritte die Steuerungsmaßnahmen festlegt. Dabei gibt der Standard einen Überblick über die möglichen Steuerungsarten und eine Anleitung zur Wahl der richtigen Art. Im folgenden Prozessschritt *Monitoring and review* sollen regelmäßig Verbesserungspotentiale im operativen Risikomanagement identifiziert und sich daraus ergebende notwendige Anpassungen initiiert werden. Konkret sollen neue Erfahrungswerte aus Risikoereignissen kritisch reflektiert und zur Verbesserung des bestehenden Risikomanagementprozesses genutzt werden. Letztlich verlangt der Standard eine lückenlose Dokumentation der Risikomanagementaktivitäten, um Nachvollziehbarkeit und Wiederverwendbarkeit von Informationen zu gewährleisten und eine Grundlage für Verbesserungsansätze vorliegen zu haben.

3.2.2.4. Kritische Würdigung der Rahmenwerke

Organisationen sehen sich einem erhöhten Druck ausgesetzt, ihr Risikomanagement ganzheitlich und somit unternehmensweit zu betreiben.[124] Der Druck resultiert unter anderem aus regulatorischen Vorgaben, neuen Ratingkriterien und stärkerem Wettbewerb (siehe Kapitel 3.3). Mit der zunehmenden Aufmerksamkeit für ganzheitliches Risikomanagement nahm weltweit auch die Zahl unterschiedlicher Rahmenwerke zu.[125] Die vorgestellten Rahmenwerke zielen darauf ab, ein einheitliches Verständnis des ganzheitlichen Risikomanagements zu schaffen und streben an, als Vorlage zur erfolgreichen Umsetzung eines solchen zu dienen. Die vorangehenden Ausführungen zeigen auf, dass sich die weit verbreiteten Rahmenwerke COSO ERM[126] und ISO 31000 inhaltlich nur marginal unterscheiden.[127] Beide empfehlen zunächst unternehmensintern einen Rahmen zu schaffen, auf dem das Risikomanagement aufbauen kann. Dazu gehören unter anderem ein einheitliches Begriffsverständnis, die Festlegung von Zielen und die Anerkennung des Risikomanagements im Unternehmensumfeld. Auf dieser Basis wählen beide Rahmenwerke einen phasenorientierten Ansatz, so dass das Risikomanagement einem strukturierten Vorgehen folgt. Dadurch ist die Mitarbeit der gesamten Organisation gefordert und ein kontinuierlicher Informationsaustausch von Risikoinformationen zwischen allen Beteiligten notwendig. Auch die Phaseninhalte beider Rahmenwerke unterscheiden sich nicht wesentlich. Insgesamt sind COSO ERM und ISO 31000 so allgemein gestaltet, dass eine Anpassung an die eigene Organisation notwendig ist.[128]

Als kritisch werden die teilweise ungenauen Beschreibungen angesehen, die den anwendenden Organisationen viel Interpretationsspielraum bei der Umsetzung der Rahmenwerke lassen.[129] Weiterhin wird insbesondere dem COSO ERM vorgehalten, dass es dem Bereich der Internen Revision entstammt, da es aus dem COSO Internal Control Rahmenwerk abgeleitet ist.[130] Es wurde von Prüfern und Finanzexperten konzipiert, wohingegen ISO 31000 unter Einfluss von Risikomanagern und Standardisierungsexperten entwickelt wurde. Daraus resul-

---

[124] Vgl. Lundqvist 2014, S. 393.
[125] Vgl. Lundqvist 2014, S. 393.
[126] Die Ausführungen beziehen sich auf das COSO ERM Framework in der Version von 2004. Zum Zeitpunkt des Verfassens dieser Arbeit findet eine Revision des COSO ERM Frameworks statt. Die neue Version mit dem Titel „ERM Framework: Enterprise Risk Management — Aligning Risk with Strategy and Performance“ wird daher in diesen Ausführungen noch nicht berücksichtigt.
[127] Vgl. Gjerdrum und Peter 2011, S. 12; Bosetti 2015, S. 85 f.
[128] Vgl. Frigo und Anderson 2014, S. 53.
[129] Vgl. Purdy 2010, S. 885.
[130] Vgl. im Folgenden Gjerdrum und Peter 2011, S. 10.

tierend wird bemängelt, dass COSO ERM sich schwieriger in bestehende Risikomanagementstrukturen einbinden lässt. Weiterhin wird es als problematisch angesehen, wenn die Interne Revisionsabteilung einer Organisation bei der Einführung des Rahmenwerks beteiligt ist, da es Aufgabe selbiger ist, das Risikomanagementsystem zu prüfen. Letztlich bleibt zu kritisieren, dass beide Rahmenwerke nur wenig konkrete Anleitungen liefern, wie das Risikomanagement und insbesondere die einzelnen Phasen in der Praxis umgesetzt werden können. Die Vorstellung von möglichen Methoden z. B. zur Risikoquantifizierung fehlt, so dass zusätzliche Erläuterungen notwendig sind, die diese Konkretisierungen vornehmen.[131]

[131] Vgl. COSO 2012; Austrian Standards Institute 2014; Brühwiler 2016, S. 163.

3.3. Bedeutung und Status Quo

3.3.1. Bedeutung und Status Quo in privatwirtschaftlichen Organisationen

Der Erhalt und die Weiterentwicklung der Unternehmung sind die Kardinalziele eines Unternehmens.[132] Damit sie erreicht werden können, sind Entscheidungen zu treffen und somit Aktivitäten anzustoßen, die zur Zielerreichung beitragen. Die unternehmerischen Entscheidungen sind jedoch stets mit Unsicherheit und daher mit Risiken behaftet. Risiken bestehen, da Entscheider die Folgen ihrer Handlungen und externe Umwelteinflüsse bzw. das Zusammenwirken mit dem Handlungsumfeld nicht vollständig vorhersehen können.[133] Aus diesem Grund ist es das Ziel des Risikomanagements, die Gefahr der Abweichung von Unternehmenszielen zu erkennen und gemäß der Risikopräferenz des Unternehmens gegebenenfalls Maßnahmen einzuleiten, welche die Gefahr im Sinne des Unternehmens handhaben. Hierbei wird allerdings nicht angestrebt, jegliche Risiken zu unterbinden, da das Ergreifen von Chancen zwangsläufig die Risikoinkaufnahme inkludiert und somit zu den Voraussetzungen der Gewinnerzielung zählt. Vielmehr geht es darum, Risiken bewusst und kontrolliert einzugehen, um Chancen und somit Erhalt und Weiterentwicklung der Unternehmung zu sichern.[134] Die langfristige Existenzsicherung einer Unternehmung kann also nur durch das Eingehen von Risiken erreicht werden.[135] Die betriebswirtschaftlich begründete Motivation zur Einrichtung eines Risikomanagements leitet sich somit, neben den gesetzlichen Vorgaben, insbesondere auch aus den Kardinalzielen einer Unternehmung ab. Das Risikomanagement stellt daher ein unterstützendes Subsystem der Unternehmensführung dar.[136] Insbesondere in den letzten zwanzig Jahren hat sich die Unsicherheitssituation für die Unternehmen verstärkt. Hauptgründe sind insbesondere ein erhöhter Wettbewerb, globale Lieferketten und ein schneller technologischer Wandel.[137] Zusätzlich erschwert eine zunehmende politische Unsicherheit die Planbarkeit, so dass ein rein intuitives Handeln des Managements gravierende Folgen haben kann.[138] Es sollte daher das Ziel der Unternehmensführung sein, auf Basis einer definierten Risikostrategie in einer für das Unternehmen adäquaten Art und Weise mit Risiken umzuge-

[132] Vgl. Joos-Sachse 2006, S. 3.
[133] Vgl. Rosenkranz und Missler-Behr 2005, S. 20; Hasenmüller 2009, S. 10 f.
[134] Vgl. Diederichs 2012, S. 11.
[135] Vgl. Braun 1984, S. 44.
[136] Vgl. Braun 1984, S. 43.
[137] Vgl. Liebenberg und Hoyt 2003, S. 40; Hölscher et al. 2006, S. 149.
[138] Vgl. Erben 2000, S. 27 f.; Rosenkranz und Missler-Behr 2005, S. 40.

hen. Mögliche unerwünschte Entwicklungen sollten im Vorfeld antizipiert werden und ihnen durch geeignete Maßnahmen begegnet werden.[139] Die Relevanz und Bedeutung eines systematischen Risikomanagements aus betriebswirtschaftlichen Gründen ist somit offensichtlich. Weiterhin wird seit geraumer Zeit die Ausgestaltung des Risikomanagementsystems durch Ratingagenturen berücksichtigt, so dass weitere Anreize bestehen ein solches System professionell zu implementieren.[140] Da die Ratings einen Einfluss auf eine erfolgreiche Kreditvergabe haben, sind die bestimmenden Einflussfaktoren des Ratings im Rahmen des Risikomanagements entsprechend bedeutsam und sollten daher die Gestaltung des jeweiligen Risikomanagements beeinflussen. Ist dieses schlecht ausgestaltet, kann ein Rating entsprechend negativ ausfallen und zu Liquiditätsengpässen beitragen.

Die unternehmerische Bedeutung des Risikomanagements wird weiterhin durch mehrere Studien untermauert, die einen positiven Zusammenhang zwischen dem Betrieb eines (ganzheitlichen) Risikomanagements und der Steigerung des Unternehmenswertes erkennen lassen.[141] Da die Steigerung des Unternehmenswertes eines der Hauptziele global tätiger Unternehmen ist und vielfach eine Shareholder-orientierte Unternehmensführung vorherrscht,[142] sollte auch aus diesem Grund ein systematisches Risikomanagement betrieben werden.

Des Weiteren kann das Umfeld, in dem sich das Unternehmen bewegt, die Relevanz eines Risikomanagementsystems erhöhen. So können z. B. je nach Branche spezifische Risiken auftreten, die eine vertiefende Auseinandersetzung mit der Thematik verlangen.[143]

Als weitere Gründe für ein unternehmensweites Risikomanagementsystem werden unter anderem eine verbesserte Entscheidungsfindung aufgrund besserer Informationen, weniger volatiler Erlöse, ein größerer Konsens in der Geschäftsleitung und Wettbewerbsvorteile genannt.[144] In welchem Umfang ein Risikomanagementsystem letztlich implementiert wird, ist daher nicht nur von den gesetzlichen Vorschriften abhängig, sondern auch von den eigenen Unternehmenszielen, Wirtschaftlichkeitsüberlegungen, der Unternehmensstruktur sowie dem Unternehmensumfeld.[145]

---

[139] Vgl. Lück 2000, S. 326.
[140] Vgl. Lundqvist 2014, S. 394.
[141] Vgl. Hoyt und Liebenberg 2011; Pérez-González und Yun 2013; Farrell und Gallagher 2015.
[142] Vgl. Fiss und Zajac 2004, S. 501 f.
[143] Für einen Überblick branchenspezifischer Risiken vgl. Dörner et al. 2000, S.445-785.
[144] Vgl. Kleffner et al. 2003, S. 54; Gates 2006, S. 82; Manab et al. 2010, S. 241; Muralidhar 2010, S. 68 f.
[145] Vgl. Beroggi 1995, S. 5; Paape und Spekle 2012, S. 543 ff.

Betrachtet man den Status Quo der Implementierung und Ausgestaltung von Risikomanagementsystemen, zeigen sich Unterschiede, die insbesondere von der Unternehmensgröße, der Inhaberstruktur und der Branche abhängen. Ausgehend von der Unternehmensgröße lässt sich bei Kleinstunternehmen, kleinen und mittleren Unternehmen (KMU)[146] erkennen, dass das Risikomanagement vielfach eher unbewusst bzw. informell betrieben wird.[147] Ein systematisches Vorgehen ist seltener vorzufinden und vielfach sind die Phasen des Risikomanagements den Verantwortlichen nicht bekannt.[148] Der Implementierung eines Risikomanagementsystems stehen unter anderem die finanziellen Aufwände und die fehlende Zeit als Argumente entgegen.[149] Das Risikomanagement von KMU ist eher durch reaktive als durch proaktive Maßnahmen geprägt.[150] Es zeigt sich jedoch auch, dass KMU mit zunehmender Unternehmensgröße das Risikomanagement systematischer gestalten.[151] Neben Einzelkaufleuten und Personengesellschaften zählen insbesondere auch kleinere Kapitalgesellschaften zu den KMU. Als Beurteilungsgrundlage zur Einschätzung der Ausgestaltung des Risikomanagements bei Kapitalgesellschaften eignet sich zunächst die Risikoberichterstattung im Lagebericht dieser Unternehmen.[152] Hier zeigt sich, dass kleine und mittlere Kapitalgesellschaften weniger Risikoinformationen in den Jahresberichten preisgeben als große Kapitalgesellschaften.[153] Die Gründe werden in einer geringeren unternehmerischen Komplexität, im Mangel an konkreten rechtlichen Vorschriften zur Berichterstattung und in der bewussten Geheimhaltung kritischer Informationen gesehen. Dies lässt vermuten, dass kleine und mittlere Kapitalgesellschaften nur das berichten, was rechtlich notwendig ist.[154] Es kann aber auch als ein Indiz für unzureichend ausgestaltete Risikomanagementsysteme angesehen werden, da kleine und mittelgroße Unternehmen nachweislich weniger formalisierte Risikomanagementsysteme

---

[146] Die Zuordnung richtet sich nach der Definition der Unternehmensgrößen gemäß der Empfehlung der EU Kommission. Demnach zählen zu KMU alle Unternehmen mit bis zu 249 Mitarbeitern, 50 Mio. Umsatz und 43 Mio. Bilanzsumme. Vgl. Europäische Kommission 2003.

[147] Vgl. Gao 2013, S. 692.

[148] Vgl. Iwona 2016, S. 294.

[149] Vgl. Hwang et al. 2014, S.123; Rostami et al. 2015, S.103.

[150] Vgl. Thun et al. 2011, S. 5519.

[151] Vgl. Iwona 2015, S. 296; Brustbauer 2016, S. 80 f.

[152] Hierbei wird unterstellt, dass aus dem Lagebericht Erkenntnisse über das Risikomanagementsystem gewonnen werden können. Da über die Risikolage gegebenenfalls nur selektiv berichtet wird, liefert der Lagebericht eventuell keine valide Aussage über die tatsächliche Ausgestaltung des Risikomanagementsystems. Diese Gefahr relativiert sich allerdings, da die Prüfungspflicht des Wirtschaftsprüfers eine nicht den tatsächlichen Verhältnissen entsprechende Berichterstattung einschränkt. Vgl. Ergün et al. 2015, S. 338.

[153] Vgl. Montag 2015, S. 223.

[154] Vgl. Montag 2015, S. 223.

aufweisen.[155] Demnach verfügen viele KMU über kein ausreichend institutionalisiertes Risikomanagementsystem.[156] Bei der inhaltlichen Ausgestaltung des Risikomanagements stehen KMU insbesondere vor dem Problem Risiken zu identifizieren und zu bewerten.[157] Des Weiteren nutzen bis zu 45 % keine Softwareunterstützung, ca. ein Drittel nutzt Tabellenkalkulationssoftware und nur knapp ein Fünftel verwendet eine spezielle Risikomanagementsoftware.[158] Dadurch werden eine unternehmensweite Risikobetrachtung und eine umfassende Risikoberichterstattung bereits aufgrund methodischer Mängel und ungeeigneter IT-Unterstützung erschwert. Das somit eine aggregierte Risikobetrachtung ebenfalls nicht zielführend erfolgen kann, ist offensichtlich.[159]
Hinsichtlich des Aufbaus von Methodenwissen, einer ganzheitlichen Betrachtung von Risikophänomenen sowie einer geeigneten IT-Unterstützung des Risikomanagements bestehen bei KMU somit noch Verbesserungspotentiale.

Bei größeren Kapitalgesellschaften korreliert die Menge der im Lagebericht veröffentlichten Risikoinformationen positiv mit der Firmengröße.[160] So lassen sich bei den nicht mehr zu den KMU zählenden mittelgroßen Kapitalgesellschaften konkretere Informationen zur Gestaltung des Risikomanagements aus den Berichten ableiten. Hierbei sind insbesondere Mängel bei der Risikoidentifizierung, der Risikobeurteilung und der Angabe von Zeithorizonten zu erkennen.[161] Weiterhin werden Risiken vielfach nicht kategorisiert und Interdependenzbetrachtungen zwischen den identifizierten Einzelrisiken bleiben aus.[162] Die Einschätzung des Risikoausmaßes erfolgt eher qualitativ als quantitativ und die Nennung von Risikoeintrittswahr-

[155] Vgl. Rostami et al. 2015, S.103; Hunziker et al. 2016, S. 38.
[156] Vgl. Bömelburg et al. 2012, S. 1166.
[157] Vgl. Bundesverband der Deutschen Industrie e.V. / PricewaterhouseCoopers AG 2011, S. 24 f.
[158] Vgl. Bömelburg et al. 2012, S. 1167.
[159] Vgl. Bömelburg et al. 2012, S. 1165 f.
[160] Vgl. Elzahar und Hussainey 2012, S. 141.
[161] Vgl. Ergün et al. 2015, S. 339 ff. In dieser Studie wurden mittelgroßen Kapitalgesellschaften gemäß Handelsgesetzbuch §267 klassifiziert. Somit fallen in diese Kategorie alle Kapitalgesellschaften die mindestens zwei der folgenden drei Kriterien nicht überschreiten: 250 Mitarbeiter im Jahresdurchschnitt, eine Bilanzsumme bis 20 Mio. sowie Umsatzerlöse bis 40 Mio., bei gleichzeitiger Überschreitung von zwei der drei Kriterien für kleine Kapitalgesellschaften (6 Mio. Bilanzsumme, 12 Mio. Umsatzerlöse, 50 Mitarbeiter im Jahresdurchschnitt).
[162] Vgl. Ergün et al. 2015, S. 341.

scheinlichkeiten fehlt mehrheitlich.[163] Es wird überwiegend auf subjektive Einschätzungen vertraut, anstatt Risiken z. B. auf Basis historischer Daten objektiv zu bemessen.[164]

Bei der Ausgestaltung des Risikomanagements in großen Kapitalgesellschaften stellt das systematische Risikomanagement grundsätzlich noch eine „junge Disziplin" dar.[165] Studienergebnisse zeigen hier, dass die Unternehmen sich vielfach bemühen die gesetzlichen Anforderungen an ein Risikomanagement zu erfüllen, aber eine ganzheitliche integrierte Sichtweise selten implementiert ist und ebenfalls oftmals eine „Silo-Sicht" vorherrscht.[166] Eine Tendenz hin zu einem über die gesetzlichen Verpflichtungen hinausgehendem ganzheitlichen Risikomanagement ist mittlerweile jedoch zu erkennen. So kann auch bei großen Kapitalgesellschaften zwischen der Unternehmensgröße und dem Betrieb eines unternehmensweiten Risikomanagementsystems ein positiver Zusammenhang bestätigt werden.[167] In jüngerer Zeit ist in Großunternehmen zudem ein Anstieg eigenständiger Risikomanagementabteilungen zu verzeichnen und die Schaffung der Funktionen eines Risikomanagers und von Risikoverantwortlichen (Risk Owner) kommt ebenfalls mit zunehmender Firmengröße häufiger vor.[168]

Im operativen Risikomanagement bestehen, wie bei mittelgroßen Kapitalgesellschaften, auch bei großen Kapitalgesellschaften noch Verbesserungspotentiale. Insbesondere können Mängel in der systematischen Pflege des bestehenden Risikokatalogs und bei der Definition von Frühwarnindikatoren ausgemacht werden.[169] Weiterhin erfolgt die Risikoquantifizierung und die Risikobeurteilung ebenfalls häufig noch subjektiv und Risiken werden oftmals einzeln betrachtet, so dass eine Betrachtung der Wechselwirkungen und eine Risikoaggregation selten durchgeführt werden. Sowohl bei nicht börsennotierten als auch bei börsennotierten Kapitalgesellschaften dominiert in den Lageberichten die Betrachtung von Finanzrisiken.[170] Hier besteht die Vermutung, dass der Risikobericht stark vom Rechnungswesen geprägt ist und somit andere Unternehmensbereiche in der Risikobetrachtung vernachlässigt werden.[171]

---

[163] Vgl. Ergün et al. 2015, S. 341.
[164] Vgl. Bömelburg et al. 2012, S. 1165.
[165] Vgl. PricewaterhouseCoopers 2012, S. 44.
[166] Vgl. Accenture 2011, S. 28 f.
[167] Vgl. Farrell und Gallagher 2015, S. 643; Lechner und Gatzert 2016, S. 19.
[168] Vgl. Pagach und Warr 2011, S. 193; PricewaterhouseCoopers 2015, S. 23.
[169] Vgl. PricewaterhouseCoopers 2015, S. 29 ff.
[170] Vgl. Dobler et al.2011, S. 17; Ergün et al. 2015, S. 340.
[171] Vgl. Ergün et al. 2015, S. 340.

Neben der Unternehmensgröße unterscheidet sich die Ausgestaltung des Risikomanagements auch aufgrund der Inhaberstruktur und der Branche, der ein Unternehmen angehört. So zeigt sich, dass Einzel- und Familienunternehmen ein weniger ausgereiftes Risikomanagementsystem betreiben als Unternehmen mit vielen Anteilseignern.[172] Mit einer zunehmenden Anzahl an institutionellen Anteilseignern nehmen die Verbreitung ganzheitlicher Risikomanagementsysteme und die Anzahl der Unternehmen mit einem Chief Risk Officer zu.[173]

Branchenspezifisch lässt sich feststellen, dass insbesondere in stärker regulierten Branchen wie z. B. der Finanzbranche, der Telekommunikations- und der Energiebranche fortgeschrittene Risikomanagementsysteme implementiert sind.[174] Dies ist aufgrund der in diesen Branchen seit Langem bestehenden regulatorischen Vorgaben nachvollziehbar.[175] Insgesamt zeigen sich zwischen den Branchen unterschiedliche Implementierungsgrade von Risikomanagementsystemen. Unternehmen des Industriesektors weisen allgemein weiterentwickelte Risikomanagementsysteme auf als Firmen aus dem Dienstleistungssektor.[176]

3.3.2. Bedeutung und Status Quo in öffentlichen Organisationen

Der Umgang mit Risiken im Rahmen der Bewältigung öffentlicher Aufgaben wie z. B. der Gewährleistung der öffentlichen Sicherheit, ist zunächst nicht neu und wird vielfach implizit vollzogen.[177] Allgemein lässt sich im angelsächsischen Raum eine längere Tradition eines systematischen Risikomanagements in öffentlichen Institutionen ausmachen als in deutschsprachigen Ländern. Dies ist auf frühzeitige politische Initiativen zurückzuführen, welche die Modernisierung und Effizienzsteigerung der öffentlichen Verwaltung verfolgten.[178] Insbesondere Großbritannien, Australien und Kanada weisen hier große Gemeinsamkeiten hinsichtlich einheitlichen Risikomanagementstandards und dem jeweiligen Umsetzungsstand auf.[179] Die Anwendung der Standards ist in diesen Ländern für bestimmte staatliche Einrichtungen verpflichtend oder wird ihnen nahegelegt.[180]

---

[172] Vgl. Mafrolla et al. 2016, S. 682.
[173] Vgl. Pagach und Warr 2011, S. 201; Brustbauer 2014, S. 81.
[174] Vgl. Liebenberg und Hoyt 2003, S. 46; Beasley et al. 2005, S. 529; Paape und Speklé 2012, S. 544; Soltanizadeh et al. 2014, S. 336; Lechner und Gatzert 2016, S. 21.
[175] Vgl. Kleffner et al. 2003, S. 62; Beasley 2005, S. 525; Khan et al. 2016, S. 1997.
[176] Vgl. Colquitt et al. 1999, S. 46; Soltanizadeh et al. 2014, S. 336.
[177] Vgl. Offerhaus 2009, S. 80.
[178] Vgl. Offerhaus 2009, S. 107; Palermo 2014, S. 324.
[179] Vgl. Offerhaus 2009, S. 107.
[180] Vgl. beispielhaft Victorian Department of Treasury and Finance 2015, S. 3.

Bezüglich des Umsetzungsstandes wird die weite Adaption der Standards gelobt, jedoch bestehen in der Ausführung der Risikomanagementaktivitäten insbesondere Mängel in einer behördenübergreifenden Betrachtung, in der Quantifizierung der Risiken und in der Zuweisung klarer Verantwortlichkeiten.[181] Weiterhin wird häufig eine fehlende Definition der Risikotoleranz durch die Führungsebene kritisiert.[182]

Im deutschsprachigen Raum besteht im öffentlichen Recht keine konkrete Vorgabe zum Betrieb eines Risikomanagementsystems.[183] Öffentliche Körperschaften auf Bundes-, Landes und Kommunalebene sind zwar grundsätzlich angehalten mit den ihnen zur Verfügung stehenden Finanzmitteln wirtschaftlich und sparsam umzugehen, allerdings sieht das öffentliche Recht nahezu keine Haftung für ein Fehlverhalten in Risikosituationen vor.[184] In dieser Ausgangslage liegt somit aus Sicht einer öffentlichen Institution zunächst kein Grund vor, ein Risikomanagementsystem zu betreiben. Im Zuge ihrer Aufgabenwahrnehmung sind öffentliche Institutionen allerdings vielfältigen Risiken ausgesetzt, die ihre Zielerreichung gefährden. Ihre Ziele sind dabei im Gegensatz zu Unternehmen nicht gewinn- sondern sachorientiert und verfolgen die Erfüllung öffentlicher, hoheitlicher Aufgaben und Leistungen.[185] Da das Risikomanagement bei den Zielen einer Organisation ansetzt, lassen sich die Methoden der Risikomanagementphasen somit prinzipiell auch auf öffentliche Institutionen übertragen, um die Zielerfüllung zu unterstützen.[186] Die Handlungsfähigkeit öffentlicher Leistungserbringer kann auf diese Weise verbessert werden.[187] Weiterhin ergibt sich durch die weiter voranschreitende Umstellung von der Kameralistik auf die kaufmännische Buchführung der Bedarf für ein Risikomanagementsystem, da die durch die Umstellung notwendig gewordene Aufstellung eines Jahresabschlusses die Darstellung der Risikosituation erfordert.[188]

Aus diesen Gründen bietet sich der Betrieb eines Risikomanagementsystems für öffentliche Organisationen grundsätzlich an. Tatsächlich gestaltet sich die Umsetzung in der Praxis jedoch schleppend. Betrachtet man die Einführung des kaufmännischen Rechnungswesens als möglichen Anstoß zur Implementierung eines Risikomanagementsystems, stellt sich folgende

---

[181] Vgl. Offerhaus 2009, S.109; Victorian Auditor-General 2013, S. 7.
[182] Vgl. National Audit Office 2011, S. 8.
[183] Vgl. Schwintowski 2009, S. 183 f.
[184] Vgl. Schwintowski 2009, S. 184 und S. 187 ff.
[185] Vgl. Budäus und Hilgers 2009, S. 37.
[186] Vgl. Budäus und Hilgers 2009, S. 37.
[187] Vgl. Motel und Richter 2016, S. 73.
[188] Vgl. Burth und Hilgers 2012, S. 7.

Situation dar. In Deutschland wird insbesondere auf Bundes- und Landesebene weiterhin die Kameralistik bevorzugt, obwohl den Kommunen die kaufmännische Buchführung von Landesseite überwiegend vorgeschrieben wird.[189] In manchen Bundesländern, wie z. B. in Bayern, besteht für die Kommunen ein Wahlrecht. Auf Länderebene haben bisher nur wenige Bundesländer auf eine kaufmännische Buchführung umgestellt und auch der Bund lässt keine Bereitschaft zur Umstellung erkennen.[190] Vereinzelt finden sich Bundesbehörden, die aus eigenem Antrieb heraus zur Bewältigung der eigenen Aufgaben und ohne vorhergehende Umstellung des Rechnungswesens, ein Risikomanagementsystem erfolgreich implementiert haben.[191] Ein aus dem Rechnungswesen heraus entstehender Bedarf nach einem Risikomanagementsystem kommt somit tendenziell überwiegend auf kommunaler Ebene auf. Untersuchungen zeigen jedoch, dass nur eine Minderheit an Kommunen, die ihr Rechnungswesen umgestellt haben, auch ein ganzheitliches Risikomanagementsystem betreibt. Vielfach ist dieses nur rudimentär vorhanden.[192] So lässt sich in den Risikoberichten erkennen, dass Strukturierungs- und Standardisierungsbedarf besteht und dass ein systematisches und ganzheitliches Risikomanagement nicht zwangsläufig aus der Verantwortung zur Risikoberichterstattung heraus entsteht.[193] Es zeigt sich allerdings auch, dass mit zunehmendem Bestehen des kaufmännischen Rechnungswesens, ein systematischeres Risikomanagement stattfindet.[194] Die bestehenden kommunalen Risikomanagementaktivitäten unterliegen derzeit jedoch noch erheblichen Mängeln. Insbesondere die organisatorische Einbindung des Risikomanagements ist verbesserungswürdig und die Risiken werden überwiegend dezentral gesteuert. [195]

3.4. Organisatorische Einbettung

Die Einführung eines Risikomanagementsystems bedingt, dass es aufbauorganisatorisch verankert wird. Bereits durch die aufbauorganisatorische Einbindung kann die von der Leitungsebene forcierte Bedeutung des Risikomanagements untermauert werden.[196] Es lassen sich drei Varianten der organisatorischen Einbindung unterscheiden:

---

[189] Vgl. Burth und Hilgers 2012, S. 15.
[190] Vgl. Worms 2014, S. 62 f.
[191] Vgl. Motel und Richter 2016.
[192] Vgl. Derfuß et al. 2016, S. 250.
[193] Vgl. Burth und Hilgers 2012, S. 15.
[194] Vgl. Derfuß et al. 2016, S. 250.
[195] Vgl. Derfuß et al. 2016, S. 250.
[196] Vgl. im Folgenden Wengert und Schittenhelm 2013, S. 13 f.

1. Risikomanagement als zweite Führungsebene
2. Risikomanagement als Vorstandsbereich
3. Risikomanagementzuordnung zum Sprecher des Vorstands

Der erste Ansatz sieht vor, das Risikomanagement als eigene Abteilung dem Finanzvorstand zu unterstellen. Diese Variante wird allerdings nicht als geeignet angesehen, da die Gefahr von Konflikten besteht, da der Finanzvorstands Einfluss auf das Risikomanagement ausüben kann und bei risikomanagementbezogenen Entscheidungen Einfluss auf die anderen Resorts genommen werden muss. Der zweite Ansatz verankert das Risikomanagement direkt als eigenes Vorstandsressort, wodurch ihm unmittelbar eine hohe Bedeutung zugeschrieben wird. Dieser Ansatz birgt die Gefahr, dass die Durchsetzung der Risikomanagementziele ebenfalls auf Gegenwehr bei den anderen Ressorts stoßen könnte. Als dritte Variante der Einbindung des Risikomanagements bietet sich die Zuordnung zum Vorstandssprecher bzw. Sprecher der Geschäftsführung an. Als Querschnittsfunktion kann dem Risikomanagement auf diese Weise eine hohe Unabhängigkeit und Bedeutung beigemessen werden. Weiterhin können die Risikomanagementziele mit Unterstützung des Vorstandsprechers besser durchgesetzt werden.[197]

[197] Vgl. Wolf und Runzheimer 2009, S. 171; Wengert und Schittenhelm 2013, S. 13 ff.

4. Phasen des Risikomanagements

4.1. Überblick

Zur Sicherstellung eines systematischen Vorgehens wird im Rahmen des operativen Risikomanagements ein phasenorientiertes Vorgehen unter Berücksichtigung der Unternehmensstrategie empfohlen.[198] Die sich daraus ergebenden Risikomanagementphasen unterscheiden sich je nach Autor in ihrer Anzahl.[199] Die Phasen sind im Einzelnen[200]:

- die Risikoidentifizierung,
- die Risikoquantifizierung,
- die Risikobeurteilung,
- die Risikosteuerung,
- sowie die Risikoüberwachung.

Die Phasen der Risikoidentifizierung, Risikoquantifizierung und Risikobeurteilung werden häufig unter der Phase der Risikoanalyse zusammengefasst. Neben der Anzahl der Phasen weichen auch ihre Bezeichnungen bei den jeweiligen Autoren ab, jedoch unterscheiden sich die Inhalte nicht wesentlich.

4.2. Phase der Risikoanalyse – Risikoidentifizierung

4.2.1. Zielsetzung der Risikoidentifizierung

Die Grundlage jeglicher Risikomanagementaktivitäten ist die systematische Identifizierung und Erfassung der Risiken, der sich eine Unternehmung ausgesetzt sieht. Die Risikoidentifizierungsphase schafft die notwendige Informationsbasis für das Risikomanagement.[201] Ohne sie wären die nachfolgenden Phasen obsolet. Daher kommt ihr auch eine besonders bedeutende Rolle zu.[202] Der Umfang der Risikoidentifizierung ergibt sich dabei aus den risikostrategischen Vorgaben des Managements. So kann versucht werden generell alle Risiken zu identifi-

---

[198] Vgl. Braun 1984, S. 64 ff.; Diederichs 2012, S. 49.
[199] Zu unterschiedlichen Definitionen der Phasen des Risikomanagements vgl. z. B. Mugler 1979, S. 78 ff.; Härterich 1987, S. 38 ff.; Sauerwein und Thurner 1998, S. 20 ff.; Kromschröder und Lück 1998, S. 240 ff.; Gampenrieder und Greiner 2002, S. 284 f.; Kazap und Kaymak 2007, S. 2116.
[200] Vgl. Siepermann 2008, S. 34.
[201] Vgl. Erben 2000, S. 11; Kajüter 2012, S. 155.
[202] Vgl. Tchankova 2002, S. 290; Vose 2008, S. 5.

zieren oder nur Teilerhebungen durchzuführen. Vielfach wird in der Literatur gefordert, dass eine umfassende Identifizierung möglichst aller Risiken durchzuführen ist.[203] Dennoch sollte im Idealfall auch die Wesentlichkeit eines Risikos berücksichtigt werden, damit die Erhebung wirtschaftlich bleibt.[204] Die Einschätzung der Wesentlichkeit muss in der Risikoidentifizierungsphase mithilfe des Erfahrungswissens des Entscheiders erfolgen, da noch keine Quantifizierung und Bewertung der Risiken stattgefunden hat. Unabhängig vom Identifizierungsumfang ist es Ziel der Risikoidentifizierung, Risiken möglichst frühzeitig zu erkennen, um etwaige Handhabungsmaßnahmen rechtzeitig einleiten zu können.[205] Daraus resultiert, dass die Risikoidentifizierung regelmäßig erneut durchgeführt wird, da neue Risiken entstehen können oder bereits bekannte Risiken gegebenenfalls nicht mehr bestehen. Aus Gründen der Übersichtlichkeit sowie für spätere Analysen ist es zielführend, die Risiken nach Risikoarten zu ordnen. Diese lassen sich anhand unterschiedlicher Kriterien bilden. Hierfür eignen sich z. B.[206]

- die Zuordnung nach Unternehmensbereichen,
- die Einordnung nach Zeitpunkt der Entstehung und Fristigkeit (kurz-, mittel-, langfristig),
- der Grad der Auswirkung des Risikos,
- die Häufigkeit des Auftretens.

Weiterhin sollen in der Risikoidentifizierungsphase die Risikoursachen und -wirkungszusammenhänge aufgedeckt sowie etwaige Wechselwirkungsbeziehungen entdeckt werden.[207] Als Ergebnis der Risikoidentifizierung entsteht ein Risikokatalog, welcher aufgrund des regelmäßigen Durchlaufens der Phase stets aktuell ist.[208]

---

[203] Vgl. Brebeck 1997, S. 384.
[204] Vgl. Kajüter 2012, S. 155.
[205] Vgl. Diederichs 2012, S. 51; Paetzmann 2012, S. 17.
[206] Vgl. Rosenkranz und Missler-Behr 2005, S. 27; Paetzmann 2012, S. 69 f. Zur Komplexität der Risikokategorisierung siehe Kapitel 2.5.
[207] Vgl. Häntsch und Huchzermeier 2013, S.130; Kajüter 2012, S. 163.
[208] Vgl. Pauli 2008, S. 286.

4.2.2. Methoden der Risikoidentifizierung

Eine Vielzahl von Identifizierungsmethoden kann zur Unterstützung der Aufdeckung von Risiken herangezogen werden. In der Praxis werden meist mehrere Methoden in Kombination angewendet.[209] Es lassen sich

- Analytische Methoden (z. B. FTA oder FMEA),
- Kollektionsmethoden (z. B. Checklisten oder Dokumentenanalyse),
- Empirische Methoden (z. B. Interviews oder Statistiken)
- und Kreativitätsmethoden (z. B. Brainstorming oder Delphi-Methode)

unterscheiden.[210]

Abbildung 6 liefert, ohne Anspruch auf Vollständigkeit, einen Überblick über diese Methoden. Analytische Methoden dienen der systematischen Identifizierung von Risiken, ihren Ursachen und ihren Wirkungen. Sie sind generisch anwendbar und benötigen kein Risikospezialwissen. Vielfach genutzte analytische Methoden sind die Fehlerbaumanalyse (FTA), die Fehlermöglichkeits- und Einflussanalyse (FMEA) sowie die Szenarioanalyse.[211] Die FTA ist präventiv ausgerichtet. Sie geht von einem negativen bzw. unerwünschten Ereignis aus und leitet die Ursachen, die zu diesem Ereignis führen können, Stufe für Stufe ab (siehe Abbildung 7). So ergibt sich ein Diagramm, das einer Baumstruktur ähnelt. In der ersten Stufe unter dem Top-Ereignis werden zunächst die direkten Auslöser des Ereignisses dokumentiert. Diese können wiederum weiter in ihre Ursachen aufgespalten werden. Dabei können alle Ursachen mittels logischer Verknüpfungen oder festen Bedingungen verknüpft werden. Final erfolgt für jeden Zweig und die Zweigkombinationen die Einschätzung einer Eintrittswahrscheinlichkeit. So kann eine Priorisierung der Ursachen erfolgen und eine Ableitung notwendiger Maßnahmen zur Gegensteuerung durchgeführt werden.[212]

[209] Vgl. Schenk 1998, S. 43 ff.; Vanini, 2012, S. 147.
[210] Vgl. Siepermann 2008, S. 37.
[211] Vgl. Romeike et al. 2013, S. 22 f.
[212] Vgl. Wolf und Runzheimer 2009, S. 45.

Analytische Methoden
Ausfalleffektanalyse
Ereignisbaumanalyse (ETA)
Fehlerbaumanalyse (FTA)
Fehlermöglichkeits- und Einflussanalyse (FMEA)
Fishbone- / Ursache-Wirkungs-Diagramm
Flow-Chart-Analyse
Management Oversight and Risk Tree (MORT)
Störfallablaufanalyse
SWOT-Analyse
Szenarioanalyse
What-If Analyse
Empirische Methoden
Befragungen / Interviews / Workshops
Einzelfallanalyse
Statistiken
Kollektionsmethoden
Checklisten/Risikokataloge
Dokumentenanalyse
Inspektion / Begleitung
Organisationsanalyse
Kreativitätsmethoden
Brainstorming / Brainwriting (Methode 635)
Delphi-Methode
Morphologische Analyse
Synektik

Abbildung 6: Methoden der Risikoidentifizierung[213]

Die Anwendung der FTA macht insbesondere Sinn, wenn mehrere Ursachen zu einem unerwünschten Ereignis führen können. Weiterhin ist sie nützlich, wenn herausgestellt werden soll, wie mehrere Ursachen im Zusammenspiel agieren. Sie kann genutzt werden, um Ursache-Wirkungsketten darzustellen und auf Basis der Analyse präventive Maßnahmen zu konzipieren und auszuführen. Üblicherweise wird die Methode zur Beschreibung von Fehlern technischer Systeme verwendet und erfordert eine detaillierte Kenntnis des Systems.[214] Sie lässt sich aber auch, wie in Abbildung 7 dargestellt, auf die Risikoanalyse anderer Phänomene übertragen.

[213] Vgl. Siepermann 2008, S. 37.
[214] Vgl. Vanini 2012, S. 143.

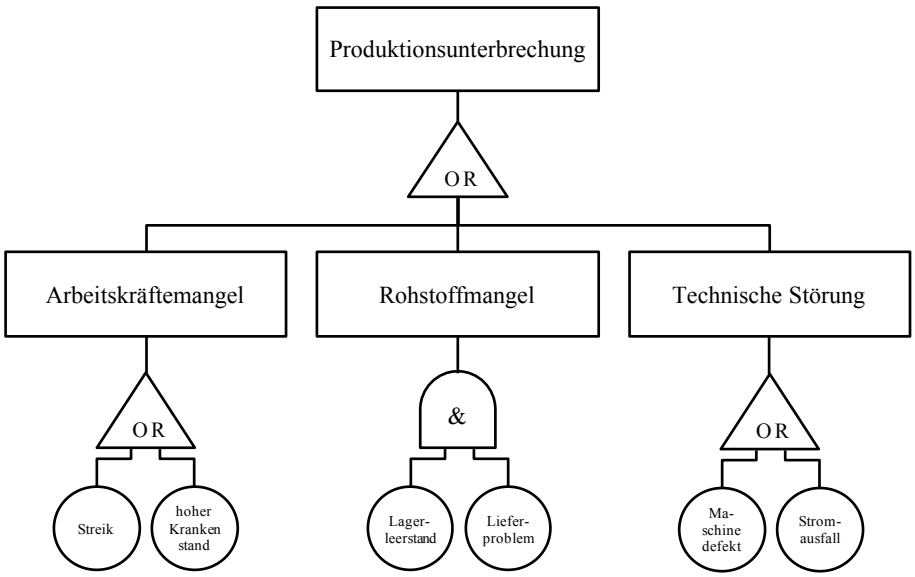


Abbildung 7: Beispiel für einen Fehlerbaum ohne Eintrittswahrscheinlichkeiten

Ein beliebtes analytisches Verfahren zur Prozess- und Systemanalyse ist die Fehlermöglichkeits- und Einflussanalyse (FMEA). Sie untersucht die Ursachen und Wirkungen von Fehlern in Teilbereichen eines komplexen Gesamtsystems, um anschließend die Auswirkungen auf das Gesamtsystem einzuschätzen.[215] Dazu wird das Gesamtsystem zunächst in seine Subsysteme aufgespalten. Für jede Teilkomponente werden dann mögliche Fehler identifiziert, die zu einem unerwünschten Verhalten der Teilkomponente führen können. Ebenso werden die Eintrittswahrscheinlichkeit jedes Fehlers und die Auswirkungen auf das Gesamtsystem erfasst. Ziel der FMEA ist die vorzeitige Identifizierung von möglichen Fehlern und ihren Auswirkungen. Methodisch werden bei der FMEA Tabellenarbeitsblätter verwendet, welche die betroffene Funktion, ihre Fehlerursachen, die Fehlerwirkungen, die bedrohten Objekte und eine Risikobeurteilung enthalten. Im Allgemeinen werden die drei Arten System-, Konstruktions- und Prozess-FMEA unterschieden.[216] Dabei fokussiert sich die System-FMEA auf die Analyse des Gesamtsystems und dem Zusammenspiel zwischen den Subsystemen. Im Rahmen der Konstruktions-FMEA werden Risiken in der Gestaltung einzelner Produktkomponenten in der Produktentwurfsphase betrachtet. Die Prozess-FMEA hat die Untersuchung von möglichen Fehlern, ihren Ursachen und Wirkungen auf Prozessebene zum Gegenstand.

[215] Vgl. zu den Ausführungen zur FMEA Gleißner und Romeike 2005b, S. 182 ff.
[216] Vgl. Piaz 2002, S. 91; Gleißner und Romeike 2005b, S. 183; Vanini 2012, S. 142.

Die Szenarioanalyse wird je nach Autor zu den analytischen[217] oder den Kreativitätsmethoden[218] gezählt. Sie ist grundsätzlich ein exploratives Prognoseverfahren[219], welches einem strukturierten Vorgehen folgt, aber aufgrund der Bildung von Szenarien eine gewisse Kreativität erfordert. Sie hilft mögliche zukünftige Entwicklungspfade zu antizipieren. Das Vorgehen bei der Szenarioanalyse folgt einem in fünf Phasen gegliederten, strukturierten Prozess.[220] Zunächst wird der konkrete Gegenstand, für den Szenarien konstruiert werden sollen, abgegrenzt (z. B. ein bestimmtes Produkt). Dabei wird auch festgelegt, was nicht Gegenstand der Betrachtung ist und ausgeschlossen wird. In Phase 2 werden wichtige Schlüsselfaktoren (z. B. Variablen, Trends, Ereignisse) erhoben. Sie sind in der späteren Analyse die zentralen Beobachtungspunkte, da sie mit dem Szenariogegenstand in einer bedeutenden Beziehung stehen.

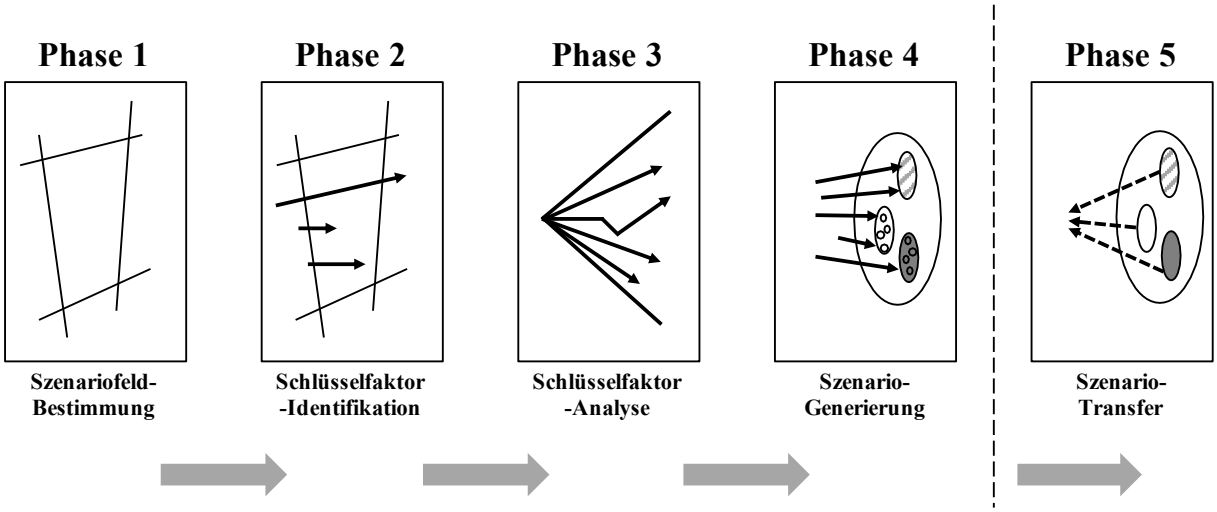


Abbildung 8: Phasen der Szenarioanalyse[221]

Anschließend werden die möglichen zukünftigen Ausprägungen der Faktoren analysiert (Phase 3) und aus einer bestimmten Konstellation von Faktoren Szenarien generiert (Phase 4). Diese können z. B. den angenommenen Worst-, Normal- und Best-Case widerspiegeln. Aus den entworfenen Szenarien können dann Risiken abgeleitet werden. Abschließend kann opti-

[217] Vgl. Siepermann 2008, S. 37.
[218] Vgl. Romeike et al. 2013, S. 20.
[219] Vgl. Wolf und Runzheimer 2009, S. 47 f.
[220] Vgl. für die Ausführungen zur Szenarioanalyse Kosow und Gaßner 2008, S. 20 ff.
[221] Vgl. Kosow und Gaßner 2008, S. 20.

onal im Rahmen der Risikobeurteilung aus den erzeugten Szenarien ein Transfer auf die Gegenwart vorgenommen werden, um zu entscheiden wie mit den Erkenntnissen der Generierung umgegangen wird (Phase 5). So können z. B. Strategien für das weitere Agieren auf Basis eines Szenarios festgelegt werden.

Zu den Kollektionsmethoden zählen Verfahren, die auf dem Sammeln und Zusammentragen von Risiken aus Datenbeständen wie z. B. Dokumenten, bekannten Verfahrensweisen und Erfahrungswissen beruhen. Zu den Methoden zählt bspw. die Anwendung von Checklisten bei der Durchführung neuer Projekte. Die Checklisten enthalten dabei bekannte Risiken z. B. aus vergangenen Projekten und helfen so, diese zu berücksichtigen. Andererseits bergen sie auch die Gefahr, dass nicht alle Risiken berücksichtigt werden, da diese in der Vergangenheit nicht auftraten. So sind sie für die Identifizierung unbekannter neuer Risiken ungeeignet.[222]

Die empirischen Methoden stützen sich auf Erhebungen wie Statistiken oder Experteninterviews. Mittels interner Statistiken können z. B. häufige Schadensfälle entdeckt werden und einen ersten Anhaltspunkt für tiefgehende Ursachenanalysen bieten. Bei Experteninterviews stehen insbesondere die Erhebung unbekannter bzw. nicht dokumentierter Problemstellungen und Verfahrensweisen im Vordergrund. Sie eignen sich, wenn nicht viel über Risikophänomene in bestimmten Bereichen bekannt ist. Gegebenenfalls sind zwar die Risiken bekannt, nicht aber ihre Ursachen und Auswirkungen. Diese können über Interviews mit direkt betroffenen Personen antizipiert werden.[223]

Die Kreativitätsmethoden verfolgen das Ziel, unbekannte Risiken zu identifizieren, indem versucht wird, übliche Denkmuster zu überwinden. Eine der bekanntesten Methoden aus diesem Bereich ist das Brainstorming. Hierbei werden mehrere Teilnehmer angeregt zu einer Problemstellung alle Gedanken zu äußern, die ihnen in den Sinn kommen. Dabei soll keine Äußerung durch andere Teilnehmer kritisiert werden, um der Kreativität freien Lauf zu lassen. Ziel ist es, neue Problembereiche aufzudecken.[224] Ein weiteres häufig verwendetes Verfahren ist die Delphi-Methode. Hierbei werden Experten, meist anonym, in mehreren Runden hinsichtlich ihrer Einschätzung einer zukünftigen Entwicklung befragt. Nach der ersten Runde werden die Antworten ausgewertet und an die Experten zurückgespielt. Diese sollen dann erneut Stellung nehmen und bei Antworten die extrem von der allgemeinen Einschätzung ab-

[222] Vgl. Vanini 2014, S. 70.
[223] Vgl. Häntsch und Huchzermeier 2013, S. 130.
[224] Vgl. Piaz 2002, S. 86.

weichen, diese explizit begründen. Am Ende kann so über mehrere Runden herausgefunden werden, inwieweit ein Konsens oder Dissens besteht.[225] Vielfach wird die Methode auch unter den empirischen Methoden eingeordnet, da sie letztlich eine Befragung darstellt. Aufgrund der in die Zukunft gerichteten Überlegungen sind jedoch kreative Denkprozesse erforderlich. Die Methode eignet sich daher auch in Kombination mit der Szenarioanalyse und hilft bei der Identifizierung neuer Risiken.[226]

4.3. Phase der Risikoanalyse – Risikoquantifizierung

4.3.1. Zielsetzung der Risikoquantifizierung

Im Rahmen der Risikoquantifizierung werden die identifizierten Risiken zahlenmäßig abgebildet, um eine Vergleichbarkeit und eine angemessene Risikobeurteilung zu ermöglichen. Die Risikoquantifizierung ist notwendig, um erwartete Erträge und damit verbundene Risiken sinnvoll gegeneinander abzuwägen und dadurch die Qualität unternehmerischer Entscheidungen zu verbessern.[227] In Abhängigkeit des betrachteten Risikos erfolgt die Quantifizierung in unterschiedlichen Einheiten, wie z. B. in Geldeinheiten oder in Mengen, die zur besseren Beurteilung idealerweise in eine monetäre Größe überführt werden sollten. Im Falle einer zunächst nicht-monetären Quantifizierung wie bspw. in Mengeneinheiten, ist die bezifferte Menge dazu entsprechend mit einem Wertbetrag in Geldeinheiten wie z. B. dem Stückdeckungsbeitrag zu multiplizieren.

4.3.2. Methoden der Risikoquantifizierung

4.3.2.1. Quantifizierung von Einzelrisiken

Ausgehend von der Definition des Risikos als die Gefahr einer negativen Abweichung einer Ist-Größe G^I von ihrer Plan-Größe G^P ist der sogenannte Risikowert R, der die Abweichung darstellt, zu quantifizieren. Der Risikowert R ist definiert als:[228]

$$R = G^I - G^P$$

[225] Vgl. Kosow und Gaßner 2008, S. 63
[226] Vgl. Kosow und Gaßner 2008, S. 63.
[227] Vgl. Gleißner 2011, S. 182.
[228] Vgl. zur formalen Darstellung der folgenden Ausführungen Siepermann 2008, S. 26 ff.

Wird das Risiko wirksam, so wird die Plangröße G^P unterschritten. R ist dann negativ und als Verlust zu verstehen. Demgegenüber steht der Fall einer Chance, so dass G^I die geplante Größe G^P überschreitet. R hat dann einen positiven Wert, der als den Plan übertreffenden Gewinn zu verstehen ist. Aufgrund der in die Zukunft gerichteten Betrachtung entspricht die tatsächlich realisierte Ist-Größe G^I einer Zufallsvariable.[229] Damit der Planwert bei Risikoeintritt R_T^P für den Planungszeitraum $T = [t, t']$ bereits in t bestimmt werden kann $(t < t')$, muss G^I für den Zeitpunkt t' in t ermittelt werden. Da die zukünftigen Ausprägungen von G^I im Zeitpunkt t unbekannt sind und jedes Risiko im Grunde einer Wahrscheinlichkeitsverteilung unterliegt, ist daher zunächst die Wahrscheinlichkeitsverteilung von G^I zu bestimmen. Dies kann auf drei Arten erfolgen: [230]

- per Annahme einer Verteilung
- per Simulation mit historischen Daten
- per Simulation mit selbst erzeugten Daten.

Im ersten Fall wird eine Wahrscheinlichkeitsverteilung aus der parametrischen Verteilungsklasse[231] mit den notwendigen Parametern vom Entscheider festgelegt (z. B. Normalverteilung mit Erwartungswert und Standardabweichung).
Die Simulation auf Basis historischer Daten ermittelt die Verteilung der Größe G^I auf Basis der historischen Realisierungen der Risikofaktoren des Referenzzeitraums (Historische Simulation). Bei der Simulation mittels selbst erzeugter Daten (Monte Carlo Simulation) werden die möglichen zukünftigen Ausprägungen der Größe G^I unter gewissen Annahmen in einer sehr großen Anzahl von Zufallsexperimenten ermittelt.
Im Ergebnis erhält man bei allen drei Verfahren eine Verteilungsfunktion, mit deren Hilfe die Bildung von Messgrößen, sogenannte Risikomaße, vorgenommen werden kann. Ein klassische Risikomaß aus der Statistik ist die Varianz, welche die mittlere quadratische Abweichung vom Erwartungswert darstellt. Sie ist ein symmetrisches Risikomaß, da sie negative und positive Abweichungen vom Erwartungswert quantifiziert. Sie ist daher als Risikomaß

[229] Vgl. Cottin und Döhler 2013, S. 109.
[230] Vgl. Daldrup 2005, S. 18; Löhr 2010, S. 90.
[231] Dazu gehören z. B. Normal-, Binominal-, Poisson-, Gamma- und inverse Gaußverteilung.

ungeeignet, weil das Risiko lediglich als die Gefahr der negativen Abweichung von einem Referenzwert definiert ist. Bei stets normalverteilten Risiken wäre die Anwendung eines solchen symmetrischen Risikomaßes denkbar, jedoch liegen in der Realität meist asymmetrische Risikoverteilungen vor, so dass die Varianz sich nicht zur Quantifizierung von Risiken gemäß der in dieser Arbeit zugrunde gelegten Definition eignet.[232] In der Literatur und Praxis werden zur Quantifizierung des Risikos insbesondere die folgenden Risikomaße vorgeschlagen:[233]

- Maximum Possible Loss
- Value at Risk
- Risikoerwartungswert
- Expected Shortfall / Conditional Value at Risk.

Diese können als Substitut für die erwartete Ist-Größe $G_t^{I(t')}$ genutzt werden.

Maximum Possible Loss (MPL)

Der Maximum Possible Loss hat seinen Ursprung in der Versicherung von Feuerereignissen und drückt den maximal möglichen Schaden aus, der durch ein Risiko entstehen kann. Unter der Annahme, dass $G_{t'}^{M}$ die Menge aller möglichen Werte von G zum geplanten Zeitpunkt t' ist, $G_{t'}^{M} = \{G_{t'}^{I} \mid t' geplanter\ Zeitpunkt\}$ und $G_{t'}^{MIN} = \min\left(G_{t'}^{M}\right)$ der minimalste Wert, den G in t' annehmen kann, lässt sich der Risikowert mittels

$$R_T^P(G) = G_{t'}^{MIN} - G_t^{P(t')}$$

ausdrücken. Der MPL betrachtet nur die maximal negative Ausprägung und berücksichtigt keine Chancen. Er gehört damit zu den sogenannten Downside Risikomaßen.

[232] Vgl. Daldrup 2005, S. 11 f.
[233] Vgl. Hoitsch und Winter 2004, S. 240 ff.; Siepermann 2008, S. 28.

Value at Risk (VaR)

Der Value at Risk (auch Probable Maximum Loss) ist ebenfalls ein Downside Risikomaß. Er drückt den maximalen Verlust in Geldeinheiten aus, der mit einer vom Entscheider festgelegten Wahrscheinlichkeit (Konfidenzniveau) in einem bestimmten Zeitraum nicht überschritten wird.[234] Der VaR ist eines der weit verbreitetesten Risikomaße und hat insbesondere im Finanzbereich eine bedeutende Rolle eingenommen. Dies liegt vor allem an seiner von der Verteilungsform unabhängigen Aussagekraft.[235] Zur Berechnung des VaR sind zunächst Kenntnisse oder Annahmen über die Verteilungsfunktion der betrachteten Risikopositionen zu erlangen bzw. zu treffen (s. o.). Ist die Verteilungsfunktion bestimmt, ist vom Entscheider ein Konfidenzniveau α festzulegen, welches die Wahrscheinlichkeit $(1-\alpha)$ angibt, dass in einem festgelegten Zeitraum T ein Maximalschaden in Höhe des VaR nicht überschritten wird.

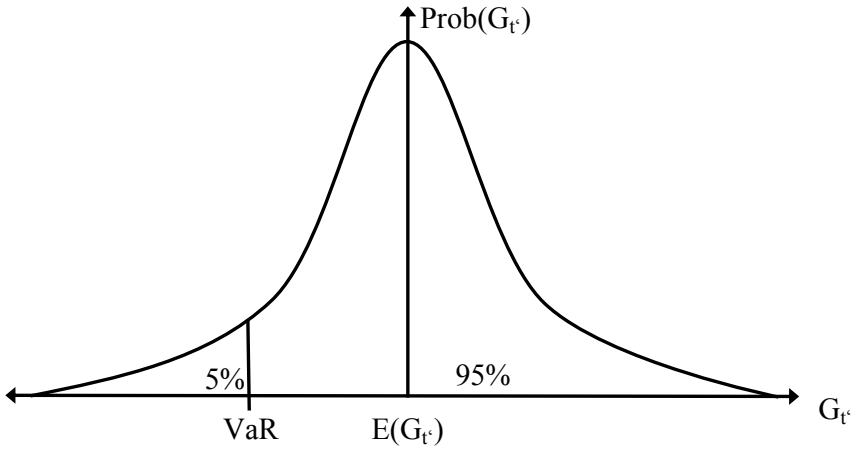


Abbildung 9: Value at Risk[236]

Der Risikowert ergibt sich dann aus:

$$R_T^P(G) = VaR(G_{t'}) - G_t^{P(t')}$$

[234] Vgl. Rau-Bredow 2002, S. 604; Daldrup 2005, S. 16.
[235] Vgl. Steinhoff 2008, S. 44.
[236] Vgl. Siepermann 2008, S. 29.

Expected Shortfall (ES) / Conditional Value at Risk (CVaR)

Als Expected Shortfall oder Conditional Value at Risk[237] wird der wahrscheinlichkeitsgewichtete Durchschnitt aller Verluste, die den VaR überschreiten, bezeichnet. Während der VaR das 1-α–Quantil betrachtet, fokussiert sich der ES auf das α-Quantil der Verteilung und bildet den wahrscheinlichkeitsgewichteten Durchschnittswert dieses Teils der Verteilung. Er berücksichtigt somit auch Extremwerte im absoluten Randbereich der Verteilung und drückt den durchschnittlichen Risikowert in α % der schlechtesten Ausprägungen der Verteilung aus.[238] Der ES entspricht dann:

$$ES\ (G_{t'}) = E[G_{t'}|G_{t'} \geq VaR]$$

Die Berechnung des Risikowertes auf Basis des ES entspricht:

$$R_T^P(G) = ES\ (G_{t'}) - G_t^{P(t')}$$

Risikoerwartungswert

MPL, VaR und ES betrachten lediglich das Risiko im engeren Sinn und beziehen keine Verrechnung von Chancen, also positiven Planabweichungen, mit ein. Diese einseitige Betrachtung fokussiert immer den Worst-Case und nicht den wahrscheinlichsten Fall. Dieser kann mit dem Risikoerwartungswert abgebildet werden. Der Risikowert ergibt sich dann aus:

$$R_T^P(G) = E(G_{t'}) - G_t^{P(t')}$$

4.3.2.2. Quantifizierung auf Basis nicht objektiv gegebener Daten

Vielfach wird vorgebracht, dass sich die Quantifizierung aufgrund unbekannter Wahrscheinlichkeitsverteilungen oder komplexer Ursache-Wirkungs-Zusammenhänge grundsätzlich als schwierig gestaltet oder „finanzielle und zeitliche Restriktionen“ sie verhindern.[239] Es muss

[237] Auch durchschnittlicher Risikowert oder Shortfall-Erwartungswert genannt.
[238] Vgl. Daldrup 2005, S. 20.
[239] Vgl. Löhr 2010, S. 87 f.; Diederichs 2012, S. 91.

somit akzeptiert werden, dass zahlreiche Risiken nicht exakt quantifizierbar sind.[240] In diesen Fällen kann versucht werden, die Eintrittswahrscheinlichkeiten und Schadensausmaße durch subjektive (Experten-) Einschätzungen anzunähern.[241] Dabei kann ein quantitatives (z. B. „Eintritt viermal in zehn Jahren“) oder ein qualitatives (z. B. Eintrittswahrscheinlichkeit ist „gering“, „mittel“ oder „hoch“) Vorgehen gewählt werden.[242] Quantitative Einschätzungen ermöglichen die Ableitung einer Verteilungsfunktion, mit welcher Risikomaße wie der Value at Risk bestimmt werden können. Im Fall von qualitativ vorliegenden Einschätzungen eines Risikos sollte idealerweise eine eindeutige Zuordnung zu Werten oder Wertklassen erfolgen, um eine Quantifizierung zu ermöglichen. Dies kann bspw. über eine Zuordnungstabelle erfolgen (siehe Abbildung 10).

certain (almost)	100 %
probable	85 %
expected	75 %
fifty-fifty	50 %
uncertain	25 %
improbale	15 %
(almost) impossible	0 %

Abbildung 10: Beispielhafte Zuordnung verbaler und numerischer Wahrscheinlichkeiten[243]

Auf dieser Basis kann beispielsweise die erwartete Eintrittswahrscheinlichkeit sowie das erwartete Schadensausmaß erfragt und damit der Risikoerwartungswert als Produkt beider Größen gebildet werden. Dieser kann dann wiederum als Erwartungswert der Standardnormalverteilung dienen, um Verteilungsinformationen zu gewinnen.

Im Gegensatz zur klassenbasierten Zuordnungstabelle, lassen sich mithilfe einer regelbasierten Fuzzy-Logik auch Risikoeinschätzungen für die Übergänge zwischen den Klassen treffen, wodurch die Einschätzung präziser wird (siehe Kapitel 9.2.4). Grundsätzlich ist die Verwendung verbaler Beschreibungen für die einschätzenden Experten nachweislich leichter zu ver-

[240] Vgl. Löhr 2010, S. 87.
[241] Vgl. Diederichs 2012, S. 90.
[242] Vgl. Steinhoff 2008, S. 141 f.
[243] Vgl. van der Gaag et al. 2002, S. 136.

stehen,[244] allerdings ist die Zuordnung von verbaler Beschreibung zu numerischem Wert auch sehr kontextspezifisch und die Abgrenzung zwischen den verbalen Beschreibungen nie ganz eindeutig. Ebenso unterliegen direkt quantitativ ausgedrückte subjektive Einschätzungen einer Ungenauigkeit, da sie durch die subjektive Wahrnehmung und die Risikoaversität des Entscheiders beeinflusst werden. Da die Genauigkeit subjektiver Einschätzungen also generell eingeschränkt ist, muss ihre Aussagekraft kritisch betrachtet werden. Ebenso sind Risiken vielfach nicht normalverteilt, so dass die Annahme einer Normalverteilung nur als Behelf angesehen werden kann. Diese Ungenauigkeiten sprechen im Rahmen des Risikomanagements eher gegen die Verwendung subjektiver Experteneinschätzungen und Verteilungsannahmen. Ihre Verwendung wird jedoch als zielführender angesehen, als ein Risiko gar nicht zu quantifizieren bzw. nicht zu berücksichtigen und es dadurch im schlimmsten Fall zu unterschätzen.[245]

4.3.2.3. Quantifizierung von Risikointerdependenzen

Regulatorische Vorgaben wie der DRS 5 und IDW PS 340 sowie IDW PS 981 verlangen die Berücksichtigung der Wechselwirkungen zwischen Risiken.[246] Diese sogenannten Risikointerdependenzen sind entsprechend zu quantifizieren. Zwar ermöglicht die Quantifizierung von Einzelrisiken einen Überblick über die Risikolage, sie vernachlässigt aber die Berücksichtigung der Interdependenzen. In der anschließenden Risikobeurteilungsphase birgt dies die Gefahr, dass Risiken einzeln als unwesentlich eingestuft werden, obwohl sie im Zusammenwirken gegebenenfalls existenzbedrohend sind.[247] Ebenso besteht die Gefahr einer Überschätzung der tatsächlichen Risikolage. Daher ist es neben der Betrachtung von Einzelrisiken von Interesse, dass etwaige Wechselwirkungen bei der Quantifizierung berücksichtigt werden.

Die Auswahl einer geeigneten Methode zur Quantifizierung von Risikointerdependenzen hängt von diversen Faktoren ab. Ebenso wie bei der Quantifizierung von Einzelrisiken ist zunächst zu unterscheiden, ob die Quantifizierung auf Grundlage subjektiv oder objektiv gegebener Daten erfolgt. Liegt keine objektive Datenbasis vor, kann nur auf Basis intuitiver Vermutungen des Entscheiders auf Interdependenzen sowie den Grad der Korrelation geschlossen werden. Ausgehend von objektiv gegebenen Daten stellt sich die Frage, ob für die betrachte-

[244] Vgl. für die folgenden Ausführungen Steinhoff 2008, S. 196 ff.
[245] Vgl. Gleißner 2011, S. 183.
[246] Vgl. Hempel und Offerhaus 2008, S. 4; Korte und Romeike 2011, S. 94; IDW 2017.
[247] Vgl. Rommelfanger 2008, S. 18.

ten Risiken alle Verteilungsinformationen bekannt sind. Sind diese nicht bekannt, bieten sich die Sensitivitätsanalyse, die Szenarioanalyse oder eine Monte Carlo Simulation als Methode zur Bestimmung des quantitativen Zusammenhangs an.[248] Diese untersuchen jeweils die Wirkung auf einen Outputwert bei Variation eines, mehrerer oder einer sehr großen Anzahl an Inputwerten.

Stehen historische Daten verteilungsabhängiger Einzelrisiken und alle Einflussfaktoren zur Verfügung, kann der Zusammenhang zwischen einer abhängigen und mehreren unabhängigen Variablen mithilfe einer Regressionsanalyse bestimmt werden. Als weiteres Verfahren bietet sich die Korrelationsanalyse an. Der Korrelationskoeffizient

$$p, mit\ -1 <= p <= +1,$$

gibt Aufschluss über Grad und Richtung des Zusammenhangs zweier Risiken. Jedoch resultiert aus einem hohen Korrelationskoeffizienten nicht, dass die Risiken auch eine kausale Abhängigkeit besitzen (sog. Scheinkorrelation). Die Beurteilung der Kausalität kann nur durch Experimente bzw. durch Experten, denen die Ursache-Wirkungs-Beziehungen bekannt sind, erfolgen. Unterstützend kann daher auf analytische Verfahren, wie z. B. die Ereignisbaumanalyse zurückgegriffen werden.[249] Zur Erfassung der Abhängigkeitsstrukturen bietet es sich an, die gemeinsame Verteilung der betrachteten Risiken bzw. ihrer Verteilungen unter Berücksichtigung der Korrelationen zu bilden. Dies leisten die Verfahren der Risikoaggregation.

4.3.2.4. Quantifizierung des Gesamtrisikos (Risikoaggregation)

Als Resultat der Quantifizierung sollte ein kumulierter Wert für das Gesamtrisiko bestimmt werden, da „nur durch Zusammenfassung aller Risiken unter Beachtung der Wechselwirkungen […] der wahre Gesamtrisikoumfang“[250] ersichtlich wird. Die Aggregation von Risiken zielt zwar in erster Linie auf das Gesamtunternehmensrisiko ab, jedoch ist eine Aggregation auf anderen Entscheidungsebenen für die Risikosteuerung und für strategische Überlegungen ebenfalls sinnvoll. Dazu zählen z. B. das Gesamtrisiko einzelner Organisationseinheiten, bestimmter Projekte oder spezifischer Risikoarten. Damit Aussagen zum Umfang eines Gesam-

[248] Vgl. Paetzmann 2012, S. 49 ff.
[249] Vgl. Löhr 2010, S. 92 f.
[250] Vgl. Rommelfanger 2008, S. 16.

trisikos getroffen werden können, sind die quantifizierten Einzelrisiken zu aggregieren. Als simpelste Form der Aggregation, bietet sich die Addition der einzelnen Risikowerte bzw. die Bildung der Gesamtverteilung aus der Zusammenführung der Verteilungen der Einzelrisiken an (Faltung)[251], die dann zur Bildung eines Risikomaßes für das Gesamtrisiko genutzt werden kann. Dies würde allerdings eine vollständige Unabhängigkeit der Risiken suggerieren und etwaige Diversifikationseffekte nicht berücksichtigen. Es droht so die Gefahr, dass das Gesamtrisiko überschätzt wird.[252] Ebenso kann durch die Annahme vollständig unabhängiger Risiken, das Gesamtrisiko unterschätzt werden, da sich Risiken durch Zusammenwirken auch verstärken können. Entsprechend sind die Abhängigkeitsstrukturen möglichst exakt zu berücksichtigen. Das Verfahren der Historischen Simulation liefert im Ergebnis die Gesamtverteilung einer Zielgröße unter Berücksichtigung von (unbekannten) Risiken und ihren Abhängigkeitsstrukturen. Zur Bestimmung der Gesamtverteilung bei bekannten Einzelverteilungen und unter Berücksichtigung der Korrelationen wird in betriebswirtschaftlichen Untersuchungen vielfach auf die Monte Carlo Simulation verwiesen.[253]

Risikoaggregation mithilfe der Historischen Simulation

Die Historische Simulation ist eine Zeitreihenanalyse und ermöglicht die Bestimmung einer Häufigkeitsverteilung für eine Zielgröße auf Basis der historischen Ausprägungen dieser Größe. Dabei wird aus Risikomanagementsicht implizit davon ausgegangen, dass die historischen Ausprägungen der Zielgröße bereits Risiken ausgesetzt waren, die auch auf ihre zukünftigen Ausprägungen einwirken. Zur Durchführung der Historischen Simulation werden für alle historischen Ausprägungen der Zielgröße die jeweiligen absoluten oder relativen Wertänderungen zwischen $n-1$ aufeinander folgenden Perioden bestimmt.[254] Anschließend wird die Ausprägung der Periode n mit jeder der ermittelten Differenzen bewertet, so dass sich unterschiedliche Ausprägungen der Zielgröße auf Basis der historischen Abweichungen ergeben. Dies führt im Ergebnis zu einer Häufigkeitsverteilung, welche implizit die (historisch aufgetretenen) Risikoeinflüsse und Risikokorrelationen berücksichtigt. Auf Basis der so ermittelten

[251] Vgl. Beck et al. 2006, S. 29 ff.
[252] Vgl. Nguyen und Molinari 2009, S. 29.
[253] Vgl. Gleißner und Meier 1999, S. 926; Wolf 2003; Bleuel 2006; Hempel und Offerhaus 2008, S. 223; Rommelfanger 2008, S. 39 ff.; Günther et al. 2009, S. 52 ff.; Wolf und Runzheimer 2009, S. 137 ff.; Löhr 2010, S. 98 ff.
[254] Vgl. Burger und Buchhart 2002, S. 126 f.

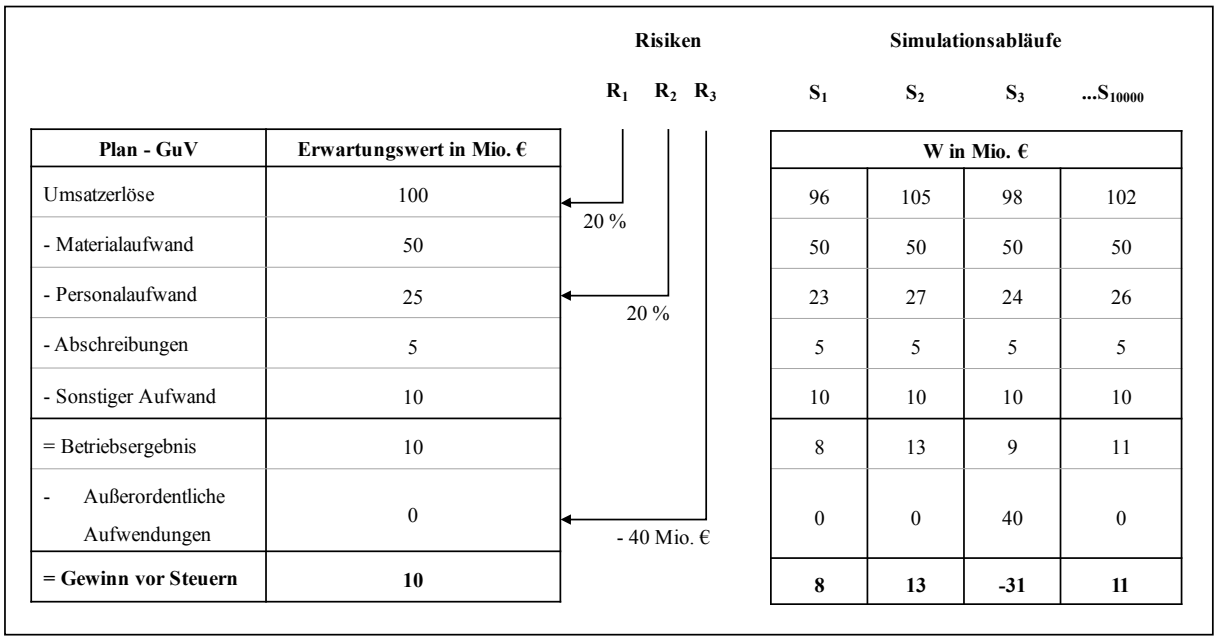
Verteilung können Risikomaße wie der Value at Risk bestimmt werden, um den Gesamtrisikoumfang in einer Kennzahl auszudrücken. Da viele Risiken äußerst selten eintreten, eignen sich zeitreihenbasierte Verfahren wie die Historische Simulation nur bedingt zur Anwendung im Risikomanagement, da sie sich gegebenenfalls nicht in den historischen Ausprägungen der Zielgröße widerspiegeln.

Risikoaggregation mithilfe der Monte Carlo Simulation

Die Monte Carlo Simulation stellt ein Instrument zur experimentellen Bestimmung der Verteilung einer Zielgröße dar. Vielfach wird vorgeschlagen sie im Rahmen der Risikoaggregation zu nutzen, um die Gesamtverteilung der Zielgröße unter Einfluss von Risiken zu erzeugen. Dazu werden die durch Verteilungsfunktionen beschriebenen Einzelrisiken meist in Bezug zur Unternehmensplanung gestellt.[255] Der Einfluss der Risiken auf die Positionen der Unternehmensplanung wird dabei mithilfe einer großen Anzahl an Zufallsexperimenten simuliert. Das Vorgehen lässt sich in drei Schritte aufteilen. Im ersten Schritt wird die Zielgröße definiert (z. B. Gewinn vor Steuern in der Plan-GuV[256]) und festgelegt, welche Einzelrisiken auf die einzelnen Positionen, die Einfluss auf die Zielgröße nehmen, einwirken (z. B. Absatzrisiko wirkt auf Umsatz). Weiterhin wird für jedes Einzelrisiko die bekannte bzw. eine vom Experten unterstellte Verteilung festgelegt. Ebenso können etwaige Korrelationen zwischen zwei Einzelrisiken mithilfe einer Korrelationsmatrix festgehalten werden. Im Falle einer positiven (negativen) Korrelation zwischen zwei Einzelrisiken, kann dies während der Simulation durch Bildung von korrelierten Pseudozufallszahlen berücksichtigt werden, so dass tendenziell hohe (niedrige) Schadensausprägungen des einen Risikos, mit hohen (niedrigen) Ausprägungen des anderen Risikos einhergehen. Im zweiten Schritt erfolgt die Durchführung der Simulation. Für die betrachtete Periode (z. B. ein Geschäftsjahr) wird dazu für jede risikobehaftete Position mehrere tausendmal eine Zufallsvariable unter Berücksichtigung der getroffenen Annahmen erzeugt und mit den nicht risikobehafteten Positionen verrechnet. So ergeben sich unterschiedliche Werte der Zielgröße. Basierend auf dem Gesetz der großen Zahlen liegt nach Durchlauf einer ausreichend großen Anzahl an Simulationen (z. B. 10000 Durchläufe) eine

[255] Vgl. Gleißner 2011, S. 191.
[256] Vgl. Löhr 2010, S. 98.

Ergebnisverteilung vor, die als Basis für die Bestimmung eines Risikomaßes für das Gesamtrisiko herangezogen werden kann. Abbildung 11 verdeutlicht das Vorgehen.



Plan - GuV	Erwartungswert in Mio. €
Umsatzerlöse	100
- Materialaufwand	50
- Personalaufwand	25
- Abschreibungen	5
- Sonstiger Aufwand	10
= Betriebsergebnis	10
- Außerordentliche Aufwendungen	0
= Gewinn vor Steuern	**10**

Simulationsabläufe			
S_1	S_2	S_3	...S_{10000}
W in Mio. €			
96	105	98	102
50	50	50	50
23	27	24	26
5	5	5	5
10	10	10	10
8	13	9	11
0	0	40	0
8	**13**	**-31**	**11**

Abbildung 11: Beispiel einer Risikoaggregation mittels Monte Carlo Simulation[257]

Der darin dargestellte Gewinn der Plan-GuV ist drei Einzelrisiken ausgesetzt, die bei Risikoeintritt die betroffenen Positionen bzw. ihre Ausprägung beeinflussen.[258] Das Risiko R_1 stellt ein Absatzmarktrisiko dar, welches zu einem Umsatzrückgang führen kann. Risiko R_2 beschreibt ein Beschaffungsmarktrisiko (erhöhte Personalkosten). R_1 und R_2 werden als normalverteilt angenommen, wobei sie jeweils mit einer Standardabweichung σ von 20 % um den Erwartungswert der jeweiligen Position schwanken. Im Beispiel wird zwischen den Risiken R_1 (Umsatzrückgang) und R_2 (Personalaufwand) eine negative Korrelation angenommen. Risiko R_3 unterliegt einer Binomialverteilung und tritt mit einer Wahrscheinlichkeit von 2 % ein. Es verursacht bei Eintritt außerordentliche Aufwendungen in Höhe von 40 Mio. Euro. Die Simulationsergebnisse liefern eine empirisch ermittelte Häufigkeitsverteilung und so Informationen über den Erwartungswert des Plan-Gewinns vor Steuern und dessen Standardabweichung. Die Stärke und zugleich die Schwäche des Verfahrens liegt in der Möglichkeit un-

[257] Vgl. Löhr 2010, S. 99.
[258] Das Beispiel ist entnommen aus Löhr 2010, S. 98 ff.

terschiedliche Einzelrisiken mit verschiedenen Verteilungsfunktionen berücksichtigen zu können. Dies ermöglicht sowohl verteilungs- als auch ereignisabhängige Risiken zu einem Gesamtrisiko zusammenzuführen, bedingt aber eine sehr genaue Beurteilung der Einzelverteilungen und ihrer gegenseitigen Korrelationsbeziehungen.

4.4. Phase der Risikoanalyse – Risikobeurteilung

4.4.1. Zielsetzung der Risikobeurteilung

Die Risikobeurteilung dient der Einordnung der zuvor identifizierten und quantifizierten Risiken. In dieser Phase werden die Risiken gemäß ihrer Bedeutung in eine Rangordnung gebracht. Die Risikobeurteilung liefert somit wichtige Informationen für die folgende Phase der Risikosteuerung, indem auf Basis der Beurteilung festgelegt werden kann, welche Risiken aufgrund ihres Gefährdungspotentials für die weitere Unternehmensentwicklung dringlicher betrachtet werden müssen als andere.[259] Die Beurteilung der Risiken ist grundsätzlich von der Risikoeinstellung des Managements abhängig. Diese muss von diesem vorgegeben werden. Darauf aufbauend werden Schwellenwerten festgelegt, um die Risiken auf Basis der Ergebnisse der Quantifizierungsphase geeignet kategorisieren zu können und unter diesen eine Rangordnung hinsichtlich einzuleitender Steuerungsmaßnahmen erstellen zu können.[260] Ein Schwellenwert ist dabei als Wesentlichkeitsgrenze zu verstehen.[261] Wird diese überschritten, gilt das Risiko als eingetreten. Für alle Risiken müssen Schwellenwerte in adäquaten Messgrößen definiert und die entsprechenden Ausprägungen regelmäßig kontrolliert werden.

4.4.2. Methoden der Risikobeurteilung

Konnte im Rahmen der Risikoquantifizierung die Verteilung der Risiken auf Basis objektiv gegebener Daten oder aufgrund von Experteneinschätzungen bestimmt werden, lassen sich Risikomaße wie der Value at Risk berechnen und für die Risikobeurteilung verwenden. Idealerweise wurden alle Risiken mit demselben Maß quantifiziert, um anhand des Maßes eine Rangfolge für die Steuerung der Risiken zu bilden.

---

[259] Vgl. PwC 1999, S. 11; Rücker 1999, S. 109.
[260] Vgl. Diederichs et al. 2004b, S. 192.
[261] Vgl. zur Definition von Schwellenwerten Burger und Buchhart 2002, S. 47 f.

Liegen überwiegend subjektive Risikoeinschätzungen vor, bietet sich eine Kategorisierung der Risiken in Wesentlichkeitsklassen an.[262] Hierbei werden die Risiken anhand der eingeschätzten Eintrittswahrscheinlichkeiten und Schadenausmaße in ordinal oder kardinal skalierten Klassen eingruppiert. Im Falle von ordinal skalierten Klassen erfolgt dies z. B. nach Gefahren mit geringer, mittlerer und hoher Eintrittswahrscheinlichkeit bzw. geringem, mittleren und hohem Schadensausmaß.[263] Kardinal ließe sich dies in Intervallen z. B. nach Schadensausmaß in Höhe von <10 Mio., 10-25 Mio., 25-100 Mio. und >100 Mio. bzw. Eintrittswahrscheinlichkeit <10 %, >10-50 %, >50-90 % und >90 % gestalten.[264] Die Klassengrenzen und Bezeichnungen müssen dabei unternehmensindividuell festgelegt werden. Die Eingruppierung bezieht sich immer auf einen bestimmten Zeitpunkt und muss bei Veränderungen der Risikosituation entsprechend angepasst werden.

Die in Wesentlichkeitsklassen eingeordneten Risiken können im Anschluss mithilfe der sogenannten Risikomatrix (auch Risk Map oder Risikoportfolio genannt) visualisiert werden (siehe Abbildung 12).

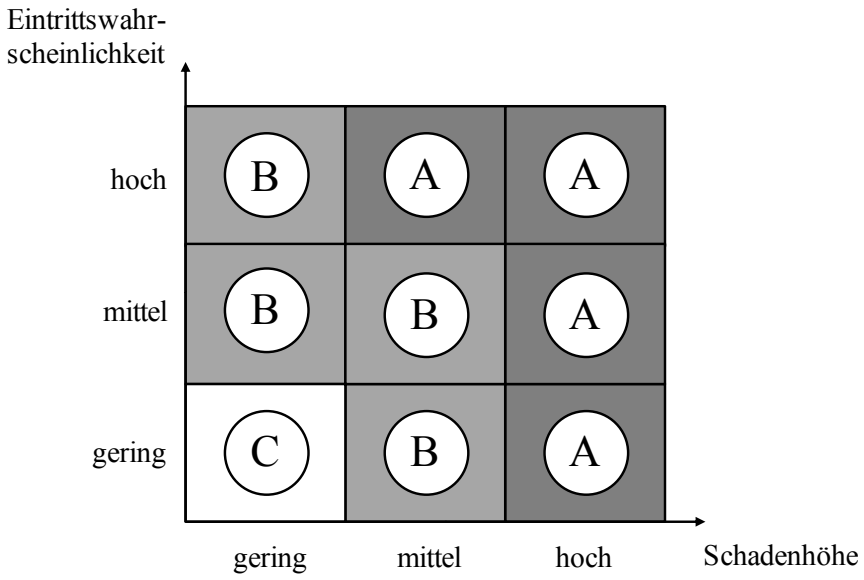


Abbildung 12: Beispiel einer ordinal skalierten Risikomatrix

[262] Vgl. bzgl. folgender Ausführungen Romeike 2003, S. 192; Löhr 2010, S. 87 ff.
[263] Eine abweichende Anzahl an Klassen ist theoretisch möglich, allerdings wird empfohlen diese gering zu halten. Vgl. Burger und Buchhart 2002, S. 104.
[264] Vgl. Diederichs 2012, S. 92.

Die Risikomatrix wird insbesondere aufgrund ihrer leichten Verständlichkeit vielfach in der Praxis verwendet[265] und ist auch in internationalen Standards als geeignete Methode aufgeführt.[266] Nach der Einordnung der Risiken in die Klassen, dient sie als Ausgangspunkt der visuellen Risikobeurteilung. In dem Beispiel in Abbildung 12 können die A-Risiken z. B. als existenzgefährdend, die B-Risiken als erfolgsgefährdend und die C-Risiken als unbedeutend interpretiert werden. Die Darstellung soll Ordnung und Vergleichbarkeit zwischen den Risiken erzeugen und helfen, sie hinsichtlich ihrer Wesentlichkeit zu bewerten, um Steuerungsmaßnahmen einleiten zu können.[267] Je nach Risikoeinstellung des Managements kann so in Abhängigkeit von der Wesentlichkeit eine Rangordnung der Risiken erzeugt und Steuerungsmaßnahmen für die als wesentlicher angesehenen Risiken eingeleitet werden.

Die Darstellungsform der Risikomatrix hat diverse Schwächen, welche insbesondere die Aussagekraft der dargestellten Risikosituation einschränken. Die größte Schwäche besteht darin, dass die Wahrscheinlichkeitsverteilung der Risiken keine Berücksichtigung findet. Weiterhin gehen durch die Klassenbildung Informationen über die genaue Eintrittswahrscheinlichkeit und Schadenshöhe sowie die Risikowechselwirkungen verloren.[268] Letztere sind nur implizit in Eintrittswahrscheinlichkeit und Schadenshöhe enthalten, aber nicht aus der Matrix ersichtlich.[269] Dies ist kritisch, wenn sich, z. B. in Bezug auf Abbildung 12, mehrere C-Risiken zu einem A-Risiko aufschaukeln. Die Risikomatrixdarstellung führt dann im Rahmen der Risikobeurteilung zu einer Unterschätzung dieser C-Risiken. Die Darstellung der Risikowirkung (in Form der Klasseneinteilung bzw. des Schadenerwartungswertes) erfolgt weiterhin nur für eine konkrete Ausprägung des Risikos wie bspw. dem Durchschnitts- oder Höchstschaden und kann so dazu führen, dass falsche Rückschlüsse über das wahre Bedrohungspotential gezogen werden.[270] Trotz dieser Schwächen wird die Risikomatrix insbesondere zur Kommunikation der (vermeintlichen) Risikosituation verwendet.

---

[265] Vgl. Wolf und Runzheimer 2009, S. 209.
[266] Vgl. Duijm 2015, S. 22.
[267] Vgl. Burger und Buchhart 2002, S. 103.
[268] Vgl. Dobler 2005, S. 150.
[269] Vgl. Cox 2008, S. 499; Diederichs 2012, S. 94.
[270] Vgl. Cottin und Döhler 2006, S. 98.

4.5. Phase der Risikosteuerung

4.5.1. Zielsetzung der Risikosteuerung

Auf Basis der Ergebnisse der Risikobeurteilung werden in der Phase der Risikosteuerung Strategien zum Umgang mit den Risiken festgelegt.[271] Grundsätzlich können Steuerungsmaßnahmen getroffen werden, welche entweder bei den Risikoursachen oder den Risikowirkungen ansetzen.[272] Sie zielen darauf ab, die Eintrittswahrscheinlichkeit zu mindern, das Schadensausmaß zu reduzieren oder eine Kombination aus beidem zu realisieren. Das Ziel der Risikosteuerung ist es, die Chancenwahrnehmung bzw. die unternehmerischen Aktivitäten so zu gestalten, dass entstehenden Risiken durch geeignete Steuerungsmaßnahmen, im Sinne der Risikostrategie des Unternehmens, begegnet wird. Die Wahl der Steuerungsstrategie hängt somit von der allgemeinen Risikostrategie des Unternehmens und damit von seiner Risikoaversion bzw. Risikoaffinität ab.[273]

4.5.2. Methoden der Risikosteuerung

Als Grundstrategien der Risikosteuerung lassen sich der Risikoausschluss, die Risikominderung und die Risikoakzeptanz unterscheiden (siehe Abbildung 13).[274] Die Strategie der Risikovermeidung strebt an, keine Risiken einzugehen. Dieses Vorgehen schließt zwar negative Konsequenzen aus, aber es verursacht auch Opportunitätskosten aufgrund des entgangenen Nutzens bei Eingehen des Risikos. Vielfach wird eine Risikovermeidung dann angestrebt, wenn nur wenig Einfluss auf die weitere Entwicklung ausgeübt werden kann. Beispielhaft seien die Aufgabe bestimmter Geschäftsfelder oder die Nicht-Erschließung von riskanten Märkten genannt.[275]

---

[271] Vgl. Zhang und Fan 2014, S. 412.
[272] Vgl. Schierenbeck und Lister 2002, S. 359.
[273] Vgl. Becker et al. 2015, S. 31.
[274] Vgl. im Folgenden Siepermann 2008, S. 43 ff.
[275] Vgl. Rosenkranz und Missler-Behr 2005, S. 45.

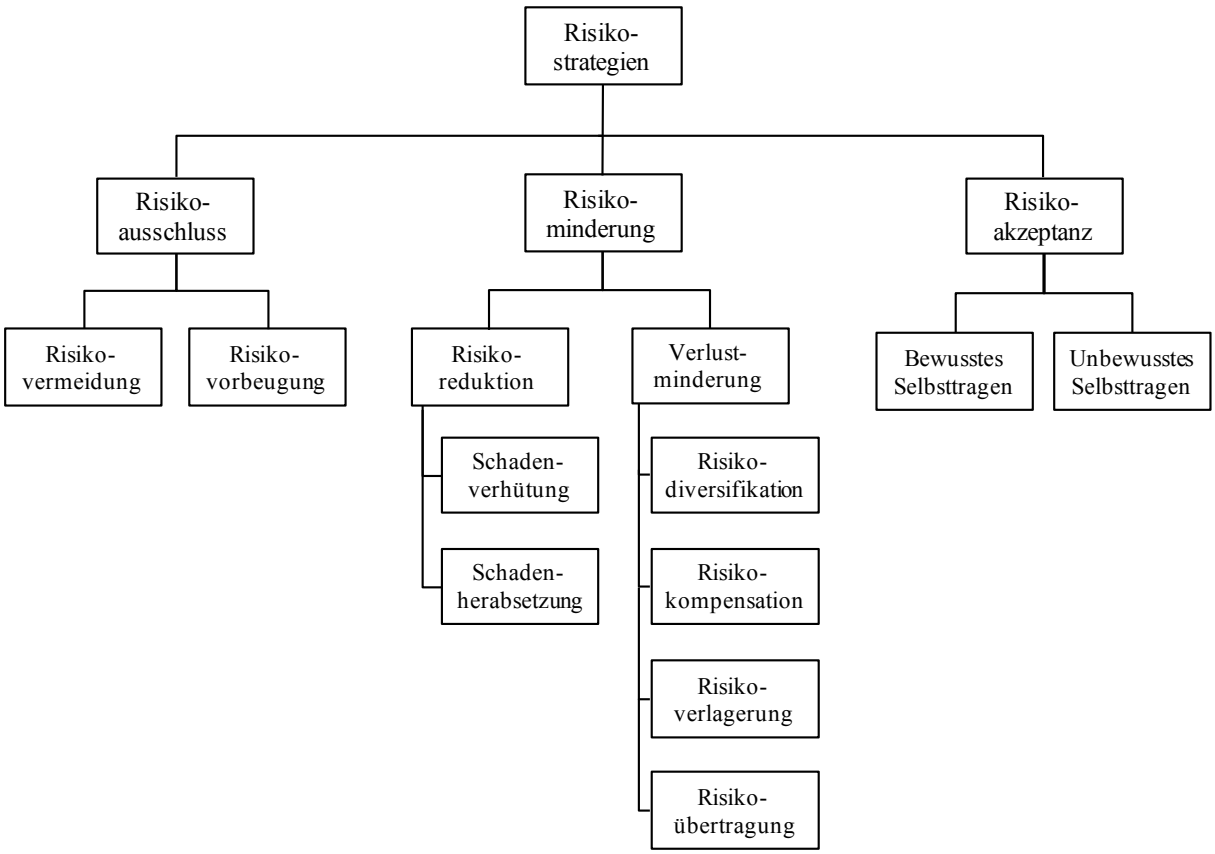


Abbildung 13: Risikostrategien[276]

Im Rahmen von risikovorbeugenden Maßnahmen wird versucht die Eintrittswahrscheinlichkeit oder das Schadenausmaß vor Risikoeintritt auf null zu setzen. Beispielhaft ließe sich dem Risiko eines Gebäudeschadens durch ein Erdbeben vorbeugen, indem das Gebäude erdbebensicher konstruiert wird. Vorbeugende Maßnahmen, welche die Eintrittswahrscheinlichkeit reduzieren, können z. B. technische Vorrichtungen sein, die dafür sorgen, menschliches Versagen auszuschließen.

Mindernde Risikostrategien verfolgen das Ziel, Risiken nicht gänzlich zu vermeiden, sondern ihre Eintrittswahrscheinlichkeit oder ihr Schadensausmaß auf ein akzeptables Niveau zu reduzieren. [277] Im Rahmen der Schadenverhütung werden dazu technische, personelle oder organisatorische Maßnahmen wie bspw. Mitarbeiterschulungen durchgeführt. Die Schadensherabsetzung zielt darauf ab, die Auswirkungen eines Risikoeintritts zu mindern, wie z. B. die Re-

[276] In Anlehnung an Siepermann 2008, S. 44.
[277] Vgl. Ebert 2013, S. 79.

duktion von Brandschäden durch Sprinkleranlagen. Neben den Risikoreduktionsmaßnahmen gehören Maßnahmen zur Verlustminderung zu der Kategorie der Risikominderungsstrategien. Diese streben an, dass Risikoausmaß durch Diversifikation, Kompensation, Verlagerung oder Übertragung auf andere, auf ein Minimum zu reduzieren. Bei der Diversifikation eines Risikos, wird dieses in mehrere Teilrisiken aufgeteilt. So entstehen bei Risikoeintritt nur Teilschäden. Beispielhaft könnte die Produktion einer Firma von der Lagerung räumlich getrennt werden, um das Schadensausmaß durch Umwelteinflüsse zu verteilen.[278] Im Rahmen der Kompensation wird versucht das Gesamtrisiko in negative korrelierte Teilrisiken aufzuteilen. Dazu werden Maßnahmen eingeleitet, die sich zu den bestehenden Chancen und Risiken genau gegenläufig entwickeln. Dies können z. B. Hedging-Geschäfte gegen Preisänderungsrisiken von Vorräten sein oder die Ausweitung des Unternehmensportfolios in sich gegensätzlich entwickelnde Märkte. Die Risikoverlagerung strebt an, durch adäquate Vertragsgestaltung das Risiko auf Partner zu verlagern. Dies können z. B. Qualitätsvorgaben oder vorgegebene Liefertermine sein. Eine übliche verlustmindernde Risikostrategie ist die Risikoübertragung auf andere. Gegen regelmäßige, sichere Zahlung einer geringen Prämie, wird dabei ein unsicherer Gesamtschaden an andere übertragen.[279] Der Abschluss einer Versicherung ist ein Beispiel für eine Art der Risikoübertragung.

Letztlich kann die Strategie der Risikoakzeptanz gewählt werden, wenn Risiken nicht weiter gemindert oder ausgeschlossen werden können. Dabei sollte beim bewussten Selbsttragen der Risiken das potentielle Schadensausmaß durch geeignete Finanzierung gedeckt werden können. Ebenso kann es vorkommen, dass trotz umfassender Risikoidentifizierung ein Risiko nicht erkannt wird und somit unbewusst akzeptiert wird.[280]

[278] Vgl. Thun und Hoenig 2011, S. 245; Cottin und Döhler 2013, S.189.
[279] Vgl. Rosenkranz und Missler-Behr 2005, S. 301 ff.
[280] Vgl. Siepermann 2008, S. 50.

4.6. Phase der Risikoüberwachung

4.6.1. Zielsetzung der Risikoüberwachung

Im Rahmen der Risikoüberwachung müssen zunächst die interne und die externe Überwachung unterschieden werden, da diese eine unterschiedliche Zielsetzung verfolgen. Zum Bereich der internen Risikoüberwachung gehören alle Tätigkeiten, welche auf die Sicherstellung und Prüfung der Funktionsfähigkeit des organisationsweiten Risikomanagementsystems abzielen. Hauptverantwortlich für die interne Risikoüberwachung ist die Interne Revision, welche das Risikomanagementsystem regelmäßig zu überprüfen hat. Dabei sind die Tätigkeiten und Methoden der direkt am Risikomanagementprozess beteiligten Bereiche, welche durch kontrollierende und organisatorische Maßnahmen auf den Risikomanagementprozess einwirken, auf ihre Funktionsfähigkeit hin zu überprüfen. Weiterer Bestandteil der Internen Überwachung sind die am Risikomanagement beteiligten Bereiche selbst, welche regelmäßig den Stand des Risikomanagements prüfen.[281] Hierbei wird untersucht, ob sich Anpassungserfordernisse in den einzelnen Phasen des Risikomanagements ergeben.[282] Bezogen auf die Risikoidentifizierungsphase wird z. B. untersucht, ob die bisher betrachteten Risiken weiterhin relevant sind.[283] Für die Quantifizierungs- und Bewertungsphase müssen die quantifizierten Werte und Schwellenwerte auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Den Schwerpunkt der Risikokontrolle bildet die Überprüfung des Erfolgs, der in der Risikosteuerung festgelegten Maßnahmen.[284]

Die externe Risikoüberwachung wird von Abschlussprüfern und einem etwaig vorhandenen Kontrollgremium, wie z. B. dem Aufsichtsrat einer Aktiengesellschaft, durchgeführt. Sie überprüfen bzw. überwachen das Risikomanagementsystem und die Arbeitsweise der Internen Überwachung mit dem Ziel, das Risikomanagementsystem insgesamt zu beurteilen.

Die aufgeführten Kontrollaktivitäten lassen sich alternativ in die prozessabhängige und die prozessunabhängige Überwachung unterteilen.[285] Dabei umfasst die prozessabhängige Überwachung alle kontrollierenden und organisatorischen Maßnahmen, der direkt am Risikoma-

[281] Vgl. Ebert 2013, S. 103; Gonschorek und Petzold 2014, S. 63 f.
[282] Vgl. Dobler 2005, S. 145.
[283] Vgl. Vanini 2012, S. 251.
[284] Vgl. Kajüter 2012, S. 197.
[285] Vgl. Vanini 2012, S. 250 ff.; Kajüter 2012, S. 199 ff.

nagementprozess beteiligten Stellen.[286] Die prozessunabhängige Überwachung hingegen weist keinen direkten Bezug zu den Abläufen des Risikomanagementprozesses auf, sondern prüft die Abläufe und die Gestaltung des Risikomanagementsystems (siehe Abbildung 14).

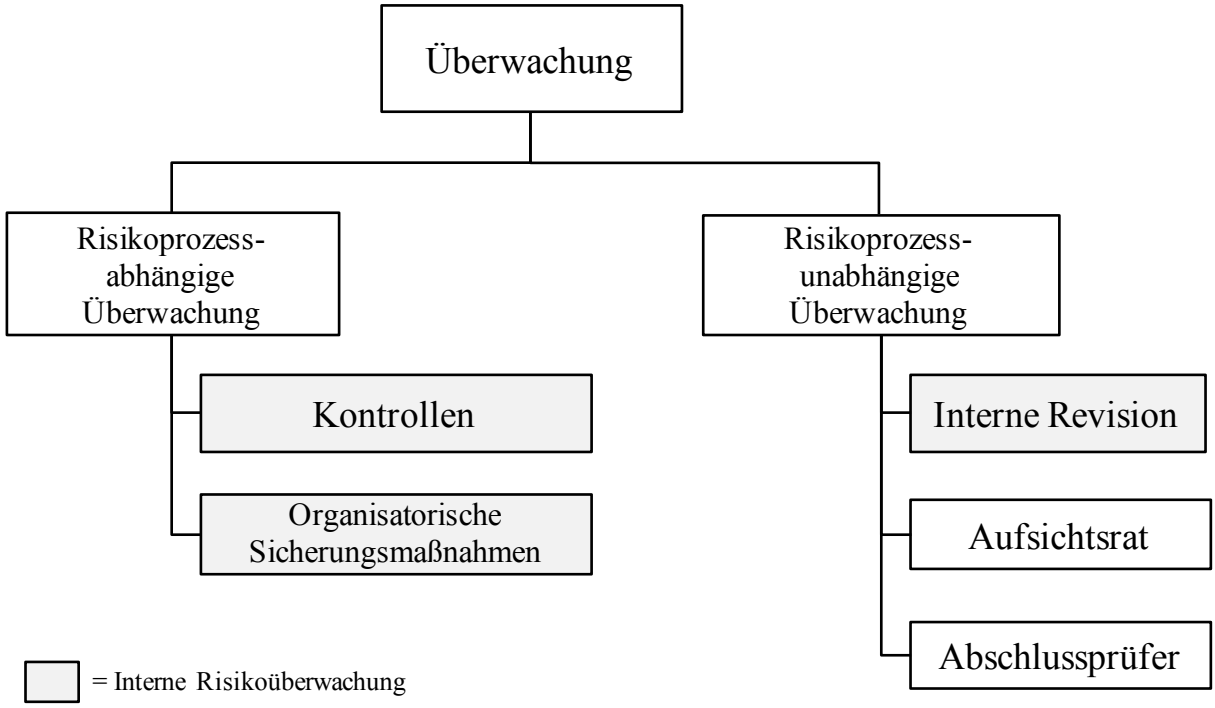


Abbildung 14: Arten der Risikoüberwachung[287]

Eng mit der Überwachung verknüpft ist die anschließende Phase des Risikoreporting. Sie verlangt von den am Risikomanagement beteiligten Bereichen die adressatengerechte Berichterstellung über die Risikolage. Dazu müssen die Adressaten mit zielgruppenspezifisch aufbereiteten Risikoberichten versorgt werden, um ihnen so einen Überblick über die Risikolage zu verschaffen.[288] Primäre Zielgruppen sind neben dem Top-Management insbesondere die Interne Revision, die Abschlussprüfer sowie die Kontrollgremien, die ihren Aufgaben nur durch ein auf ihren Informationsbedarf angepasstes Bild der Risikolage des Unternehmens nachkommen können.[289] Für die Geschäftsleitung sollte ein Risikobericht z. B. eine anschauliche Zusammenfassung der Risikolage beinhalten. Zudem sollte der Bericht Auskunft über die

[286] Vgl. Vanini 2012, S. 251.
[287] In Anlehnung an Vanini 2012, S. 250.
[288] Vgl. Schierenbeck und Lister 2002, S. 370 f.
[289] Vgl. Wolf und Runzheimer 2009, S. 162.

bedeutsamsten Risiken, ihre Auswirkungen und die eingeleiteten Steuerungsmaßnahmen enthalten.[290] Für externe Adressaten muss der Risikobericht Vorgaben von Rechnungslegungsstandards bezüglich des Risikoreporting (z. B. DRS 20) berücksichtigen.[291]

4.6.2. Methoden der Risikoüberwachung

Zur risikoprozessabhängigen Überwachung gehören Kontrollmethoden und organisatorische Sicherungsmaßnahmen. Kontrollen in diesem Sinne sind bspw. die Überwachung des Status eingeleiteter Risikosteuerungsmaßnahmen, um sicherzustellen, dass diese effektiv sind. Ebenso gehören Plausibilitätsprüfungen dazu.[292] Vielfach werden Kontrollen in Form von Soll-Ist-Abweichungsanalysen angewendet. So kann z. B. die Güte zuvor festgelegter Plan- und Schwellenwerte oder von Risikomaßen beurteilt werden. Mittels sogenannter Backtestingverfahren lässt sich in diesem Zusammenhang z. B. die Qualität von Risikoquantifizierungen testen, die auf statistischen Verfahren aufbauen. Eine Risikoquantifizierung die bspw. in einem Zeitpunkt t_0 mittels einer Zeitreihenanalyse erzeugt wurde, wird dabei im Zeitpunkt t_1 rückblickend mit den tatsächlichen Werten verglichen. Ist die Abweichung zu häufig zu hoch, sollten entsprechende Anpassungen vorgenommen werden.[293]

Zu den organisatorischen Maßnahmen der risikoprozessabhängigen Überwachung gehören z. B. Berechtigungskonzepte und Zugriffsbeschränkungen oder aber auch die strikte organisatorische Trennung von Funktionsbereichen. Die risikoprozessabhängige Überwachung fällt meist der Controllingabteilung zu.[294]

---

[290] Vgl. Diederichs 2013, S. 7.
[291] Vgl. Beretta und Bozzolan 2004, S. 267 f.; Deutsches Rechnungslegungs Standards Committee e. V. 2012, S. 26.
[292] Vgl. Diederichs und Imhof 2011, S. 173 f.
[293] Vgl. Vanini 2012, S. 252.
[294] Vgl. Diederichs 2012, S. 19 ff.; Paetzmann 2012, S. 75 f.

5. Geschäftsprozessmanagement

5.1. Überblick

Unter dem Begriff des Business Process Reengineering verschob sich in den 1990er Jahren der Fokus der betrieblichen Aufgabenerfüllung von einer Abarbeitung der Aufgaben, welche vor- und nachgelagerte Prozessschritte nicht berücksichtigt, hin zu einer prozessorientierten Sichtweise der betrieblichen Tätigkeiten.[295] Diese zeichnet sich durch eine strukturierte Gliederung der aus den Unternehmenszielen abgeleiteten Aufgaben in abteilungs- und unternehmensweit zusammenhängende sowie unternehmensübergreifende Geschäftsprozesse aus. Unter einem Geschäftsprozess versteht man dabei eine zeitlich strukturierte und sachlogische Menge von Aktivitäten, die gemeinsam ein „unternehmensrelevantes Ziel verfolgen und zur Bearbeitung auf Unternehmensressourcen zurückgreifen".[296] Es können Kern- und Hilfsgeschäftsprozesse unterschieden werden. Die Kernprozesse leisten einen direkten Beitrag zur Wertschöpfung und haben einen unmittelbaren Bezug zur Produkterstellung bzw. Dienstleistungserfüllung (z. B. ein Produktionsprozess). Die Hilfsprozesse haben keinen direkten Bezug zur Wertschöpfung. Sie unterstützten die Leistungserzeugung durch Aktivitäten, die im Rahmen der Geschäftstätigkeit notwendig sind (z. B. ein Personalbeschaffungsprozess).[297] Im Zuge der Weiterentwicklung hin zu einem kontinuierlichen Prozessmanagement hat sich das Geschäftsprozessmanagement (GPM)[298] heute als ein Führungsinstrument etabliert.[299] GPM stellt im Wesentlichen die Gesamtheit der Konzepte, Methoden und Techniken zur Unterstützung der Gestaltung, Verwaltung, Konfiguration, Ausführung und Analyse von Geschäftsprozessen dar.[300] Trotz vielfach abweichender Vorstellungen über den Kern des GPM,[301] ist sein übergeordnetes Ziel die Verbesserung von Geschäftsprozessen hinsichtlich Effizienz und Effektivität.[302] Ein effektives GPM soll zu flexibleren Organisationen führen, die auf Marktveränderungen besser reagieren können[303] und für Prozesskunden Mehrwerte erzeugen.[304]

---

[295] Vgl. Rump 1999, S. 17 f.; van der Aalst 2016, S. 2.
[296] Vgl. Rump 1999, S. 19.
[297] Vgl. Becker und Kahn 2012, S. 4 ff.
[298] Im Englischen Business Process Management (BPM).
[299] Vgl. Scheer und Klueckmann 2009, S. 15.
[300] Vgl. Weske 2012, S. 5.
[301] Vgl. Smart et al. 2008, S. 494; Wong 2013, S. 720.
[302] Vgl. Hung 2006, S. 22.
[303] Vgl. Stohr und zur Muehlen 2008, S. III f.
[304] Vgl. Kirchmer 2017, S. 9 ff.

5.2. Phasen des Geschäftsprozessmanagements

Zur Strukturierung der GPM Aktivitäten existieren diverse Phasenmodelle.[305] Das GPM unterliegt zunächst vielfältigen Rahmenbedingungen wie bspw. der organisatorischen Einbettung, der Unternehmensstrategie und den daraus abgeleiteten Unternehmenszielen. Die Rahmenbedingungen beeinflussen alle Aktivitäten innerhalb der Phasen:[306]

- Prozessdesign,
- Prozessimplementierung,
- Prozessdurchführung und -überwachung,
- und Prozessevaluation.

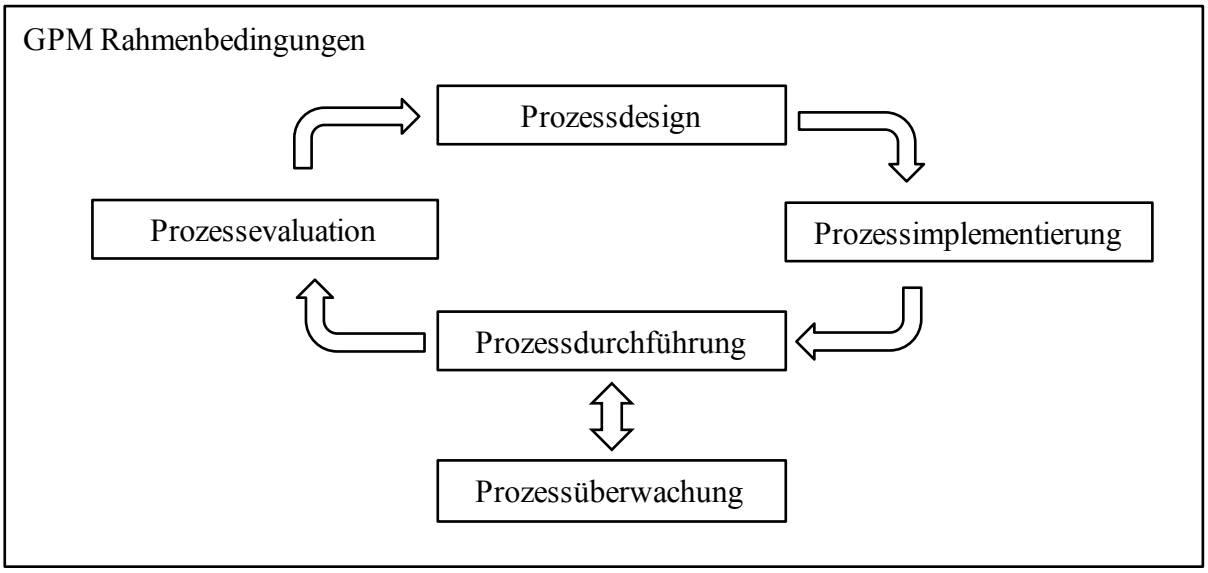


Abbildung 15: GPM-Phasen[307]

[305] Vgl. de Morais et al. 2013 für eine Analyse diverser Ansätze.

[306] Nahezu alle Phasenmodelle, die organisatorische und strategische Rahmenbedingungen berücksichtigen, stellen die dazugehörigen Aufgaben in einer oder mehreren Phasen den anderen Phasen voran. In dieser Arbeit wird jedoch die Ansicht vertreten, dass die organisatorischen und strategischen Vorgaben während der gesamten Zeit des Phasendurchlaufs Veränderungen ausgesetzt sind und sie daher in allen Phasen Einfluss ausüben bzw. der Einfluss sich während des Phasendurchlaufs ändern kann (z. B. Austausch eines Process Owners während der Prozessdurchführung). Daher sollten die organisatorischen und strategischen Aspekte selbst nicht als eine vorangestellte Phase verstanden werden, sondern als beeinflussendes Konstrukt aller Phasen.

[307] Vgl. zur Muehlen und Ho 2006, S. 456.

Organisatorisch verankert wird das GPM z. B. durch die Einrichtung eines Steuerungskomitees.[308] Dieses sorgt für die Identifizierung und Festlegung der zu handhabenden Kerngeschäftsprozesse und die Festlegung der Prozessverantwortlichen (sogenannte Process Owner). Die Prozessverantwortlichen bestimmen und analysieren gemeinsam die Abhängigkeiten zwischen den Kernprozessen. Im Ergebnis entsteht eine Prozesslandkarte der Kerngeschäftsprozesse und ihrer Verbindungen untereinander. Losgelöst von den rahmenbildenden Tätigkeiten und Vorgaben, durchläuft jeder Geschäftsprozess die aufgeführten fünf Phasen.

5.2.1. Phase des Prozessdesigns

In der Prozessdesignphase werden die Geschäftsprozesse ausgehend von ihren Zielen beschrieben. Dazu werden die einzelnen Prozessaktivitäten, die benötigten Ressourcen (z. B. Mitarbeiter, IT etc.) und die jeweiligen zeitlichen und sachlogischen Zusammenhänge zueinander in Verbindung gesetzt, um die definierten Prozessziele zu erfüllen. Interne und externen Einflüsse sowie Schnittstellen werden dabei ebenfalls berücksichtigt.[309] Für die spätere Prozessüberwachung und -evaluation werden in dieser Phase, ausgehend von den Prozesszielen, konkrete Kennzahlen abgeleitet, anhand welcher sich der Grad der Zielerfüllung messen lässt.[310] Des Weiteren fallen die Strukturierung und Definition der aufbauorganisatorischen Einbindung in diese Phase.[311] Entsprechend werden hier Zuständigkeiten für die Durchführung der Prozessaktivitäten definiert. Die Beschreibung der Prozesse kann textuell, tabellarisch oder grafisch erfolgen. Überwiegend hat sich eine grafische Modellierung mithilfe geeigneter Modellierungssprachen wie z. B. der Ereignisgesteuerten Prozesskette (EPK) oder der Business Process Modell and Notation (BPMN) durchgesetzt. Die dabei erzeugten Prozessmodelle dienen zunächst der Dokumentation der Geschäftsabläufe. Aufgrund der standardisierten Darstellung dieser Modelle können unterschiedliche Stakeholder auf einer gemeinsamen Basis ein Verständnis der Prozessabläufe erlangen. Weiterhin bilden die im Prozessdesign gestalteten Prozessmodelle den Ausgangspunkt für die Optimierung bestehender Prozessabläufe.[312] Innerhalb eines Prozesses sind an verschiedenen Stellen Entscheidungen auf Basis festgelegter Bedingungen zu treffen (z. B. bei Prozessverzweigungen und innerhalb von

[308] Vgl. Weske 2012, S. 376.
[309] Vgl. zur Muehlen und Ho 2006, S. 457.
[310] Vgl. Weske 2012, S. 376.
[311] Vgl. Rieke 2009, S. 81.
[312] Vgl. Weske 2012, S. 12 ff.

Aktivitäten). Zur Abbildung dieser Bedingungen unterscheidet man zunächst Routing Rules und Business Rules,[313] die idealerweise bereits in der Prozessdesignphase definiert werden. Routing Rules stellen Bedingungen für Prozessverzweigungen dar, auf deren Basis entschieden wird, welcher Prozesspfad eingeschlagen wird. Sie sollten direkt im Prozessmodell notiert werden, damit die Prozessabfolge eindeutig ist. Für die Phase der Prozessdurchführung, muss zum Teil auf komplexe Geschäftsregeln, die Business Rules, zurückgegriffen werden. Sie stellen Richtlinien und Geschäftspraktiken dar, die das Verhalten des Unternehmens leiten und die Prozessverläufe präzisieren.[314] Aus Gründen der Übersichtlichkeit und Flexibilität werden diese idealerweise in einem separatem Business Rule Management System (BRMS) verwaltet. Es lassen sich diverse Arten von Business Rules unterscheiden:[315]

Business Rule Typ	**Gegenstand**
Integritätsregeln	Integritätsregeln definieren erlaubte Zustände von Daten. Eine Verletzung der Bedingung führt immer zu einem Fehler. Beispiel: *Eine EPK-Funktion besitzt genau eine ein- und genau eine ausgehende Kante.*
Ausführungsregeln	Ausführungsregeln beschreiben die Ausführungslogik einer Aktivität. Ihre Erfüllung, löst eine Aktion aus. Beispiel: *Wenn ein Kunde ein Neukunde ist, muss seine Bonität geprüft werden.*
Inferenzregeln	Inferenzregeln leiten aus einer Bedingung neue Informationen ab. Beispiel: *Wenn ein Prozess Ergebnisse für das Reporting erzeugt, ist er Sarbanes-Oxley relevant.*
Präsentationsregeln	Präsentationsregeln ändern die Darstellung. Beispiel: *Wenn ein Prozessrisiko eine hohe Priorität hat, muss das zugehörige Symbol im Prozessmodell rot dargestellt werden.*

Abbildung 16: Auswahl von Business Rule Typen[316]

[313] Vgl. Freund und Rücker 2012, S. 180.
[314] Vgl. Wagner und Klückmann 2006, S. 134.
[315] Vgl. Rieke 2009, S. 90.
[316] Vgl. Rieke 2009, S. 90.

5.2.2. Phase der Prozessimplementierung

Im Rahmen der Prozessimplementierung werden die modellierten Prozesse in den operativen Betrieb überführt. Dabei werden organisatorische und technische Aspekte berücksichtigt. Die organisatorischen Aspekte umfassen alle Maßnahmen, welche die Prozessbeteiligten in die Lage versetzen, ihre Prozessaufgaben zielorientiert zu erfüllen. Dazu gehören z. B. Schulungen und die Prozesserläuterung für die betroffenen Personen. Die technischen Aspekte beinhalten die Konfiguration der Anwendungssysteme wie z. B. von Workflow Management Systemen (WFMS), Business Process Engines und Business Rule Management Systemen sowie weiterer technischer Ressourcen, die (ggf. automatisierte) Prozessaufgaben übernehmen.[317] Systeme wie Business Process Engines ermöglichen die vollständige Verwaltung und Steuerung der Geschäftsprozesse. Mit ihnen können Prozesse modelliert, in den Betrieb überführt, gesteuert, überwacht und analysiert werden. Dabei unterstützen die Systeme sowohl Aktivitäten, die durch Menschen ausgeführt werden (z. B. manuelle Aufgabenbearbeitung in einem Anwendungssystem), als auch maschinelle automatisierte Aktivitäten, die z. B. über Schnittstellen durch externe Anwendungssysteme bearbeitet werden (siehe Abbildung 17).

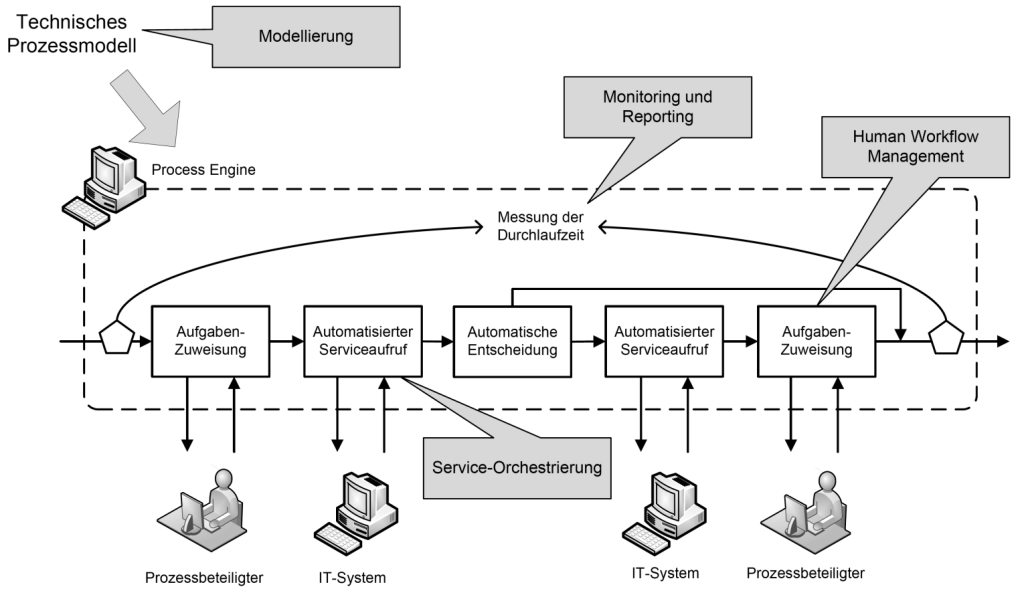


Abbildung 17: Arbeitsweise einer Process Engine[318]

[317] Vgl. Rieke 2009, S. 81.
[318] Entnommen aus Freund und Rücker 2012, S. 191.

Process Engines kennen zu jeder Zeit den Status aller Prozessinstanzen und regeln den Datenfluss zwischen den verschiedenen prozessbeteiligten Akteuren und Systemen.
Des Weiteren sind nicht nur Informationssysteme einzurichten und bereitzustellen, welche die Prozesssteuerung unterstützen, sondern insbesondere auch IT-Systeme, die im Verlauf der Prozessdurchführung benötigt werden. Dazu zählen im Einzelnen: [319]

- *Transaktionssysteme*: Ein Großteil der in Geschäftsprozessen ausgeführten Aktivitäten wird durch betriebliche Informationssysteme wie z. B. ERP-Systeme unterstützt. Sie stellen wichtige Daten bereit bzw. verarbeiten Daten, die während der Prozessdurchführung benötigt werden bzw. entstehen.
- *Systeme zur individuellen Unterstützung*: Hierzu zählen Systeme wie z. B. Office-Anwendungen oder E-Learning Systeme. Erstere werden z. B. für die Dokumentation des Outputs von Prozessaktivitäten benötigt und letztere z. B. für die Schulung von Mitarbeitern.
- *Kommunikations- und Steuerungssysteme*: Neben den Process Engines und Workflow-Management Systemen unterstützen auch andere Systeme die aktive Prozesssteuerung. Dazu zählen z. B. Groupware Lösungen zur Kommunikation.
- *Systeme zur Planung und Kontrolle*: Insbesondere langfristige, wenig standardisierte Prozesse erfordern häufig eine dedizierte Planung und Überwachung. Unter anderem kommen hier z. B. Projektmanagement-Systeme zum Einsatz.
- *Entscheidungsunterstützungssysteme*: Zur Auswertung von Prozessabläufen und zur Unterstützung von Prozessaktivitäten werden Analysetools benötigt, die z. B. ex-post Analysen der Prozessinstanzen mittels Process Mining ermöglichen oder umgekehrt den Prozessen relevante Business Intelligence Auswertungen zur Verfügung stellen.

5.2.3. Phasen der Prozessdurchführung und -überwachung

In der Phase der Prozessdurchführung werden die durch ein eindeutiges Startereignis ausgelösten Prozesse ausgeführt. Ein einzelner Durchlauf eines Prozesses wird dabei als Prozessinstanz bezeichnet.[320] Es können keine, eine oder mehrere aktive Prozessinstanzen existieren. Als Beispiel sei die Bearbeitung eines Kundenauftrags genannt. Die bei einer Auftragsertei-

[319] Vgl. im Folgenden Allweyer 2011, S. 223 ff.
[320] Vgl. Weske 2012, S. 14.

lung abzuarbeitenden Prozessschritte sind für alle Aufträge gleich. Je nach Auftragslage kann es keine aktive Prozessinstanz (kein Auftrag), eine aktive Prozessinstanz (ein Auftrag) oder mehrere aktive Prozessinstanzen (mehrere zeitgleiche Aufträge) geben. Bei mehreren aktiven Instanzen kann jede Instanz einen anderen Status besitzen.

Parallel zur Prozessdurchführung wird im Rahmen der Prozessüberwachung der Status jeder Instanz beobachtet und die Einhaltung etwaiger zuvor definierter Vorgabewerte bzw. Schwellenwerte überwacht.[321] Die Überwachung dient der Gewährleistung eines reibungslosen Ablaufes, indem Über- oder Unterschreitungen der Schwellenwerte Maßnahmen auslösen, die einem unerwünschten Prozessverhalten entgegenwirken.[322] Sie ist weiterhin bedeutend, um jederzeit den Status einer Prozessinstanz, z. B. bei einer Kundenanfrage, zu kennen. Die Ausführung und Überwachung der Prozessinstanzen erfolgt in der Regel IT-gestützt mittels der im Rahmen der Prozessimplementierung konfigurierten Informationssysteme.

5.2.4. Phase der Prozessevaluation

Üblicherweise werden die im Rahmen der Prozessausführung anfallenden Daten in einem Informationssystem gespeichert, so dass zum einen die Aufgaben der Prozessüberwachung bewältigt werden können und zum anderen ex-post Analysen der ausgeführten Prozessinstanzen möglich sind. Im Zuge der Prozessevaluation werden diese Daten ausgewertet und für das Prozessdesign bzw. das Prozessredesign Verbesserungen abgeleitet sowie gegebenenfalls neue Anforderungen an die Phase des Prozessdesigns übergeben.[323] Ein Verfahren der Prozessanalyse ist die Betrachtung verschiedener Kennzahlen wie bspw. die durchschnittliche Prozessdurchlaufzeit oder der Grad der Einhaltung von Service Level Agreements.

Daneben existieren moderne Verfahren der Datenanalyse, die es ermöglichen, die tatsächlichen Prozessabläufe nahezu exakt nachzubilden und unerwünschtes Prozessverhalten sowie strukturelle Prozessschwachstellen wie z. B. Flaschenhälse aufzudecken. Diese unter dem Begriff des Process Mining zusammengefassten Methoden zur Prozessanalyse verwenden dazu die Datenspuren, die während der Prozessdurchläufe in den IT-Systemen hinterlassen wurden. Die Datenspuren werden für das Process Mining zunächst so aufbereitet, dass ein Prozesslogfile entsteht (siehe Abbildung 18), welches Informationen über jede IT-gestützte

[321] Vgl. Neumann et al. 2012, S. 314.
[322] Vgl. Gericke et al. 2013, S. 29 f.
[323] Vgl. van der Aalst et al. 2003, S. 5.

Prozessaktivität, den Zeitpunkt der Ausführung jeder Aktivität sowie der Zuordnung jeder Aktivität zu einer eindeutigen Fallnummer beinhaltet (Minimalanforderungen für Process Mining).

Case ID	Event ID	Timestamp	Activity	Resource	...
1	35654423	30-12-2016:11.02	register request	Peter	...
	35654424	31-12-2016:10.06	examine thoroughly	Susanne	...
	35654425	05-01-2017:15.12	decide	Michael	...
	35654426	06-01-2017:11.18	reject request	Sarah	...
2	35654483	30-12-2016:11.32	register request	Peter	...
	35654485	30-12-2016:12.12	examine casually	Susanne	...
	35654487	30-12-2016:14.16	decide	Michael	...
	35654489	06-01-2017:11.22	pay compensation	Ellen	...
...	...	...	...	...	...

Abbildung 18: Logfileauszug eines Versicherungsprozesses[324]

Letztere steht für einen eindeutigen Prozessdurchlauf von Anfang bis Ende. Somit sind einer Fallnummer mehrere Ereignisse bzw. Aktivitäten zugeordnet. Weitere prozessbezogene Informationen können ebenfalls in das Logfile bzw. die Analyse mit aufgenommen werden. Unter Anwendung von Process Mining Algorithmen in speziellen Softwaretools[325] können in den Logfiles Muster von häufig wiederkehrenden Prozessabläufen identifiziert werden.[326] Meist wird das Ergebnis grafisch in einer Prozessnotation (z. B. BPMN) aufbereitet, so dass das erzeugte (tatsächliche) Prozessmodell (siehe Abbildung 19) für Schwachstellenanalysen verwendet werden kann. Neben Performanceanalysen der tatsächlichen Prozessverläufe sind hierbei Vergleichsanalysen des aus den Daten generierten Ist-Prozesses mit dem vorgesehenen Soll-Prozess möglich (Conformance Checking).[327]

[324] Vgl. van der Aalst 2011, S. 99.
[325] Vgl. z.B. https://celonis.com/ oder https://fluxicon.com/disco.
[326] Für einen umfassenden Einblick in die Verfahren vgl. van der Aalst 2011.
[327] Vgl. van der Aalst 2011, S. 191 ff.

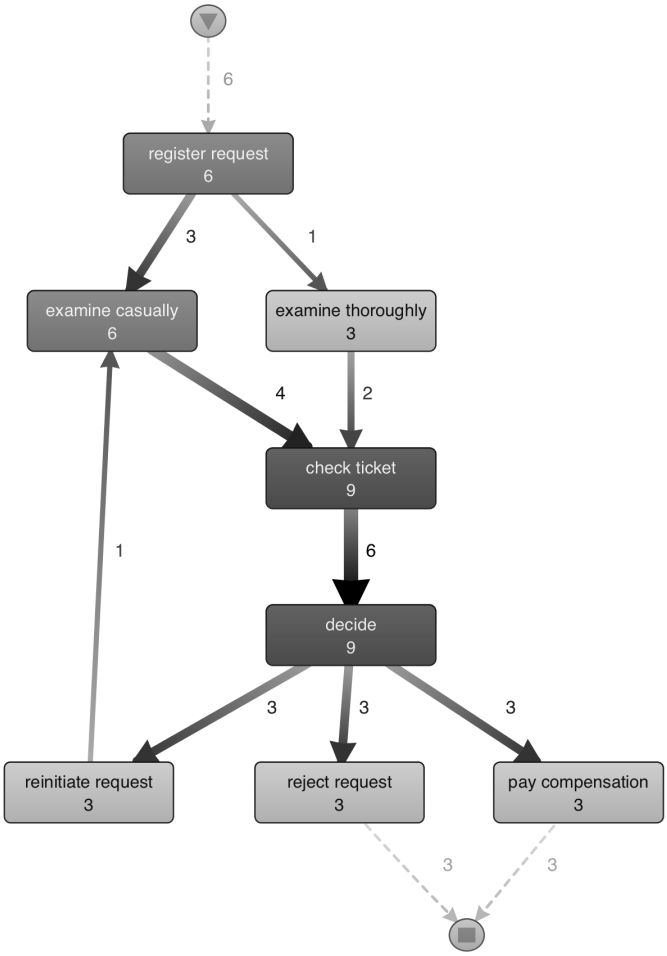


Abbildung 19: Aus Logfile erzeugter Kontrollfluss des Process Mining Tools Disco

5.3. Geschäftsprozessmodelle

5.3.1. Überblick

Einen wesentlichen Teil des Prozessmanagements machen Geschäftsprozessmodelle aus, da sie die notwendigen Schritte zur Prozesszielerfüllung leicht verständlich grafisch spezifizieren.[328] Sie bilden dazu die zeitlich-sachlogischen Abläufe der Realwelt in einem Modell ab, welches nach den Regeln einer Modellierungssprache (Notation) konstruiert wird.[329] Die Ziele der Geschäftsprozessmodellierung sind vornehmlich die Dokumentation der Prozesse und die Unterstützung bei der Optimierung selbiger.[330] Die dokumentierten Prozessmodelle dienen dem Verständnis der Prozessabläufe, helfen bei der Diskussion betrieblicher Verfahrensweisen und reduzieren komplexe organisatorische Zusammenhänge auf ein abstraktes Niveau.[331] Sie können weiterhin als Planungsinstrument genutzt werden, um strukturelle Schwachstellen vor der Implementierung des Prozesses zu entdecken und zu vermeiden. Dazu werden z. B. auf den Modellen aufbauende computergestützte Prozesssimulationen genutzt, die dabei helfen, das Prozessverhalten hinsichtlich bestimmter Charakteristika wie bspw. Durchlaufzeit, Ressourcenbeanspruchung und Kosten zu analysieren.[332] Im Rahmen der Prozessevaluation dienen die Prozessmodelle der Identifizierung von Soll-Ist-Abweichungen zwischen dem ursprünglich geplanten Modell und dem tatsächlichen erfolgten Ablauf (siehe Kapitel 5.2). Zur Modellierung von Geschäftsprozessen existiert eine Vielzahl an Notationen.[333] Weit verbreitet sind insbesondere die Notation der Ereignisgesteuerten Prozesskette (EPK) und die Business Process Model and Notation (BPMN).[334]

5.3.2. Ereignisgesteuerte Prozessketten (EPK)

Die EPK ist eine Notation zur fachkonzeptionellen Modellierung von Prozessen.[335] Sie kann durch Aneinanderreihung von Ereignissen und Funktionen komplexe Prozesszusammenhänge darstellen. Die Basiselemente der EPK sind Ereignisse, Funktionen, Operatoren und Kontrollflüsse zur Abbildung kausaler Zusammenhänge.

---

[328] Vgl. Baumgrass et al. 2014, S. 85.
[329] Vgl. Rump 1999, S. 20; Recker 2010, S. 183.
[330] Vgl. Rump 1999, S. 20 f.
[331] Vgl. Bandara et al. 2005, S. 347.
[332] Vgl. Liu et al. 2012, S. 685; Weske 2012, S. 12 f.
[333] Vgl. Recker et al. 2009, S. 334.
[334] Vgl. Kocbek et al. 2015, S. 535; Riehle et al. 2016, S. 61.
[335] Vgl. im Folgenden Becker et al. 2009, S. 43 ff. sowie Weske 2012, S. 161 ff.

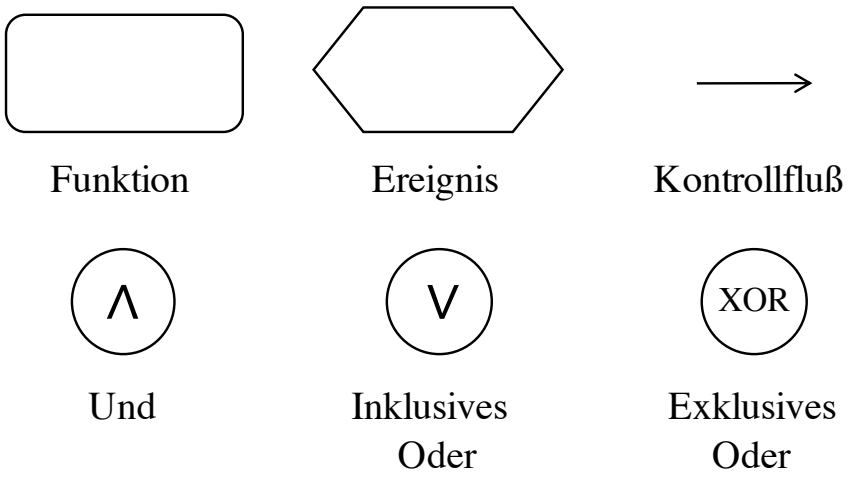


Abbildung 20: Basiselemente der EPK

Ein Ereignis repräsentiert den Eintritt eines Zustands und löst Funktionen aus oder stellt den Status nach Durchführung einer Funktion dar. Beispiele für Ereignisse sind der Eingang einer Rechnung („Rechnung geht ein“) oder das Ende eines Fertigungsauftrags („Fertigungsauftrag rückmelden“). Sie haben passiven Charakter und können keine Entscheidungen treffen. Jeder Prozess hat mindestens ein Start- und ein Endereignis. Funktionen hingegen haben aktiven Charakter und stellen Aktivitäten da, die ein Input- in ein Outputdatum transformieren. Entscheidungen, die den weiteren Prozessverlauf durch entsprechend verbundene Ereignisse beeinflussen, werden in den Funktionen getroffen. Ereignisse und Funktionen werden über Kontrollflüsse verbunden, welche die zeitlich-sachlogischen Abläufe verdeutlichen. Mittels logischer Verbindungen, den Operatoren, können Kontrollflüsse getrennt oder zusammengeführt werden. Man unterscheidet den Und Operator, den Inklusiv-Oder Operator (entweder *a oder b* oder *a und b*) und den Exklusiv-Oder Operator (*entweder a oder b,* aber *nicht beide*). Die zulässigen Verknüpfungen der EPK sind in Abbildung 21 aufgeführt. Nicht zulässig sind Verknüpfungen, in denen nach einem Ereignis eine Entscheidung (In-/Exklusiv-Oder Operator) getroffen werden muss. Ein Ereignis ist immer passiv und kann daher keine Entscheidung treffen, welcher Prozesspfad gewählt wird.

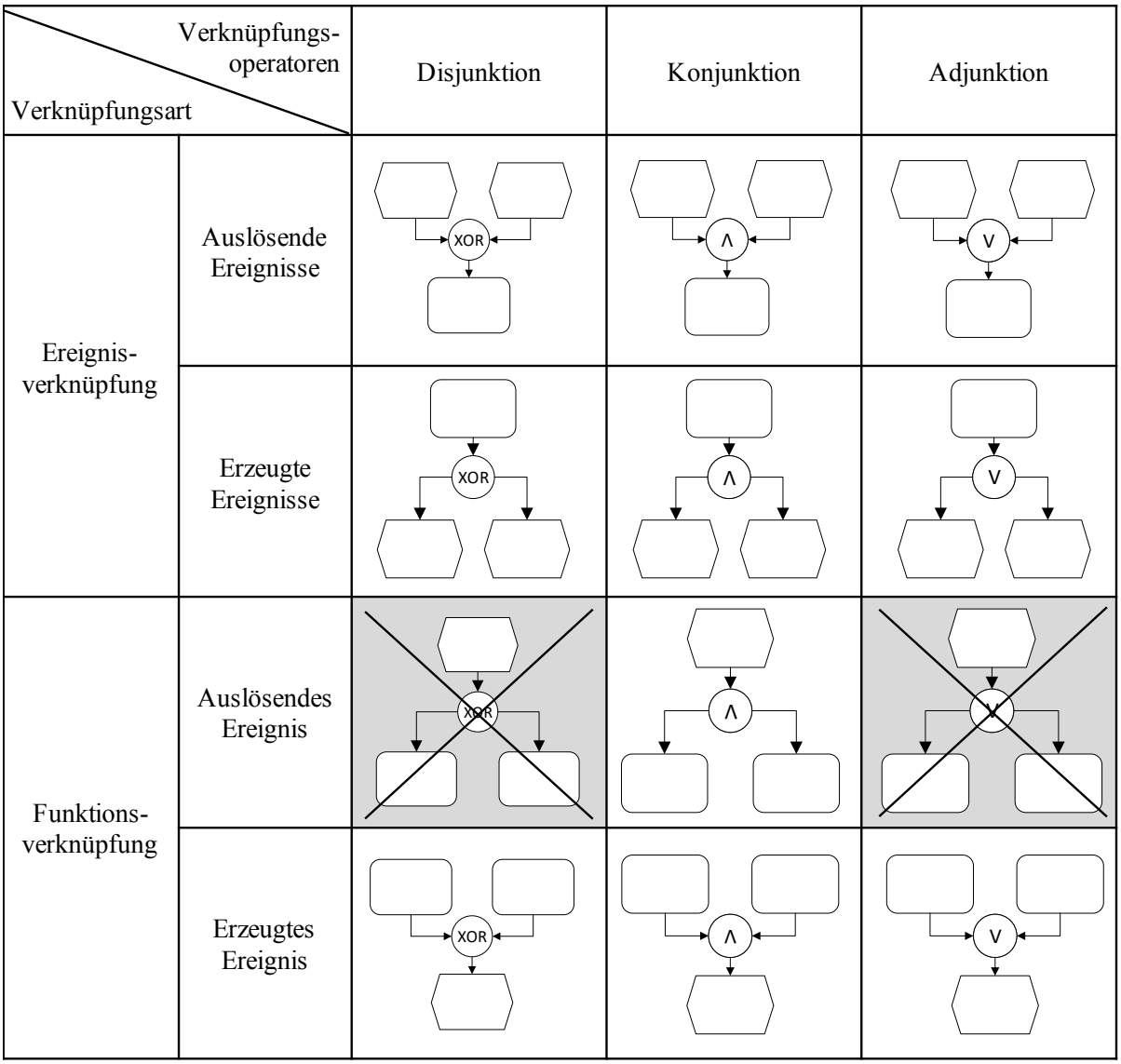


Abbildung 21: Zulässige Verknüpfungsoperatoren[336]

In Abbildung 22 verdeutlicht ein Beispiel den Aufbau einer EPK. Ein Kundenauftrag löst den Prozess aus und wird zunächst geprüft. Wenn der Auftrag abgelehnt wird, ist der Prozess beendet. Andernfalls wird der Lagerbestand überprüft. Ist nicht genug Ware im Lager, wird eine Bestellung beim Lieferanten ausgelöst. Sind die Waren auf Lager oder trifft die neue Liefe-

[336] In Anlehnung an Becker et al. 2009, S. 48.

rung vom Lieferanten ein, werden die Waren an den Kunden versendet und es erfolgt der Rechnungsversand. Das Eintreffen der Bestellung ist als externes Ereignis zu modellieren, da es losgelöst vom Prozess eintritt und nicht beeinflusst werden kann.

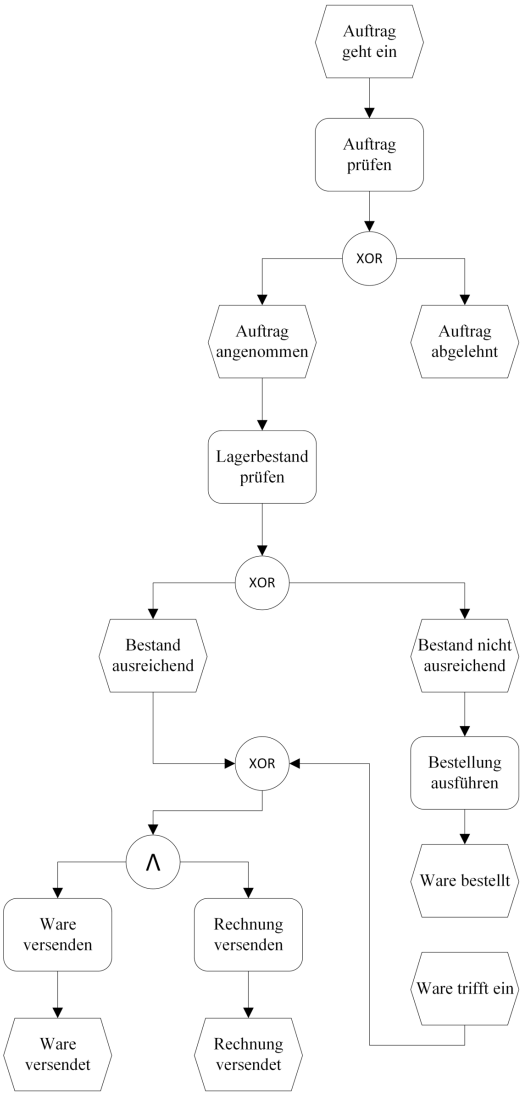


Abbildung 22: Beispiel einer EPK[337]

Die EPK wurde nach und nach durch weitere Elemente zur Erweiterten EPK (eEPK) ausgebaut. Sie ermöglichen z. B. die Integration der Organisationssicht zur Abbildung von Verantwortlichkeiten für Funktionen und die Integration der Datensicht zur Abbildung von in Funktionen benötigten Daten sowie von den Funktionen erzeugter Daten.

[337] Vgl. Weske 2012, S. 165.

Folgende Regeln gelten für die EPK:[338]

1. Es existieren Ereignisse und Funktionen, diese sind über Kontrollflüsse miteinander verbunden.
2. EPKs sind bipartite Graphen: Auf ein Ereignis muss eine Funktion folgen und auf eine Funktion ein Ereignis.
3. EPKs sind zusammenhängende Graphen: Alle Knoten müssen über Pfade (Kanten) von jedem beliebigen Knoten aus erreicht werden.
4. Für Funktionen kann ein verfeinertes Prozessmodell hinterlegt sein.
5. Es gibt Prozess-Schnittstellen – diese treten entweder vor einem Startereignis oder nach einem Endereignis ein.
6. Kontrollflüsse sind gerichtete Kanten, die von oben nach unten verlaufen und somit den Zeitablauf widerspiegeln.
7. Funktionen können weitere Informationsobjekte hinzugefügt werden.
8. Kontrollflüsse können durch Konnektoren („Und“, „Inklusiv-Oder“ und „Exklusiv-Oder“) geteilt und zusammengeführt werden.
9. Nach einem Ereignis darf kein verzweigendes „Exklusiv-Oder“ auftreten – auch dann nicht, wenn zwischen dem letzten Ereignis und dem „Exklusiv-Oder“ nur Konnektoren liegen (und keine Funktion).

5.3.3. Business Process Model and Notation (BPMN)

Die BPMN verfolgt das Ziel die Best Practices bestehender Modellierungssprachen in sich zu vereinen.[339] Insbesondere soll die Notation für alle Anwendergruppen (Fachanwender, Entwickler und prozessausführende Mitarbeiter der Unternehmung) leicht verständlich und verwendbar sein.[340] Sie strebt an, das allgemeine Problem zu beheben und dass fachlich konzipierte Prozessmodelle nicht direkt für die Konfiguration der technischen Anwendungssysteme genutzt werden können. Mit der BPMN „soll praktisch ‚auf Knopfdruck' ein lauffähiges Informationssystem (z. B. eine Business Process Engine) konfiguriert werden können, welches die Prozessausführung steuert und überwacht.“[341] Mit der Version 2.0 der BPMN wurde dazu die Ausführbarkeit der modellierten Prozesse explizit vorangetrieben, indem die Spezifikation

[338] Vgl. Becker et al. 2009, S. 57.
[339] Vgl. Weske 2012, S. 206.
[340] Vgl. Becker et al. 2009, S. 70 f.
[341] Vgl. Becker et al. 2009, S. 71.

ein Mapping der wesentlichen BPMN Elemente mit der XML-basierten Prozessausführungssprache WS-BPEL[342] beschreibt. Des Weiteren wurde die BPMN 2.0[343], im Gegensatz zu ihren Vorgängerversionen und der zuvor beschriebenen EPK,[344] um ein Metamodell erweitert, welches eine formale Spezifikation der Sprachkonstrukte vornimmt. Dadurch soll die Austauschbarkeit der Prozessmodelle zwischen verschiedenen Modellierungswerkzeugen gewährleistet werden. Weiterhin verfügt die BPMN über einen Erweiterungsmechanismus, der es ermöglichen soll, die Notation für spezifische Anwendungszwecke zu erweitern. Die Basiselemente der Notation lassen sich den fünf Kategorien Flussobjekte, Daten, Verbindungsobjekte, Schwimmlinien und Artefakte zuordnen (siehe Abbildung 23).[345]

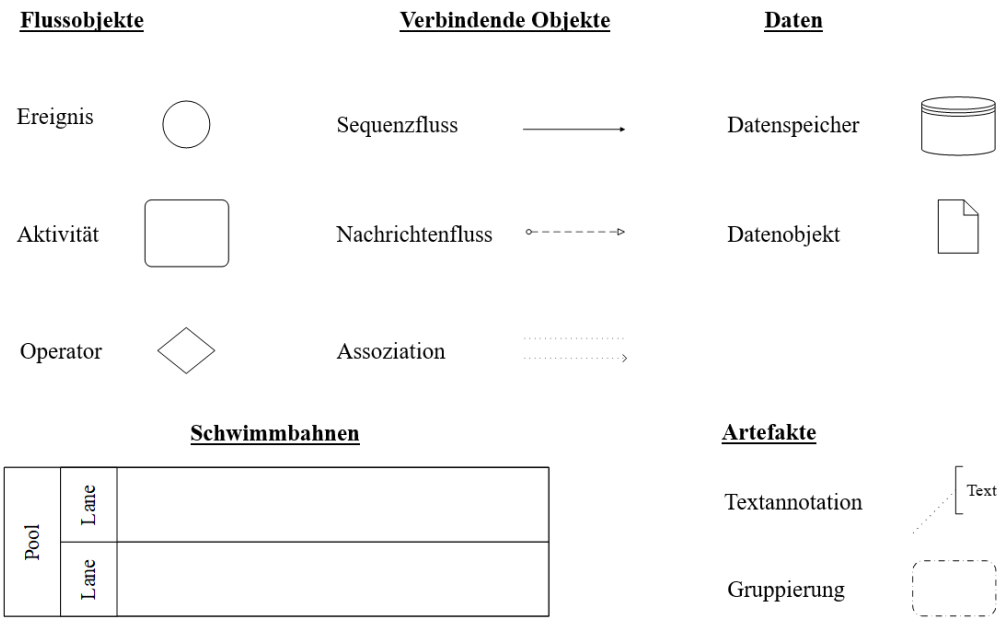


Abbildung 23: Basiselemente der BPMN

Die Flussobjekte (Flow Objects) enthalten mit Aktivitäten (Activities), Ereignissen (Events) und Operatoren (Gateways) die Grundbausteine eines Prozesses. Jede Aktivität beschreibt eine oder mehrere zusammengefasste Aufgaben des Prozesses. Durch eine textuelle Beschrei-

[342] WS-BPEL ist eine XML-basierte Sprache zur Beschreibung von Prozessen. Die Aktivitäten der Prozesse sind dabei in Form von Webservices anwendungsseitig implementiert. Spezielle BPEL-Engines erlauben die IT-gestützte Ausführung der in WS-BPEL beschriebenen Prozesse.
[343] Im Folgenden wird der Begriff BPMN Synonym für die Version 2.0 verwendet.
[344] Ursprünglich besaß die EPK keine Sprachdefinition der zugrundeliegenden Syntax und Semantik. Dies wurde erst in nachfolgenden Arbeiten versucht. Vgl. Werth 2008, S. 111 f.; Riehle et al. 2016, S. 70 f.
[345] Vgl. im Folgenden Object Management Group 2011; van der Aalst 2011, S. 42 ff.; Weske 2012, S. 208.

bung innerhalb des Aktivitätensymbols wird der Gegenstand der Aktivität verdeutlicht. Neben weiteren Spezialisierungen einer Aktivität ist eine Aufgabe (Task) als wesentliche Spezialisierung hervorzuheben. Sie umschreibt eine einzelne konkrete Aufgabe. Ereignisse beschreiben eingetretene Zustände. Im Gegensatz zu EPKs wechseln sich Funktionen und Ereignisse im BPMN Prozessfluss nicht zwingend gegenseitig ab. Auf eine Funktion kann z. B. direkt eine weitere Funktion folgen. Das trennen und zusammenführen des Kontrollflusses kann ebenfalls wie bei der EPK über Und, Inklusiv-Oder und Exklusiv-Oder Operatoren erfolgen. Artefakte (Artefacts) ermöglichen die Anreicherung des Prozesses mit Zusatzinformationen. Sie haben keinen Einfluss auf den Prozessablauf und können mit Flusselementen verbunden werden. Textannotationen dienen der Erläuterung von Sachverhalten. Gruppenartefakte ermöglichen die Kategorisierung von Elementen. Datenobjekte (Data Objects) stellen während des Prozesses benötigte (Data Inputs) oder erzeugte Daten (Data Outputs) dar. Es können sowohl digitale Dokumente als auch physische Gegenstände, wie z. B. Produkte, durch ein Datenobjekt repräsentiert werden. Mittels Datenspeichern (Data Stores) können zudem Speicherformen modelliert werden, die unabhängig von der Lebensdauer des Prozesses bestehen (z. B. ein Aktenschrank oder eine Datenbank).

Die Verbindungsobjekte verdeutlichen das Zusammenwirken aller Prozesselemente. Sequenzflüsse regeln die sach-logische Abfolge der Flussobjekte. Mittels einer Assoziation wird ein Artefakt mit den Flusselementen verbunden. Eine Assoziation mit Pfeilende weist auf die Flussrichtung hin. Nachrichtenflüsse regeln den Kommunikationsfluss zwischen allen Prozessbeteiligten. Mittels des Nachrichtensymbols (Message) werden die Inhalte der Kommunikation erfasst. Beteiligte werden jeweils mittels einer eigenen Schwimmbahn (Pool) dargestellt. Zur weiteren Differenzierung von Organisationsstrukturen können Pools in beliebig viele Bahnen (Lanes) unterteilt werden, um weitere Organisationseinheiten wie bspw. Abteilungen modellieren zu können.

Die BPMN Basiselemente werden durch weitere Elemente ergänzt, die eine Detaillierung der Flussobjekte erlauben. Ereignisse können als Start-, Zwischen- und Endereignis dargestellt werden, um zu verdeutlichen, wann sie den Sequenzfluss beeinflussen. Startereignisse können nur eine ausgehende Kante haben. Zwischenereignisse haben maximal eine eingehende und eine ausgehende Kante und Endereignisse nur eine eingehende Kante. Das Start- und manche Zwischenereignisse können mit einem „Auslöser“ wie z. B. einem Uhrzeiger- oder Briefsym-

bol angereichert werden, um zu verdeutlichen, was die genaue Ursache des Ereignisses (z. B. Eintritt eines bestimmten Zeitpunkts bzw. Eingang einer Nachricht) ist.
Aktivitäten und Aufgaben können mittels einer Markierung weiter spezifiziert werden. Abbildung 24 zeigt eine Auswahl möglicher Markierungen beider Elemente.[346] Aktivitäten werden mit einer Schleife versehen, wenn Aufgaben mehrfach hintereinander ausgeführt werden. Eine parallele Mehrfachausführung repräsentiert Aktivitäten, welche die gleichen Aufgaben mehrfach starten. Eine Aufgabe kann als Service markiert werden, wenn sie durch einen IT-gestützten Webservice durchgeführt wird. Eine Aufgabe wird als „manuelle Aufgabe“ markiert, wenn die Aufgabe nicht automatisiert, sondern von einer Person ausgeführt wird. Dies kann z. B. die visuelle Inspektion einer Warenlieferung hinsichtlich etwaiger Transportschäden sein.

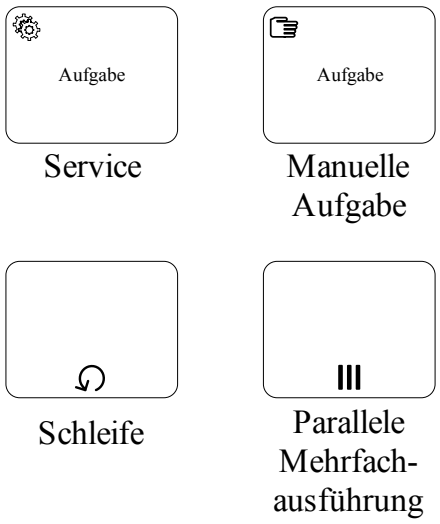


Abbildung 24: Beispiele für markierte Aufgaben und Aktivitäten.

Abbildung 25 veranschaulicht den in Abbildung 22 in EPK Notation modellierten Beispielprozess in BPMN Notation. Insbesondere werden die organisatorischen Verantwortlichkeiten für die einzelnen Prozessschritte deutlich. Weiterhin ist der nicht zwingende Wechsel zwischen Ereignissen und Funktionen, wie es bei der EPK vorgegeben ist, modelliert. Ebenso ist die klare Unterscheidung von manuellen und servicebasierten Aufgaben abgebildet.

[346] Für alle in der Spezifikation aufgeführten Markierungen vgl. Object Management Group 2011.

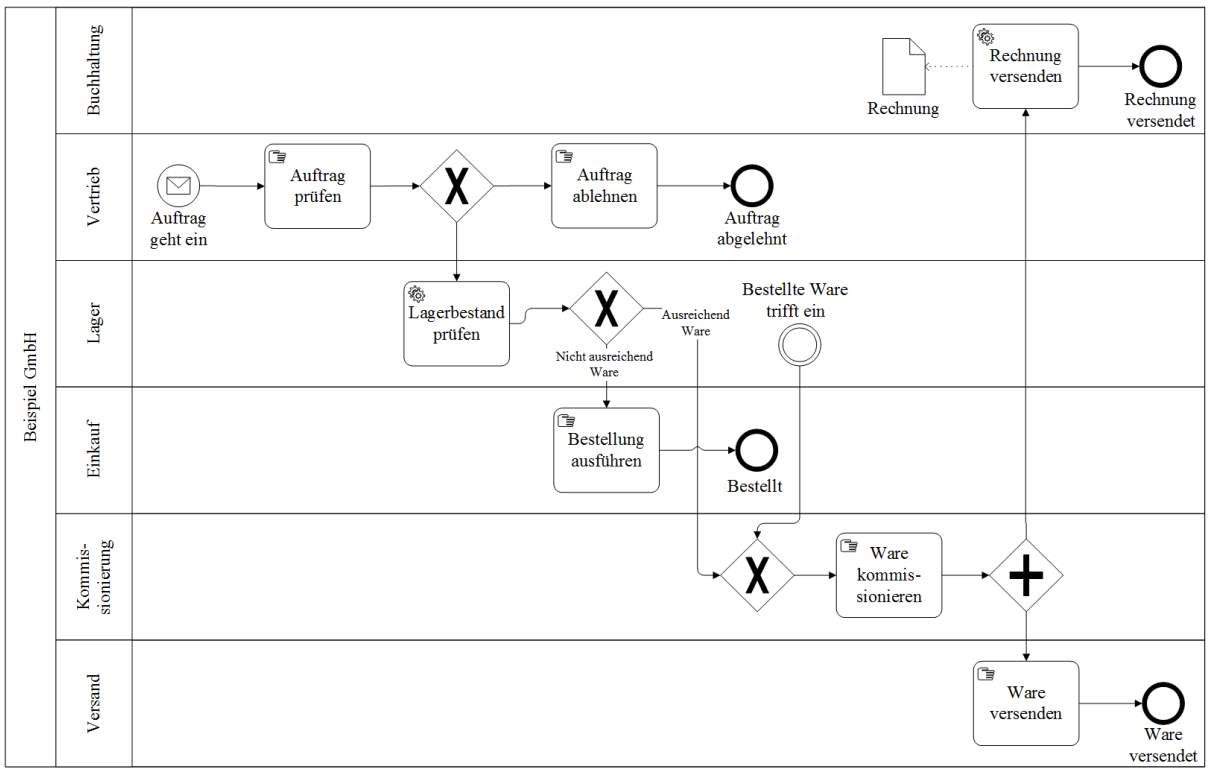


Abbildung 25: Beispiel der BPMN[347]

Neben den Prozessmodellen beschreibt die BPMN drei weitere Diagrammtypen zur Modellierung von Kollaborationen („Collaboration Diagram“), Choreographien („Choreography Diagram“) und Konversationen. Kollaborationen stellen die Interaktionen zwischen zwei Partnern mit jeweils eigenständigen Pools, die entsprechend eigene Prozessmodelle beinhalten, dar. Für den prozessübergreifenden Informationsaustausch kann zwischen den Pools über Nachrichtenflüsse eine Interaktion erfolgen. Sequenzflüsse dürfen nur innerhalb der Pools verwendet werden. So können Prozesskollaborationen zwischen zwei oder mehr Teilnehmern (z. B. Kunde und Lieferant) modelliert werden (siehe Abbildung 26). Choreographiediagramme dienen der Abbildung von Nachrichtenflüssen zwischen Partnern. Sie stellen die Reihenfolge des Nachrichtenaustausches dar, ohne auf die Details des Prozesses einzugehen.

[347] Vgl. Weske 2012, S. 165.

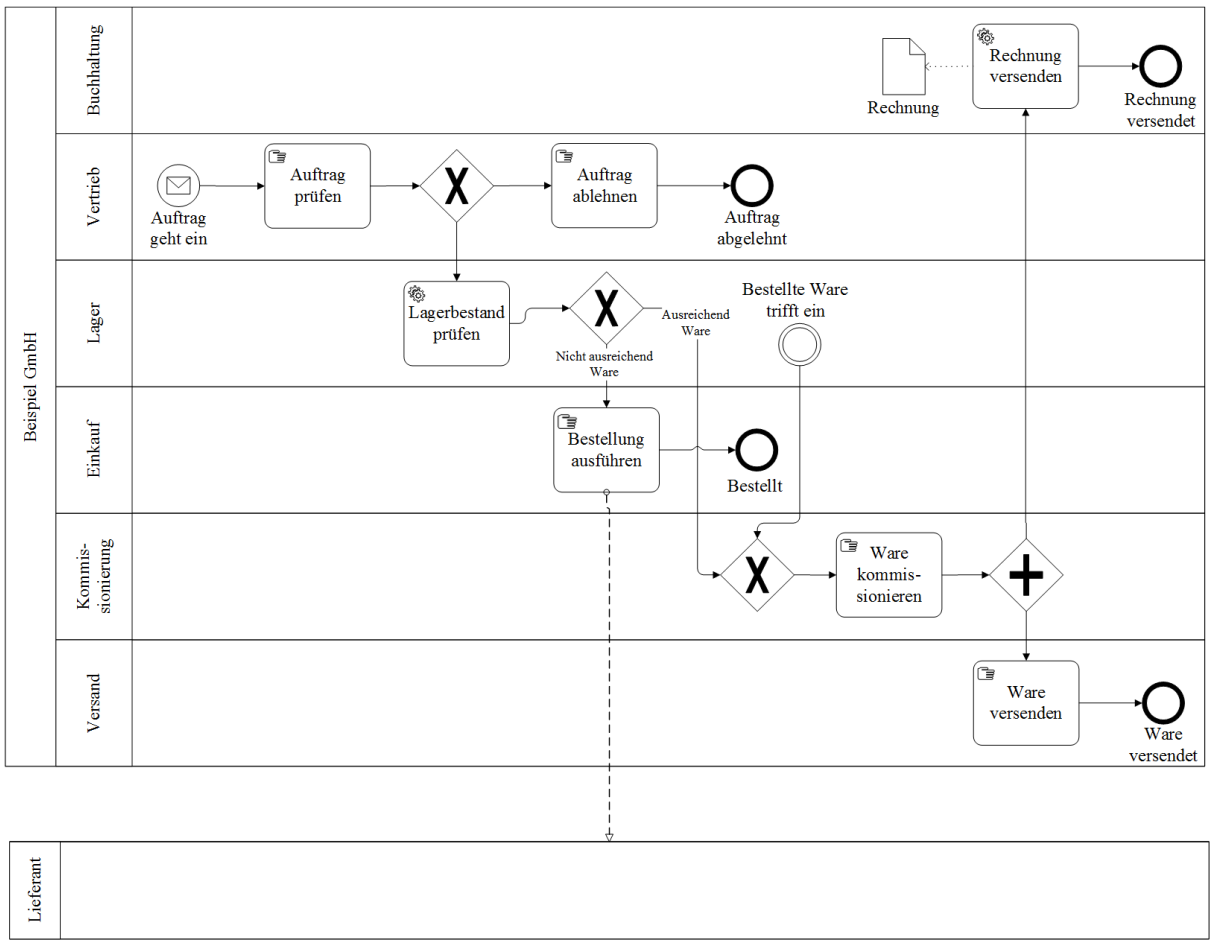


Abbildung 26: Beispiel einer BPMN Kollaborationsbeziehung

Die Choreographiediagramme dienen somit dem Überblick der Beziehungen zwischen Partnern in einem Prozess. Sie stellen eine spezielle Sicht auf Kollaborationsdiagramme dar. Wie die Aufgaben und die Zusammenarbeit unter Berücksichtigung von geschäftlichen, rechtlichen und technischen Anforderungen dann zu realisieren sind, wird detailliert mittels der Kollaborationsdiagramme modelliert.

Des Weiteren existieren in der BPMN Konversationsdiagramme, welche die reinen Kommunikationsbeziehungen zwischen Prozessbeteiligten visualisieren. Sie beschreiben den Nachrichtenaustausch zwischen den Prozessbeteiligten und stellen somit ebenfalls eine spezielle Sicht auf die Kollaborationsdiagramme dar.

Teil II: Risikomodellierung in Geschäftsprozessmodellen

6. Verbindung von Risiko- und Geschäftsprozessmanagement

6.1. Motivation

Risiko- und Prozessmanagement werden meist getrennt voneinander betrachtet, obwohl eine stärkere Verzahnung sinnvoll ist.[348] Einerseits folgt das Risikomanagement einem strukturierten Prozess, der die Aufgaben des Risikomanagements in einzelne Phasen unterteilt (siehe Kapitel 4), andererseits manifestieren sich die Unternehmensziele und somit auch die Risiken in den Geschäftsprozessen.[349] Letztere sind vielfach abteilungs- und unternehmensübergreifend und spiegeln das Zusammenspiel unterschiedlicher Akteure, Ressourcen und Funktionen wider, welche Risiken auslösen bzw. durch Risiken beeinflusst werden. Eine geschäftsprozessorientierte Sicht des Risikomanagements überwindet daher eine Risikobetrachtung, die sich nur auf einzelnen Fach- oder Funktionsbereiche beschränkt (Silo-Sicht), und findet somit ganzheitlich entlang der Wertschöpfungskette statt. Eine unternehmensweite Analyse der Risikosituation wird auf diese Weise erleichtert.[350] Gegen eine Integration der beiden Disziplinen kann angeführt werden, dass im Rahmen des kontinuierlichen Prozessmanagements bereits prozessweit analysiert wird, welche Schwachstellen und Risiken ein Prozess beinhaltet. Die Analyse beschränkt sich dabei allerdings auf den jeweiligen Prozess und zielt darauf ab, Zeit, Kosten und Qualitätsverbesserungen innerhalb des spezifischen Prozesses zu erreichen.[351] Ein ganzheitliches Risikomanagement steht hierbei jedoch nicht im Vordergrund. Im Rahmen einer unternehmensweiten Risikobetrachtung der Prozesse kann das Zusammenspiel der Risiken innerhalb der Prozesse und über Prozessgrenzen hinweg untersucht werden, um einem ganzheitlichen Ansatz gerecht zu werden, der unter anderem in regulatorischen Vorgaben gefordert wird.[352] Das COSO ERM Framework verweist in diesem Zusammenhang auf die notwendige Berücksichtigung der Geschäftsprozesse im Rahmen eines ganzheitlichen Risikomanagements.[353] Der IDW PS 340 verlangt die Risikoanalyse sämtlicher betrieblichen

[348] Vgl. Conforti et al. 2011, S. 100.
[349] Vgl. Berkau 2006, S. 159; Rikhardsson et al. 2006, S. 4 f.
[350] Vgl. Diederichs und Imhof 2011, S. 174 ff.
[351] Vgl. Rieke 2009, S. 101.
[352] Vgl. Rikhardsson et al. 2006, S. 10 f.
[353] Vgl. COSO ERM 2004, S. 19.

Prozesse.[354] Des Weiteren ist in IDW PS 381 die Analyse aller Unternehmensprozesse zum Zwecke der Prüfung des operativen Risikomanagementsystems vorgesehen.[355]

Die Verbindung von Risiko- und Prozessmanagement wird weiterhin als vorteilhaft angesehen, um Compliance- und Governancevorgaben zu erfüllen.[356] So können bspw. Risikosteuerungsmaßnahmen zur Verhinderung von Fehlern oder Missbrauch als Teil des Internen Kontrollsystems in die Geschäftsprozesse integriert werden.

Letztlich wird vielfach die Vorteilhaftigkeit der Verbindung beider Disziplinen für das Business Continuity Management (BCM) herausgestellt.[357] Dieses zielt insbesondere darauf ab, die Prozesse robuster gegen Erschütterungen während des Prozessdurchlaufs zu machen und so für unterbrechungsfreie Prozessdurchläufe zu sorgen. Eine risikoorientierte Betrachtung der Prozesse im Rahmen der Prozessdesignphase kann im Sinne des BCM helfen, Risiken, die den Prozessdurchlauf gegebenenfalls stören oder unterbrechen könnten, im Vorfeld zu antizipieren. Mögliche Störeinflüsse in Form externer Ereignisse, wie z. B. ein Unwetter oder das Marktgeschehen, können im Rahmen eines risikoorientierten Prozessdesigns bedacht werden, um einen reibungsloseren Prozessdurchlauf sicherzustellen.

Durch die Verbindung von Risiko- und Prozessmanagement ergeben sich somit diverse Vorteile. Damit diese genutzt werden können, muss eine Verbindung der Managementprozesse und der Methoden beider Disziplinen erfolgen.[358] In diesem Rahmen ist es insbesondere aus Sicht des Risikomanagements sinnvoll, wenn die Phasen des Risikomanagementprozesses sich an den Phasen des Prozessmanagements orientieren. Zur Verdeutlichung sei folgendes Beispiel angeführt:

Ein in einem Prozess identifiziertes Risiko müsste vernünftigerweise zunächst quantifiziert, beurteilt und dann mit Steuerungsmaßnahmen versehen werden, bevor der Prozess implementiert und ausgeführt wird. Nur auf diese Weise kann das Risiko von Beginn der Prozessdurchführung an gehandhabt werden. Eine alternative Orientierung der Schritte des Prozessmanagements an den Phasen des Risikomanagementprozesses wäre insbesondere aus Sicht der Risikosteuerung nicht sinnvoll, da Steuerungsmaßnahmen erst dann festgelegt würden, wenn der risikobehaftete Prozess bereits implementiert und ausgeführt wurde. Entsprechend sind die

[354] Vgl. Hampel et al. 2004, S. 116.
[355] Vgl. IDW 2017.
[356] Vgl. zur Muehlen und Rosemann 2005, S. 2; Karagiannis 2008, S. 1161 f.; Strecker et al. 2011, S. 598.
[357] Vgl. Jakoubi 2007, S. 1596; Asnar et al. 2008, S. 213; Taylor et al. 2008, S. 25; Betz 2011, S. 349.
[358] Vgl. Rieke 2009, S. 98 ff.

Phasen des Risikomanagements in den Prozessmanagementkreislauf zu integrieren, wodurch sich die nachfolgenden Vorteile ergeben.

6.2. Verbindung im Rahmen des Prozessdesigns

In der Prozessdesignphase werden die Prozessschritte, die benötigten Ressourcen und die jeweiligen Zusammenhänge, die zur Erreichung des Prozessziels beitragen, mithilfe von Prozessmodellen grafisch modelliert (siehe Kapitel 5.3). Die Orientierung an den in dieser Phase modellierten Geschäftsprozessen wird in der Literatur, insbesondere zur Unterstützung der Risikoidentifizierung, als sinnvoll angesehen.[359] Für die Prozessdesignphase und die Risikoidentifizierungsphase ergeben sich folgende Schnittstellen. Zunächst kann durch ein schrittweises Vorgehen entlang der modellierten Prozessabläufe sichergestellt werden, dass kein wesentlicher Prozessbestandteil bei der Risikoidentifizierung ausgelassen wird. Weiterhin können durch die Detailbetrachtung der Zusammenhänge aller involvierten Objekte, Ressourcen und Funktionen entlang des Prozessmodells potentielle Risiken erkannt und erfasst werden.[360] Dies gilt auch für mögliche Ursache-Wirkungs-Zusammenhänge und Risikointerdependenzen zwischen den identifizierten Risiken.[361] Nach erfolgter Analyse der Risikophänomene mithilfe der Prozessmodelle ist es sinnvoll, noch während der Prozessdesignphase die Modelle mit den identifizierten Risikoinformationen anzureichern und die Prozessdokumentation zu ergänzen.[362] Relevante und zu erfassende Informationen sind neben den Risiken zum einen die Verbindungen zu den Prozesselementen, auf welche die Risiken wirken bzw. welche die Risiken verursachen (Objekte, Ressource, Funktionen, Logikkonnektoren) und zum anderen die Verbindungen zu den Risiken, mit denen sie in einem Ursache-Wirkungsgefüge zusammenhängen oder mit denen sie korrelieren.

Weiteres Verbindungspotential ergibt sich zwischen den Phasen des Prozessdesigns und der Risikoquantifizierung sowie der Risikobeurteilung. Durch die Erfassung der Risiken im Prozessmodell bietet es sich an, diese auch hinsichtlich ihrer Wesentlichkeit für die unterschiedlichen Stakeholder unterscheidbar zu machen. Die bereits mit Risiken ergänzte Prozessdokumentation wird daher sinnvollerweise um Informationen aus der Phase der Risikoquantifizierung angereichert, so dass auch eine wertmäßige Beschreibung des jeweiligen Risikos erfolgt.

---

[359] Vgl. Wolf und Runzheimer 2008, S. 111; Diederichs 2012, S. 62 ff.
[360] Vgl. Brabänder und Ochs 2002, S. 19.
[361] Vgl. Hengmith 2005, S. 17.
[362] Vgl. Rieke und Winkelmann 2008, S. 348.

Dies empfiehlt sich nicht nur für die modellierten Risiken, sondern auch für die modellierten Risiko-Ursache-Wirkungsketten bzw. etwaige Korrelationen, die gegebenenfalls keinen kausalen Zusammenhang aufweisen. Auf dieser Basis kann für jegliche Risiken bzw. Risikozusammenhänge eine Beurteilung hinsichtlich der Wesentlichkeit erfolgen.[363] Als bedrohlicher beurteilte Risikophänomene könnten im Prozessmodell visuell (z. B. farblich) hervorgehoben werden, um sehr kritische Prozessbereiche von eher unkritischen auf einen Blick unterscheiden zu können.

Falls ein Risiko identifiziert wurde, kann im Rahmen der Verbindung zwischen Prozessdesign und Risikosteuerung der Prozess entweder noch während der Modellierung verändert werden, um z. B. das Risiko zu umgehen oder es können Risikosteuerungsmaßnahmen in den Prozess implementiert und den beurteilten Risiken zugewiesen werden, damit deutlich wird, welches Risiko wie behandelt wird.[364]

Im Ergebnis liefert die Verbindung von Prozessdesign und Risikomanagement durch die um Risikoinformationen angereicherten Geschäftsprozessmodelle einen ganzheitlichen Überblick über die Prozessrisiken, ihre Zusammenhänge, ihre Wesentlichkeit und zugewiesene Risikosteuerungsmaßnahmen. Auf diese Weise ist die Risikosituation für jeden Stakeholder anhand des mit Risiken angereicherten Prozessmodells nachvollziehbar.

[363] Für Methoden zur Quantifizierung und Beurteilung von Risiken siehe Kapitel 4.3.2 und 4.4.2.
[364] Für Methoden der Risikosteuerung siehe Kapitel 4.5.2.

Prozessmanagementphase	Verbindungspotential
Prozessdesign	*Risikoidentifizierung* • Detailbetrachtung der Zusammenhänge aller Prozesselemente zur Aufdeckung von Risiken sowie ihren Zusammenhängen • Risikodokumentation im Prozessmodell *Risikoquantifizierung* Erfassung der Ergebnisse der Quantifizierung (z. B. Risikomaße oder Wahrscheinlichkeitsverteilungen) von Einzelrisiken, Risiko-Ursache-Wirkungsketten und Korrellationen *Risikobeurteilung* Unterscheidung von Risiken gemäß Wesentlichkeit *Risikosteuerung* • Handhabung identifizierter Risiken während des Prozessdesigns durch Planung von Risikosteuerungsmaßnahmen • Visualisierung von Risikosteuerungsmaßnahmen und ihrer Zusammenhänge

Abbildung 27: Verbindungspotentiale mit dem Prozessdesign

6.3. Verbindung im Rahmen der Prozessimplementierung

Im Rahmen der Prozessimplementierung wird der Prozess in den Betrieb überführt. Damit die in der Prozessdesignphase charakterisierten Risikophänomene in den folgenden Phasen des Prozessmanagements berücksichtigt werden können, sind aus Sicht des Risikomanagements in dieser Phase die folgenden Schritte durchzuführen:

- Einrichtung der unterstützenden Informationssysteme
- Einrichtung der Business Rules mit Risikobezug
- Schulung und Sensibilisierung der Mitarbeiter

Im Rahmen einer erstmaligen Prozessimplementierung ist ein Risikomanagement-Informationssystem (RMIS) einzurichten, welches die Abbildung der Geschäftsprozesse und der im Prozessdesign ermittelten Risikophänomenen erlaubt. Weiterhin ist die Anbindung des RMIS an die für das Risikomanagement relevanten datenliefernden Informationssysteme herzustellen (z. B. ERP-Systeme).[365] Bei der generellen Implementierung neuer Prozesse sind im RMIS die Prozesse, ihre Risiken und die zugehörigen Datenquellen zu verknüpfen, damit die Aufgabenerfüllung des Risikomanagements während der Folgephasen der Prozessdurchführung, -überwachung und -evaluation durch das RMIS unterstützt werden kann.
Business Rules stellen Unternehmensleitlinien dar und geben eindeutige Regeln vor, wie (komplexe) Zusammenhänge zu handhaben sind. Business Rules mit Risikobezug sind im Rahmen der Risikoüberwachung und Risikosteuerung zu definieren. Ein Beispiel für eine Business Rule in diesem Kontext ist:

Wenn der Value at Risk des Risikos Absatzrückgang innerhalb eines Monats über 500.000 € steigt, dann alarmiere den Risk Owner.

Business Rules werden idealerweise in einem Informationssystem (Business Rule Management System) erfasst und verwaltet.
Letztlich sind die Mitarbeiter im Rahmen der Implementierung für das an den Prozessen orientierte Risikomanagement zu schulen und zu sensibilisieren. Dies umfasst nicht nur die Sensibilisierung für vorhandene Risiken, sondern auch für die Identifizierung neuer Risiken und die entsprechende Kommunikation risikomanagementrelevanter Sachverhalte in den Prozessen.

Prozessmanagementphase	**Verbindungspotential**
Prozessimplementierung	• Einrichtung der Informationssysteme • Definition und Implementierung der Business Rules mit Risikobezug • Schulung und Risikosensibilisierung der Mitarbeiter

Abbildung 28: Verbindungspotentiale mit der Prozessimplementierungsphase

[365] Vgl. im Folgenden Rieke 2009, S. 116.

6.4. Verbindung im Rahmen der Prozessdurchführung und -überwachung

Für die Phasen der Prozessdurchführung und -überwachung ergeben sich Verbindungspotentiale mit den Risikomanagementphasen der Risikoidentifizierung, der Risikosteuerung und der Risikoüberwachung. Im Rahmen der Risikoidentifizierung könnten während der Prozessdurchführung bisher unberücksichtigte Risiken in Echtzeit identifiziert und gesteuert werden, wobei die Realisierung einer solchen Echtzeitanalyse noch weiterem Forschungsbedarf unterliegt.[366] Bei der parallel zur Prozessdurchführung ablaufenden Prozessüberwachung werden die bei der Ausführung eines Prozesses erzeugten Daten, gegebenenfalls in Kennzahlen verdichtet, beobachtet. Neben den prozessrelevanten Daten könnten hierbei auch Daten mit Risikobezug betrachtet werden, die für die Risikoüberwachung relevant sind. Sie könnten zur Echtzeitbemessung und Überwachung der Risikomessgrößen (z. B. von Risikomaßen wie dem Value at Risk) genutzt werden. Dazu würden die Risikomessgrößen noch während der Prozessdurchführung auf (drohende) Überschreitungen ihrer Schwellenwerte überprüft.[367] Im Falle einer drohenden bzw. eingetretenen Überschreitung eines Schwellenwertes gilt das Risiko gegebenenfalls als bedrohlich bzw. schlagend geworden und es kann noch während der Prozessdurchführung eine Alarmierung des Risk Owners erfolgen, der dann die in der Risikosteuerung definierten Maßnahmen anzustoßen bzw. zu überwachen hat. Diese Überwachungsaktivitäten könnten nicht nur für prozessspezifische Risiken realisiert werden,[368] sondern auch für prozessübergreifende Wirkungsgefüge, indem alle aktiven Prozessinstanzen, zwischen deren Risiken Interdependenzen bestehen, in das Risikomanagement mit einbezogen werden.

---

[366] Vgl. für die folgenden Ausführungen Suriadi et al. 2014, S. 950 f.

[367] Welche Prozessdaten in welche Risikomessgrößen einfließen, muss in der Prozessimplementierungsphase festgelegt werden.

[368] Vgl. Rieke 2009, S. 117.

Prozessmanagementphase	Verbindungspotential
Prozessdurchführung und -überwachung	*Prozessbegleitende Risikoidentifizierung* Echtzeitidentifizierung von Risiken *Prozessbegleitende Risikoüberwachung* • Regelmäßige Bestimmung der Risikomessgrößen mittels Prozessdaten und Überwachung von (drohenden) Schwellenwertüberschreitungen • Benachrichtigung von Risk Ownern bei (drohendem) Risikoeintritt *Prozessbegleitende Risikosteuerung* Einleitung von Risikosteuerungsmaßnahmen bei Identifizierung bisher unbekannter Risiken und bei Risikoeintritt bereits bekannter Risiken

Abbildung 29: Verbindungspotentiale mit Prozessdurchführung und -überwachung

6.5. Verbindung im Rahmen der Prozessevaluation

Im Rahmen der Prozessevaluation werden die vergangenen Prozessverläufe untersucht und Verbesserungspotentiale für die Gestaltung der zukünftigen Prozessdurchführungen abgeleitet. Dabei können einerseits strukturelle Verbesserungen erarbeitet werden, welche ein anderes Design des Prozessverlaufs zur Folge haben oder aber funktionale Verbesserungen, welche auf einzelne Aktivitäten innerhalb des jeweiligen Prozesses abzielen und diese hinsichtlich bestimmter Zielgrößen wie z. B. die Durchlaufzeit optimieren. Verbindungspotentiale ergeben sich mit den Bereichen der Risikoidentifizierung (z. B. Ursachenanalyse schlagend gewordener Risiken), der Unterstützung der Risikoquantifizierung und -beurteilung (z. B. Messgrößenberechnung) sowie der Risikosteuerung (z. B. Überprüfung des Risikosteuerungsmaßnahmenerfolgs). Die Prozessevaluation nutzt gewöhnlicher Weise die Daten der prozessunterstützenden Informationssysteme, um die vergangenen Prozesse zu analysieren.[369] Dies sind einerseits Workflow-Management Systeme mit einer integrierten Überwachungskomponente und andererseits Process Mining Tools. Erstere verfügen über Informationen vergangener und aktueller Prozessinstanzen und können insbesondere Aussagen zu Leis-

[369] Vgl. im Folgenden Weske 2012, S. 15.

tungskennzahlen wie bspw. Durchlaufzeiten und Status von Prozessinstanzen geben. Letztere nutzen die Systemlogs der betrieblichen Informationssysteme, um die tatsächlichen Prozessverläufe zu rekonstruieren. Im Rahmen der Risikoidentifizierung während der Prozessevaluation können so unerwünschte Planabweichungen vom Prozessziel identifiziert werden. Dazu werden Soll-Ist-Vergleiche der Prozessverläufe durchgeführt, indem der Soll-Prozessverlauf mit dem tatsächlichen Ist-Prozessverlauf verglichen wird (sogenanntes Conformance-Checking).[370] Weitergehend ist denkbar, dass im Falle einer Planabweichung die Daten der vergangenen Prozessdurchführungen für eine Ursachenanalyse genutzt werden.[371] Dazu sind alle Prozessinstanzen mit ihren Daten (Attributen) in zwei Kategorien zu klassifizieren. Solche, die zu Planabweichungen führen und solche, die wie geplant verlaufen. Anschließend kann mittels Klassifikationsverfahren aus dem Bereich des Data Minings bestimmt werden, welche Kombination von Daten (Attributen) regelmäßig zu Planabweichungen führt. Diese Attribute korrelieren entsprechend hoch mit einem Risiko und können als Ursachen für das Risiko gelten. Sie sind daher anschließend näher zu überprüfen. Aus den historischen Daten der Prozessdurchführungen können im Rahmen der Prozessevaluation Informationen gezogen werden, die dazu dienen die Risikoquantifizierung und die Risikobeurteilung zu verbessern. Zum Beispiel können für einen bestimmten Zeitraum die Eintrittswahrscheinlichkeiten und das Schadensausmaß schlagend gewordener Risiken aus den Daten bestimmt werden. Sofern ausreichend Daten vorliegen, ließe sich auch die Verteilungsfunktion bestimmen. Auf Basis dieser neuen Informationslage ließen sich dann die bestehende Quantifizierung und die Risikobeurteilung aktualisieren. Letztlich ergeben sich Schnittstellen zwischen Prozessevaluation und Risikokontrolle, indem in dieser Phase der Maßnahmenerfolg überprüft wird und die Erkenntnisse gegebenenfalls für eine Verbesserung der Risikosteuerung genutzt werden.

[370] Vgl. van der Aalst 2011, S. 191 f.
[371] Vgl. Suriadi et al. 2014, S. 951.

Prozessmanagementphase	Verbindungspotential
Prozessevaluation	*Risikoidentifizierung* • Ex-post Analyse von Prozessdaten zur Ermittlung von eingetretenen Risiken (Planabweichungen) • Bestimmung von Ursachen häufig eingetretener Risiken mittels Data Mining (Klassifikationsverfahren) *Risikoquantifizierung* Ermittlung von Eintrittswahrscheinlichkeit und Schadensausmaß (der Verteilung) eines Risikos auf Basis der historischen Prozessdaten *Risikobeurteilung* Datenbasierte Überprüfung der ursprünglichen Risikobeurteilung und ggf. Anpassung *Risikokontrolle* Datenbasierte Prüfung, ob eingeleitete Risikosteuerungsmaßnahmen zu gewünschter Entwicklung geführt haben

Abbildung 30: Verbindungspotentiale mit der Prozessevaluation

7. Entwicklung einer risikoorientierten Prozessnotation

7.1. Motivation

Zur Realisierung der Verbindung von Risiko- und Geschäftsprozessmanagement bietet sich neben der Verbindung der Managementprozesse eine Verbindung der Methoden an.[372] Aus diesem Grund soll im Folgenden die Geschäftsprozessmodellierung, welche die Basis des Prozessmanagements darstellt,[373] um eine Risikosicht erweitert werden. Die Prozessnotation soll zu einer risikoorientierten Prozessnotation (ROPN) weiterentwickelt werden, auf deren Basis sich möglichst viele der identifizierten Verbindungspotentiale nutzen lassen. Dazu sind Anforderungen an die Notation aus den im vorherigen Kapitel erarbeiteten Schnittstellen zwischen den beiden Managementdisziplinen zu formulieren.

7.2. Anforderungen aus Sicht eines risikoorientierten Prozessdesigns

Die im Prozessdesign zu erfüllenden Anforderungen an die Notation lassen sich aus den Phasen der Risikoidentifizierung, der Risikoquantifizierung, der Risikobeurteilung und der Risikosteuerung ableiten, zu denen im Prozessdesign Schnittstellen bestehen (siehe Kapitel 6.2).

Risikoidentifizierung

Im Rahmen der Risikoidentifizierung werden die Prozessrisiken identifiziert und zu Dokumentationszwecken mit ihren Charakteristika erfasst (siehe Kapitel 4.2). Die Prozessrisiken lassen sich dazu sowohl Top-Down aus den Prozesszielen ableiten als auch Bottom-Up anhand der bereits modellierten Prozesse.[374] Ein Prozess kann grundsätzlich ein oder mehrere Ziele verfolgen, deren Erreichung durch die Prozessaktivitäten unterstützt wird.[375] Die Aktivitäten (Funktionen) werden unter Einsatz von Ressourcen (z. B. Maschinen oder Personen) durchgeführt und benötigen bzw. erzeugen ggf. Daten. Die Aktivitäten und Ressourcen unterliegen dabei diversen Risiken, deren Eintritt die Prozessziele beeinflussen kann. Die Relevanz jedes Risikos hängt von den verfolgten Prozesszielen ab. Ist bspw. eine schnelle Prozessdurchführung das einzige definierte Ziel eines Prozesses, so ist ein Risiko, welches eine Verzögerung des Prozessdurchlaufs erzeugt, als relevanter einzustufen als ein Qualitätsrisiko.

---

[372] Vgl. Sienou et al. 2007, S. 120.
[373] Vgl. Deiters 1997, S. 54; Rump 1999, S. 12; Buchanan und McMenemy 2012, S. 252 ff.
[374] Vgl. Rieke 2009, S. 115.
[375] Vgl. im Folgenden zur Muehlen und Rosemann 2005.

Entsprechend sind die festgelegten Prozessziele ausschlaggebend, da von ihnen abhängt, welche Risiken zu modellieren sind. Die Berücksichtigung der Prozessziele im risikoorientierten Prozessmodell stellt somit eine erste Anforderung dar.

Aufgrund der möglichen Komplexität der Risikophänomene wird in der Literatur vereinzelt vorgeschlagen, unterschiedliche Modelle für die Beschreibung der Risikolage in Prozessen zu erzeugen. Zur Muehlen und Rosemann (2005) schlagen z. B. die separate Erzeugung von vier Modellen vor, welche die Risikostruktur (Risk Structure Model), die Verbindung zwischen Risiken und Zielen (Risk Goal Model), die kausalen Abhängigkeiten und Eintrittswahrscheinlichkeiten der Risiken (Risk State Model) sowie die Verbindungen zwischen Risiken und Prozesselementen (Event-driven Process Chain with Risks) vorsehen. Diese Vorgehensweise führt allerdings dazu, dass bei der alleinigen Betrachtung des risikoorientierten Prozessmodells die Risikozusammenhänge und die Relevanz der einzelnen Risiken nicht erkennbar sind. Dadurch wird den Stakeholdern ein erhöhter Analyseaufwand und ein erhöhtes Expertenwissen abverlangt, um die Risikosituation eines Prozesses nachzuvollziehen. Sinnvoller erscheint eine Abbildung der Risiken und ihrer Zusammenhänge in einem Modell. Dazu sind die identifizierten Risiken mittels eines eigenen Symbols im Prozessmodell darzustellen und die jeweiligen Risikocharakteristika (wie z. B. die Risikobezeichnung, die Risikokategorie, die betroffenen Prozessziele, die Risk Owner, etc.) dem Risikoelement per Annotation oder per Attribut zuzuweisen.[376] Neben Einzelrisiken liegen idealerweise Kenntnisse über Risiko-Ursache-Wirkungsketten (RUWK) und Risikokorrelationen vor (siehe Kapitel 4.2), die im Sinne der Vollständigkeit ebenfalls modelliert werden sollten. Im Falle von RUWK kann die Überlegung angestellt werden, sowohl Risikoursachen als auch Risikowirkungen im Prozessmodell zu unterscheiden und separat zu modellieren. Dies erscheint jedoch nicht sinnvoll, da ein Risiko in einer RUWK zugleich Ursache und Wirkung zweier unterschiedlicher Risiken sein kann. Zur Erläuterung sei folgendes Beispiel aufgeführt:

Es existiere eine aus drei Risiken R_1, R_2 und R_3 bestehende RUWK $R_1 \rightarrow R_2 \rightarrow R_3$. Das Risiko R_2 ist zugleich Wirkung von Risiko R_1und Ursache von Risiko R_3. Würde im Rahmen der Modellierung eine Unterscheidung von Ursache und Wirkung vorgenommen werden, müsste R_2 zweimal modelliert werden. Dies würde zu Redundanzen führen und bei mehreren

[376] Vgl. Brabänder und Ochs 2002, S. 23 f.; zur Muehlen und Rosemann 2005; Weiß und Winkelmann 2011, S. 5.

RUWK entsprechend unübersichtlich werden, wodurch der abstrahierende Charakter des Prozessmodells verloren gehen würde. Die Struktur einer RUWK lässt sich eleganter über die verbindenden Kanten zwischen den Risiken darstellen. Entsprechend sollte ein einziges Risikoelement zur Modellierung jeglicher Art von Risiko Bestandteil einer risikoorientierten Prozessmodellierung sein. Dadurch lässt sich die Risikosituation des Prozesses im Prozessmodell deutlich visualisieren. Für den Fall, dass viele Risiken identifiziert werden und das risikoorientierte Prozessmodell unübersichtlich wird, kann die DV-technische Darstellung der Prozessrisiken für mehr Übersichtlichkeit sorgen.[377] Hierzu können bspw. zusammenhängende Risiken aggregiert dargestellt werden oder nur hoch priorisierte Risiken visualisiert werden.
Damit die Zusammenhänge der Risikophänomene deutlich werden, muss ein Risikoelement mit den Prozesselementen auf die es Einfluss nehmen kann, wie Flussobjekte (z. B. Funktionen und Logikkonnektoren), verbindende Objekte (z. B. Sequenz- und Nachrichtenflüsse) und Ressourcen (z. B. Maschinen, Personen oder Daten) verknüpft werden können. Ebenso sollten die Risiken untereinander über Kanten verbunden werden können, um RUWKs und ihre kausalen Abfolgen abbilden zu können. So werden die Risikozusammenhänge für alle Stakeholder direkt im Prozessmodell nachvollziehbar. Dabei sollten die Kanten selbst bereits Informationen über die Art des Zusammenhangs liefern,[378] da Risiken sich gegenseitig verstärken, abschwächen oder die Wahrscheinlichkeit ihres Eintritts beeinflussen können (siehe Kapitel 4.3). In diesem Kontext ist zu berücksichtigen, dass ein Risiko zu einem oder mehreren Risiken eine kausale Verbindung besitzen kann. Entsprechend sollten die Kanten mit logischen Konnektoren (Und, Oder, Exklusiv-Oder) verknüpft werden können, damit sich Risikozusammenhänge eindeutig modellieren lassen. Weiterhin sollten bekannte Korrelationen zwischen Risiken, bei denen kein kausaler Zusammenhang nachgewiesen werden kann, in einer ROPN berücksichtigt werden. Dies kann ebenfalls über spezifische Kanten zwischen den korrelierenden Risiken oder über eine Attribuierung der Risiken erfolgen. Die Art des Zusammenhangs (positive / negative Korrelation) und der Grad der Korrelation sollten ebenso dargestellt werden können.

[377] Vgl. Hengmith 2005, S. 22.
[378] Vgl. Hengmith 2005, S. 22; Sienou et al. 2009, S. 176 f.; Strecker et al. 2011, S. 604.

Risikoquantifizierung

Zur Integration der Ergebnisse der Risikoquantifizierung in das risikoorientierte Prozessmodell (ROPM) sollte es möglich sein, die Ergebnisse der Quantifizierung (wie z. B. die Eintrittswahrscheinlichkeit, das Schadensausmaß bzw. die Verteilungsfunktion und Risikomaße) im ROPM zu vermerken.[379] Dies ist insbesondere sinnvoll, wenn die Quantifizierung und die Beurteilung der Risiken von unterschiedlichen Stakeholdern vorgenommen werden.

Risikobeurteilung

Die festgelegten Schwellenwerte, ab denen ein Risiko bzw. das Gesamtrisiko einer RUWK als wesentlich beurteilt wird, sind im ROPM zu erfassen, damit die Risikobeurteilung für jeden Betrachter nachvollziehbar ist. Die Möglichkeit einer zusätzlichen Erfassung von Anmerkungen zur Beurteilung erscheint sinnvoll, da jedes Individuum einem Bezugsobjekt einen anderen Wert beimisst und auf diese Weise die Beurteilung nachvollziehbarer wird. Zur Visualisierung der Ergebnisse der Risikobeurteilung kann es hilfreich sein, die beurteilten Risiken und RUWK im Prozessmodell in Abhängigkeit ihrer Wesentlichkeit visuell zu unterscheiden.

Risikosteuerung

Die im Rahmen der Risikosteuerung festgelegten Risikosteuerungsmaßnahmen sind sinnvoller Weise im ROPM abzubilden.[380] Damit sie von üblichen Prozessfunktionen unterschieden werden können, sollten sie durch ein eigenes Element repräsentiert werden. Zur eindeutigen Unterscheidung der Maßnahmen untereinander und zur Nachvollziehbarkeit ihrer (erwarteten) Wirkungen, sollten die wesentlichen Charakteristika im ROPM festgehalten werden. Dazu sind neben einer eindeutigen Bezeichnung insbesondere die Maßnahmenstrategie bzw. die erwarteten (quantifizierten) Wirkungen und der für die Durchführung der Maßnahme Verantwortliche zu erfassen. Maßnahmen können einerseits auf die Risikoeintrittswahrscheinlichkeit und das Risikoausmaß der behandelten Risiken wirken. Sie können andererseits aber auch Einfluss auf Prozessaktivitäten haben. Dies muss durch entsprechende Verknüpfungsmöglichkeiten in der Modellierung berücksichtigt werden können. Die Verbindungen zwischen

[379] Vgl. Hengmith 2005, S. 22; Strecker et al. 2011, S. 598.
[380] Vgl. zur Muehlen und Rosemann 2005, S. 9; Sienou et al. 2009, S. 176; Weiß und Winkelmann 2011, S. 5.

Maßnahmen und Prozess- bzw. Risikoelementen werden zur Komplexitätsreduktion idealerweise mit den gleichen Symbolen modelliert, die bereits zur Verknüpfung von Risiko- und Prozesselementen genutzt werden. Eine Maßnahme wird entweder durch den Eintritt eines bestimmten Zustandes (Risikoschwellenwert) oder durch das Erreichen eines bestimmten Zeitpunkts gestartet bzw. beendet. Für den Fall, dass der Maßnahmenstart oder das Maßnahmenende von mehreren Bedingungen abhängig ist, müssen beliebig viele Zustände sowie dazugehörige Bedingungen definiert werden können.

Prozessmanagementphase	**Anforderungen**
Prozessdesign	*Risikoidentifizierung und -erfassung* • Erfassung der Prozessziele • Modellierung von Einzelrisiken mittels eines Risikosymbols • Erfassung von Risikocharakteristika (wie z. B. Risikobezeichnung, -art, betroffene Ziele, Risk Owner) per Annotation oder Attribut • Abbildung von Risiko-Ursache-Wirkungs-Beziehungen bzw. -ketten • Kanten zur Verbindung von Risiken mit Prozesselemente und anderen Risiken; Kanten spezifizieren die Art des Zusammenhangs • Logikkonnektoren (Und, Oder, Exklusiv-Oder) zwischen den Kanten zur Darstellung komplexer Zusammenhänge zwischen Risiken • Darstellung von Korrelationen zwischen Risiken • Erfassung der Art des Zusammenhangs und des Grades der Korrelation

Prozessmanagementphase	Anforderungen
	Risikoquantifizierung Annotation oder Attribuierung der Risiken bzw. verbindender Kanten und der RUWK mit den Ergebnissen der Quantifizierung (Eintrittswahrscheinlichkeit, Schadensausmaß, bzw. Verteilungsfunktion, Risikomaße) *Risikobeurteilung* • Als Ergebnis der Risikobeurteilung ist die Wesentlichkeitsgrenze für jedes Risiko in Form eines Schwellenwertes zu erfassen • Visuelle Unterscheidung der Risiken anhand des Grades der Wesentlichkeit (optional) • Begründung zur Wahl der Wesentlichkeitsgrenze (optional) *Risikosteuerung* • Modellierung von Risikosteuerungsmaßnahmen • Erfassung der wesentlichen Maßnahmencharakteristika (z. B. Bezeichnung, Maßnahmenart, quantifizierte Wirkungen, Verantwortlichkeit) • Kanten zur Verbindung von Maßnahmen mit Prozess- und Risikoelementen • Festlegung eines Zeitpunkts oder eines Risikoschwellenwerts zur Einleitung des Maßnahmenstarts und -endes für jedes Risiko, das durch die Maßnahme gesteuert werden soll • Festlegung komplexer Regeldefinitionen für die Aktivierung und Beendigung von Maßnahmen, die sich auf mehrere Risiken beziehen bzw. von Bedingungskombinationen abhängen

Abbildung 31: Anforderungen an ein risikoorientiertes Prozessdesign

7.3. Anforderungen aus Sicht einer risikoorientierten Prozessimplementierung, -durchführung, -überwachung und -evaluation

Die Anforderungen an die Notation, die sich aus den Phasen der Prozessimplementierung, Prozessdurchführung, Prozessüberwachung und Prozessevaluation ergeben (siehe Kapitel 6.3 ff.), können zusammengefasst werden, da sie sich alle auf die Erfassung und Verarbeitung risikorelevanter Daten beschränken. In den genannten Phasen werden risiko- und prozessbezogene Daten benötigt (z. B. die Eintrittswahrscheinlichkeit eines Prozessrisikos), die in den Informationssystemen, die das Prozess- und das Risikomanagement unterstützen, verarbeitet und vorgehalten werden. Idealerweise basiert das ROPM auf einer Prozessnotation, die eine maschinenlesbare Beschreibung von Prozessabläufen und somit eine informationstechnische Unterstützung durch ein Risikomanagement-Informationssystem (RMIS) ermöglicht. Die Daten aus anderen betrieblichen Informationssystemen können dann über Attribute den Elementen des risikoorientierten Prozessmodells zugewiesen werden. Damit die Aktualität der Daten sichergestellt ist, ist das unterstützende RMIS mit den betrieblichen Informationssystemen zu verbinden.[381] So können Prozessmodelle in ein RMIS mit entsprechender Funktionalität importiert oder in diesem modelliert werden. Die benötigten Attribute der Risikoelemente des ROPM wurden in den Anforderungen an das risikoorientierte Prozessdesign aufgeführt (siehe Kapitel 7.2).

Prozessmanagementphase	Anforderungen
Prozessimplementierung, -durchführung, -überwachung und -evaluation	• Verwendung einer maschinenlesbaren Notation zur informationstechnischen Unterstützung • Hinterlegung der im Prozessdesign aufgeführten Charakteristika in der Prozessmodellbasis (Attribution) für alle Elemente mit Risikobezug. Für Risiken sind dies z. B. die Risikobezeichnung, der Risk Owner, Verteilungsinformationen und der Risikoschwellenwert.

Abbildung 32: Anforderungen an risikoorientierte Prozessimplementierung, -durchführung, -überwachung und -evaluation

[381] Vgl. Rieke 2009, S. 119.

7.4. Bestehende Ansätze

Suriadi et al. (2014) geben einen umfassenden Überblick über die bestehende Literatur zur Verknüpfung des Risikomanagements mit dem Prozessmanagement. Sie identifizieren insgesamt 27 Ansätze für ein risikoorientiertes Geschäftsprozessmanagement, welche sie in drei Gruppen kategorisieren. Dabei unterscheiden sie Ansätze, welche die Prozessdesignphase (Design Stage), die Prozessdurchführungsphase (Run-Time Stage) und die Prozessevaluationsphase (Post-Execution Stage) unterstützen. Aufbauend auf diesem Überblick wurden mittels Literaturrecherche 13 weitere Quellen zum risikoorientierten Prozessmanagement gefunden (siehe Abbildung 33).[382] Nahezu die Hälfte aller Ansätze basiert auf Standardprozessnotationen wie der EPK oder der BPMN. Die weiteren Ansätze sind mehrheitlich generisch beschrieben oder basieren vereinzelt auf proprietären (z. B. PowerDesigner) bzw. domänenspezifischen (z. B. SBPML für den Bankensektor) Notationen.

Ansätze zur Unterstützung der Prozessdesignphase

Die überwiegende Anzahl der Ansätze unterstützt die Prozessdesignphase und fokussiert sich auf die risikoorientierte Gestaltung von Geschäftsprozessen oder die Anreicherung der Prozessmodelle mit Risikoinformationen. Bai et al. (2006), Bergholtz et al. (2005), Bhuiyan et al. (2007), Fenz et al. (2010, 2009, 2008) und zur Muehlen et al. (2006) stellen jeweils Ansätze vor, die ein risikoorientiertes Prozessdesign unterstützen. Bhuiyan et al. bspw. untersuchen dazu strategische Abhängigkeiten zwischen Akteuren einer Organisation und identifizieren so die Aktivitäten, die einem erhöhten Risiko ausgesetzt sind. Dabei unterstellen sie, dass Aktivitäten, die auf mehrere Akteure verteilt sind, ein geringeres Risiko zu scheitern aufweisen als Aktivitäten, die von weniger bzw. nur einem Akteur ausgeführt werden. Für den Fall des Scheiterns der Aktivität modellieren sie entsprechende Ausweichprozesse auf Basis der Analyse der kritischen Aktivitäten. Dabei verwenden sie die Standardprozesselemente der BPMN. Fenz et al. stellen eine Reihe an Methoden vor, um das unternehmensweite Risikoniveau zu ermitteln. Dazu analysieren sie die Risiken der in den Prozessen involvierten IT Ressourcen und schließen daraus auf das allgemeine Prozessrisiko. Betz et al. (2011), Taylor et al. (2008) und Jallow et al. (2007) nutzen Simulationsverfahren, um zu analysieren, inwiefern Prozesse risikobehaftet sind und verbessert werden können.

[382] Fünf der 13 zusätzlich identifizierten Ansätze wurden bereits in Anton et al. 2016, S. 49 untersucht.

	Autor/en	Prozessdesignphase	Prozessdurchführungsphase	Evaluationsphase	Notation
1.	Ahmed/Altuhova (2014)	x	(x)		BPMN 2.0
3.	Asnar/Giogini (2008)	x			Generisch
4.	Bai et al. (2007)	(x)			Generisch
5.	Bergholtz (2005)	(x)			BMO
6.	Bernasconi (2013)	x	(x)		BPMN 2.0
7.	Betz et al. (2011)	x			XML Netze
8.	Bhuiyan (2007)	x	(x)		BPMN 1.x
9.	Brabänder (2002)	x			EPK
10.	Conforti (2013)	(x)	x		BPMN 2.0
11.	Cope (2010)	x			BPMN 1.1
12.	Diederichs/Imhof (2011)	x			EPK
13.	Fenz (2010)	(x)			Generisch
14.	Hengmith (2005)	x			EPK
15.	Herrmann (2006)	x			UML
16.	Jakoubi (2007)	x			Generisch
17.	Jallow (2007)	x			Generisch
18.	Jans (2011)			x	Generisch
19.	Kaegi (2006)	(x)			BPMN 1.x
20.	Kang (2009)		x	x	Generisch
21.	Karagiannis (2007)	x			ADONIS
22.	Lambert (2006)	x			IDEF

	Autor/en	Prozessdesignphase	Prozessdurchführungsphase	Evaluationsphase	Notation
23.	Marcinkowski (2012)	x			BPMN 2.0
24.	Meland (2012)	x			BPMN 2.0
25.	Mock (2005)	x			EPK
26.	Muehlen (2006)	(x)			-
27.	Panayiotou (2010)	(x)			PowerDesigner
28.	Pittl (2017)	x			SWRL
29.	Rieke (2007)	x			EPK
30.	Rieke/Winkelmann (2008)	x			EPK
31.	Rosemann / zur Muehlen (2005)	x			EPK
32.	Rotaru (2009)	(x)			EPK
33.	Sadiq (2007)	x			Generisch
34.	Sienou (2007)	x			EPK
35.	Singh (2008)	(x)			-
36.	Strecker (2011)	x			MEMO
37.	Taylor (2008)	x			jBPM/JPDL
38.	Vaca (2011)	x			BPMN 1.x
39.	Weiß (2011)	x			SBPML
40.	Wickboldt (2011)			x	Generisch

Abbildung 33: Bestehende Ansätze für risikoorientiertes Geschäftsprozessmanagement

Die Anreicherung der Prozessmodelle um Risikoaspekte sieht die Mehrheit der Ansätze vor. Eine Gruppe dieser Ansätze ermöglicht dabei im Wesentlichen nur die Modellierung von Risiken und Risikosteuerungsmaßnahmen. So beschränken sich Lambert et al. (2006) auf die Risikoidentifizierung und -erfassung. Ihr Ansatz ermöglicht lediglich den Namen identifizierter Risiken per Annotation einer Prozessaktivität im Prozessmodell zuzuweisen ohne die Risiken weiter zu spezifizieren. Rotaru et al. (2009) modellieren von den Prozesszielen ausgehend, welche Risiken auftreten können und minimiert werden sollen. Diese Risikominimierungsziele werden dazu neben dem Prozessmodell abgebildet und mit den Prozessfunktionen, welche das jeweilige Ziel fördern, über eine ungerichtete Kante verbunden. Komplexere Risikozusammenhänge und zusätzliche Risikoinformationen werden in dem Ansatz nicht berücksichtigt. Ahmed und Altuhova (2014) modellieren Risiken sowie Risikosteuerungsmaßnahmen im Prozessmodell mittels des Aufgabensymbols aus dem BPMN 2.0 Standard und färben dieses zur Unterscheidung ein. Dabei steht Rot für ein Risiko und Blau für eine Maßnahme. Darüber hinaus annotieren sie die risikobehafteten Prozesselemente und umschreiben das Risiko mithilfe des ebenfalls im Standard vorhandenen Elements der Text-Annotation direkt im Modell. Da ihre Methode auf die Unterstützung des Managements der Informationssicherheit abzielt, führen sie des Weiteren spezifische Symbole zur Annotation von IT- und Datenressourcen in die BPMN 2.0 ein. Der Ansatz ist jedoch flexibel genug, um auch im Rahmen des allgemeinen Risikomanagements genutzt werden zu können. Weitergehende Aspekte des Risikomanagements, wie z. B. eine detaillierte Erfassung notwendiger Risikocharakteristika und die Abbildung von Risiko-Ursache-Wirkungsketten sind nicht realisierbar.

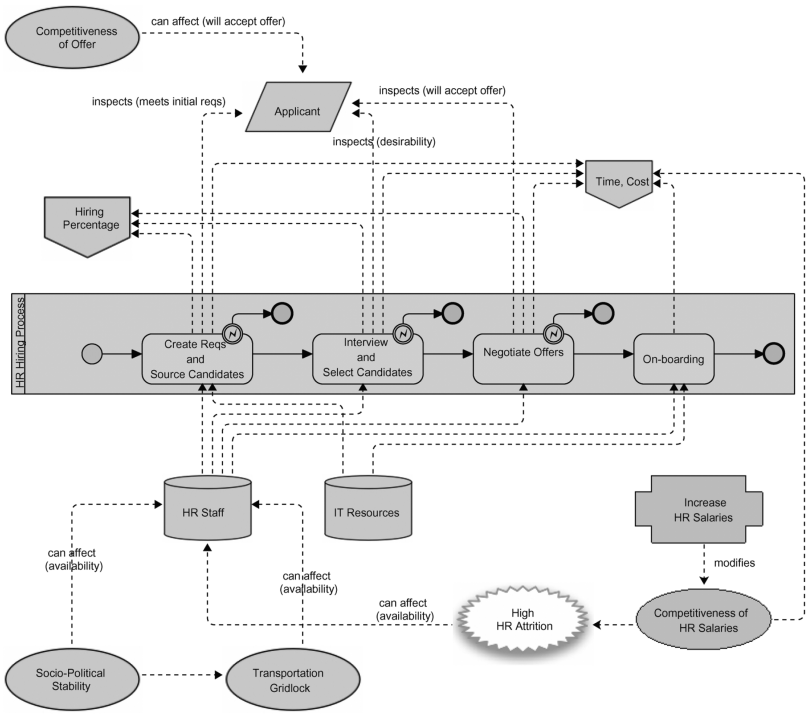


Abbildung 34: Risikoorientiertes Prozessmodell nach Cope et al.[383]

Cope et al. (2010) hingegen stellen einen Ansatz vor, der neben der Abbildung von Risiken und Steuerungsmaßnahmen auch die Modellierung kausaler Zusammenhänge zwischen den Risikophänomenen im Prozessmodell erlaubt (siehe Abbildung 34). Die Abbildung logischer Verknüpfungen ist jedoch nicht möglich, so dass nur sequentielle kausale Abhängigkeiten zwischen den Risiken modellierbar sind. Aspekte der Risikoquantifizierung und -beurteilung werden von Cope et al. nicht berücksichtigt. Sadiq et al. (2007) implementieren Symbole für Kontrollen und Maßnahmen im Prozessmodell als Teil des Internen Kontrollsystems. Den Kontrollen werden Bedingungen zugewiesen, anhand welcher Verstöße (Risiken) in den Prozessaktivitäten überwacht werden. Die Risiken werden hierbei implizit durch die Integration der Kontrollen mitmodelliert. Jeder Kontrolle können weiterhin eine oder mehrere Maßnahmen zugewiesen werden, die bei Erfüllung der Bedingungen entsprechend ausgelöst werden. Im Beispiel von Sadiq et al. sind dies im Kontext des Internen Kontrollsystems bspw. die Benachrichtigung verantwortlicher Personen oder die Einleitung von Ermahnungen. Aufgrund der Fokussierung auf die Interne Kontrolle sind die Maßnahmen nur reaktiv modellierbar und

[383] Entnommen aus Cope et al. 2010, S. 4:8.

der Ansatz daher für das Risikomanagement nicht geeignet. Ebenso entwickeln Panayiotou et al. (2010) eine BPMN Erweiterung für das Interne Kontrollsystem. Im Prozessmodell verknüpfen sie die Aktivitäten mit Kontrollelementen, welche die Kontrollen spezifizieren. An die verbindenden Kanten annotieren sie das mögliche Risiko. In einer ergänzenden Tabelle ermöglichen sie Detailangaben wie z. B. die Beurteilung des Risikos. Eine Modellierung von einzuleitenden Maßnahmen ist nicht möglich. Meland und Gjaere (2012) adressieren die Modellierung von Prozessbeeinträchtigungen, die rein von IT Systemen ausgehen. Sie argumentieren, dass für die Modellierung dieser Risiken keine weiteren Elemente in die Notation eingefügt werden müssen, damit die Anzahl an Notationselementen geringgehalten werden kann. Entsprechend stellen sie einen Ansatz vor, um Risikoaspekte mit den bestehenden Elementen der BPMN 2.0 abzubilden. Dies ist aus Sicht des Prozessmanagements vorteilhaft, um zusätzliche Komplexität zu vermeiden. Aus Sicht des Risikomanagements ist diese Vereinfachung nachteilig, da nicht alle Besonderheiten von Risikophänomenen, wie z. B. die Erfassung prozessübergreifender Risiko-Ursache-Wirkungsketten, berücksichtigt werden können.

Eine zweite Gruppe von Ansätzen bietet neben der Erfassung von Risiken im Prozessmodell, die Darstellung der Ergebnisse der Risikoquantifizierung. Varela-Vaca et al. (2011) ergänzen auf Basis der BPMN das Prozessmodell um risikorelevante Informationen. So werden die Prozessziele und die Ergebnisse der Risikoquantifizierung im Modell notiert. Eine Abbildung der konkreten Risiken erfolgt neben dem eigentlichen Prozessablauf. Dabei werden die Risiken und die Risikostruktur abgebildet. Es fehlt jedoch eine Darstellung der logischen Zusammenhänge zwischen den Risiken, eine Modellierung der Risikoverantwortlichkeiten und die Abbildung von Risikosteuerungsmaßnahmen. Bernasconi et al. (2013) erfassen Risiken im Prozessmodell mittels des Datenobjekts des BPMN 2.0 Standards und ergänzen das Prozessmodell um eine Fuzzy Cognitive Map (FCM), welche Prozessrisiken und Ursachenzusammenhänge visualisiert und die Einflussstärke an den verbindenden Kanten der FCM anzeigt (siehe Abbildung 35). Risiko-Ursachen-Wirkungszusammenhänge und die Ergebnisse der Risikoquantifizierung können so dargestellt werden. Eine umfassende Integration des Konzeptes in die Prozessmodellierung bleibt allerdings aus, da die FCMs losgelöst vom Prozessmodell modelliert werden. Sie lassen sich entsprechend auch auf andere Risiken als Prozessrisiken anwenden. Des Weiteren können keine Risikosteuerungsmaßnahmen mit diesem Ansatz abgebildet werden.

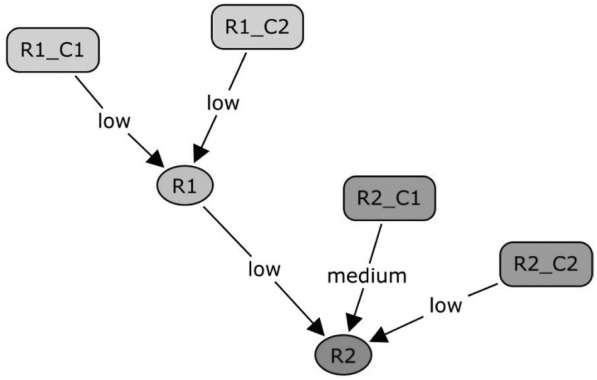


Abbildung 35: Fuzzy Cognitive Map[384]

Mock und Corvo (2005) ermitteln für jedes Risiko eine Prioritätsnummer (RPN = F*C*D), indem sie das Produkt aus der Häufigkeit des Auftretens (F), der Konsequenz (C) und der Erkennbarkeit (D) des Risikos bilden und an die risikobehafteten Ressourcen einer EPK anhängen. Jeder Faktor kann dabei Werte von 1 (gering) bis 10 (hoch) annehmen. Entsprechend gilt ein RPN von 1 als geringes Risiko, ein RPN von 125 als mittleres Risiko und ein RPN von 1000 als hohes Risiko. Die Modellierung komplexer, logisch verknüpfbarer Risikostrukturen und Risikosteuerungsmaßnahmen wird nicht ermöglicht. Dies führt zur mehrfachen Modellierung von ein und demselben Risiko. Hengmith (2005) schlägt vor, mögliche fehlerhafte Prozessausführungen als Risiko in der EPK zu modellieren. Dazu soll die Fehlerwahrscheinlichkeit eines Prozesspfades an den Kanten einer EPK festgehalten werden. Bei einer Exklusiv-Oder-Verknüpfung gleicht der Wert der Wahrscheinlichkeit, dass der Prozesspfad fälschlicherweise ausgeführt wird. Bei einer UND-Verknüpfung entspricht er der Wahrscheinlichkeit der fälschlichen Auslassung des Prozesspfads. Als zusätzliche Option lassen sich mit dem Ansatz ungeplante Prozessabkürzungen modellieren. Weitere Risikoaspekte können nicht erfasst werden, so dass der Ansatz sich ebenfalls lediglich für eine einfache Risikobetrachtung nutzen lässt. Pittl et al. (2017) beschreiben eine Möglichkeit auf Basis der Semantic Web Rule Language (SWRL)[385] Prozessrisiken außerhalb eines Prozessmodells in einem Annotationenmodell zu erfassen. Die Risikoannotationen sind über ungerichtete Kanten mit den betroffenen Aktivitäten im Prozessmodell verbunden, damit der Bezug erkennbar wird. Weiter-

[384] Entnommen aus Bernasconi et al. 2013, S. 117.
[385] Vgl. https://www.w3.org/Submission/SWRL.

hin kann die Wahrscheinlichkeitsverteilung jedes Risikos erfasst werden. Vorteilhaft an der außerhalb des Prozessmodells erfolgenden Erfassung der Risiken ist die Anwendbarkeit auf beliebige Prozess- bzw. Unternehmensmodelle. Nachteilig ist die zunehmende Unübersichtlichkeit der Risiko-Aktivitätszusammenhänge bei der Modellierung vieler Risiken, da entsprechend pro Risiko eine Kante das Prozessmodell mit dem Annotationenmodell verknüpft. Des Weiteren wird von Pittl et al. nicht beschrieben, wie die Abbildung von Risiko-Ursache-Wirkungs-Ketten, Risikoverantwortlichkeiten und Risikosteuerungsmaßnahmen realisiert werden kann. Aus Risikomanagementsicht ist der beschriebene Ansatz somit unvollständig. Zur Muehlen und Rosemann (2005) führen insgesamt vier Modelle ein, um eine risikoorientierte Prozessmodellierung zu realisieren. In der um Risikoobjekte erweiterten EPK stellen sie die risikobehafteten Prozessfunktionen dar. Ergänzend wird innerhalb des „Risk Structure Models“ die hierarchische Beziehung zwischen den Risiken visualisiert. Mittels des „Risk Goal Models“ wird aufgezeigt, welche Risiken welche Prozessziele beeinflussen. Mithilfe des „Risk State Models“ lassen sich sequentielle und komplexe Risiko-Ursache-Wirkungsketten sowie die jeweiligen Eintrittswahrscheinlichkeiten aller Ursachen und Wirkungen abbilden (siehe Abbildung 36). Verantwortlichkeiten und Risikosteuerungsmaßnahmen werden in dem Ansatz nicht berücksichtigt.

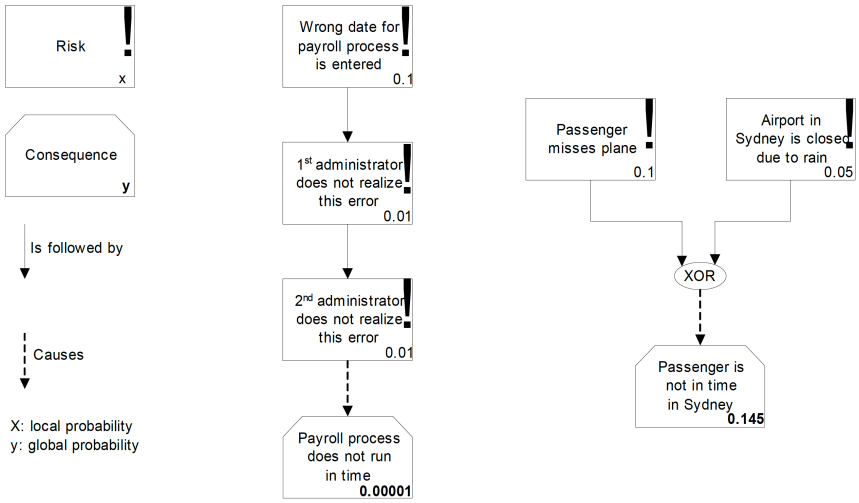


Abbildung 36: Risk State Model[386]

[386] Entnommen aus zur Muehlen und Rosemann 2005.

Eine dritte Gruppe von Ansätzen berücksichtigt sowohl Aspekte der Risikoidentifizierungsphase, der Risikoquantifizierung als auch der Risikosteuerung innerhalb der Prozessmodellierung. Brabänder und Ochs (2002) ergänzen die EPK um ein Risikoobjekt, welches an die zugehörige Prozessfunktion angehangen wird (siehe Abbildung 37). Details zum Risiko, wie die einzuleitenden Steuerungsmaßnahmen und die Verantwortlichkeit, modellieren sie in einer separaten Risikodetailanalyse. Ebenso stellen sie separat drei Rechenwege zur Bestimmung des Risikoausmaßes vor. Zwei der Rechenwege nehmen direkten Bezug zum bestehenden Prozessmodell.

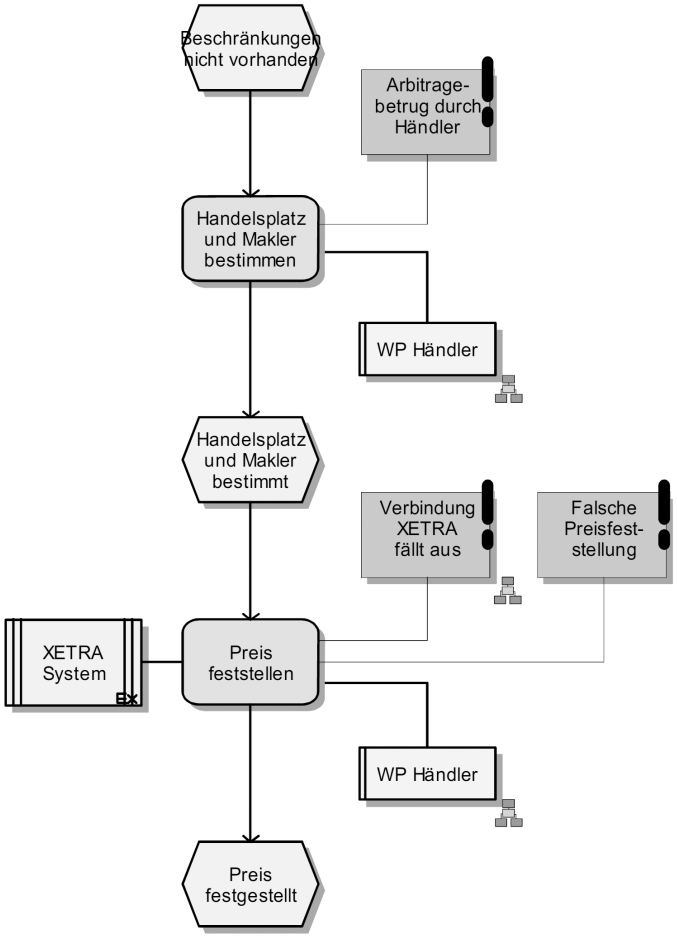


Abbildung 37: Risikoorientierte EPK[387]

Karagiannis (2007) sowie Diederichs und Imhoff (2011) ergänzen das Prozessmodell jeweils mit einer Tabelle, um Risikodetailinformationen zu erfassen. Beide Ansätze erfassen in der

[387] Entnommen aus Brabänder und Ochs 2002, S. 24.

Tabelle das Risiko, qualitative Aussagen zur Risikobedrohung und die vorgesehenen Risikosteuerungsmaßnahmen. Hermann und Herrmann (2006) fokussieren sich auf die Sicherheit von Geschäftsprozessen. Dazu führen sie Sicherheitsanforderungen ein, die während der Prozessdurchführung überprüft werden, so dass Steuerungsmaßnahmen im kritischen Fall automatisch gestartet werden können, um dem Risiko entgegen zu wirken. Anhand des erforderlichen Sicherheitsgrades (Skala von 0-7) und des Bedrohungspotentials (Skala von 0-7) eines kritischen Objekts ermitteln sie ein „Risk Level“. Ist dieses gleich 0, liegt kein Risiko vor. Marcinkowski und Kuciapski (2012) erweitern die BPMN 2.0 um Risikoelemente, Risikosteuerungsmaßnahmen und eine Einschätzung von Risikoeintrittswahrscheinlichkeit und Schadensausmaß. Alle Erweiterungen werden dabei direkt im Prozessmodell modelliert. Bei vier dieser fünf Ansätze basiert die „Quantifizierung“ auf subjektiven Einschätzungen zum vorliegenden Risiko. Lediglich Brabänder und Ochs (2002) berücksichtigen die Daten historischer Prozessverläufe im Rahmen der Quantifizierung. Weiterhin modellieren sie als Einzige den verantwortlichen Risk Owner. Eine Modellierung von Ursache-Wirkungs-Beziehungen zwischen den Risiken ist mit keinem der fünf Ansätze möglich.

Eine sehr ausführlichere Modellierung von Risikophänomenen ermöglicht die Gruppe der Ansätze von Jakoubi et al. (2007), Rieke (2009), Sienou et al. (2007), Strecker et al. (2011) und Weiß und Winkelmann (2011). Ähnlich wie zur Muehlen und Rosemann (2005) und Pittl et al. (2017) führen Jakoubi et al. und Sienou et al. das Prozessmodell ergänzende Modelle ein, um die Risikophänomene zu beschreiben. Jakoubi et al. unterscheiden zwischen der Prozessschicht, einer CARE-Schicht und einer TIP-Schicht. Die in der Prozessschicht modellierten Geschäftsprozessaktivitäten werden innerhalb der „Condition, Action, Ressource and Environment (CARE)“-Schicht in ihre einzelnen Bestandteile zerlegt. Dabei wird die Beziehung zwischen jeder Aktivität und den eingesetzten Ressourcen sowie die Aktivität beeinflussenden Umweltfaktoren modelliert. Die Ressourcen und das Umfeld unterliegen Bedrohungen, welche separat in der „Threat Impact Process“-Schicht abgebildet werden. Zwischen den Schichten zeigen gerichtete Kanten, in welchem Zusammenhang die jeweiligen Elemente stehen. Jakoubi et al. ermöglichen mit dem Ansatz die Darstellung sequentieller Risiko-Ursache-Wirkungsbeziehungen sowie zugehöriger Risikosteuerungsmaßnahmen in Bezug auf eine Prozessaktivität. Komplexe logisch verbundenen Risikozusammenhänge und aktivitätsübergreifende Risikobezüge werden nicht explizit als modellierbar beschrieben. Die Abbildung

eines Risk Owners fehlt. Sienou et al. (2007) führen eine Reihe an Elementen und Diagrammen ein, um Risikomanagementaspekte mit Bezug zu einem Geschäftsprozess zu modellieren. Dabei lösen sie ebenfalls die eigentliche Risikomodellierung von den Prozessmodellen, indem für jede Prozessaktivität separat ein Risikoszenariodiagramm (siehe Abbildung 38), ein Risikostrukturdiagramm und ein Szenariosteuerungsdiagramm (siehe Abbildung 39) eingeführt wird. Innerhalb des Risikoszenariodiagramms lassen sich alle auf eine Prozessaktivität beziehenden Risiko-Ursache-Wirkungsketten darstellen. Dabei sind komplexe Verbindungen mithilfe von logischen Konnektoren abbildbar. Ebenso werden die betroffenen Prozessziele abgebildet.

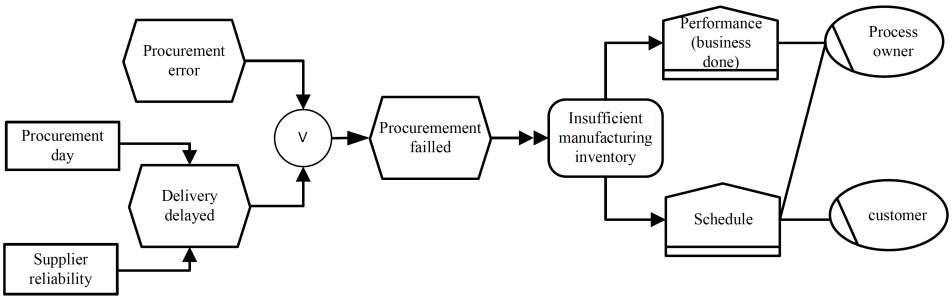


Abbildung 38: Risikoszenariodiagramm[388]

Im Risikostrukturdiagramm wird mittels der Darstellung von Aggregationsbeziehungen visualisiert, aus welchen Subrisiken ein Risiko besteht. Im Szenariosteuerungsdiagramm werden für jedes Risiko die vorgesehenen Steuerungsmaßnahmen modelliert. Für jede Maßnahme wird festgehalten, welchen Einfluss sie auf die Eintrittswahrscheinlichkeit und das Schadensausmaß des Risikos hat. Die Schwäche des Ansatzes liegt insbesondere in der separaten Betrachtung der Risiken verschiedener Prozessaktivitäten. Die Risiken lassen sich lediglich pro Aktivität modellieren. Falls ein Risiko jedoch mehrere Aktivitäten beeinflusst, kann dies nicht dargestellt werden bzw. es muss mehrfach modelliert werden. Obwohl Stakeholder grundsätzlich modelliert werden können, fehlt jedoch eine eindeutige Kennzeichnung des Risk Owners.

[388] Entnommen aus Sienou et al. 2007, S. 126.

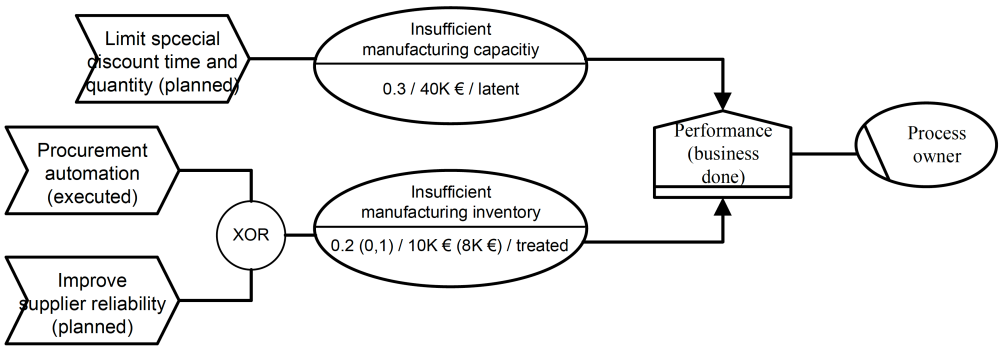


Abbildung 39: Szenariosteuerungsdiagramm[389]

Rieke (2009)[390] erweitert die EPK zu einer risikoorientierten EPK. Dabei verwendet er weitestgehend die bestehenden EPK-Elemente, indem diese mit Annotationen und grafischen Ergänzungen angereichert werden. Lediglich ein sogenannter „Break-Operator“ wird neu eingeführt. Dieser ermöglicht die Darstellung der prozessunterbrechenden Wirkung eines Risikoereignisses. Insgesamt lassen sich mit dem Ansatz die an Prozessfunktionen angebundenen Risiken, Risikosteuerungsmaßnahmen und Annotationen mit Risikobezug (z. B. die Eintrittswahrscheinlichkeit) modellieren. Ebenso beschreibt Rieke die Möglichkeit der Darstellung komplexer Risiko-Ursache-Wirkungsketten. Eine Abbildung der Verantwortlichkeiten wird nicht beschrieben. Konkrete Erläuterungen, in welchem Zusammenhang die modellierten Steuerungsmaßnahmen zu den Risiken stehen (z. B. Bedingungen für den Start der Maßnahme) oder welchen Einfluss sie ausüben (z. B. quantifizierte Wirkung), werden nicht aufgeführt. Strecker et al. (2011) stellen auf Basis der Multi Perspective Enterprise Modeling Methode (MEMO) mehrere Konstrukte vor, mit welchen Risiken beliebig detailliert in Organisationsmodellen (u. a. auch in Prozessmodellen) modelliert werden können. Dabei berücksichtigen sie Risiko-Ursache-Wirkungsketten, Quantifizierungsaspekte, Risikosteuerungsmaßnahmen und Verantwortlichkeiten. Der Schwerpunkt ihrer Betrachtung liegt im Bereich der IT-Infrastrukturrisiken, allerdings lässt sich der Ansatz auch auf beliebige andere Domänen anwenden. Der Ansatz ermöglicht eine umfassende risikoorientierte Prozessmodellierung. Die Modellierung von Risiko-Ursache-Wirkungsketten ist jedoch nicht überzeugend, da die Ver-

[389] Entnommen aus Sienou et al. 2007, S. 127.
[390] In Rieke und Winkelmann (2008) sowie Rieke (2009) wird derselbe Ansatz vorgestellt, jedoch führt Rieke (2009) die Aspekte detailliert aus. Entsprechend wird an dieser Stelle nur auf Rieke (2009) eingegangen.

bindungen zwischen risikobehaftetem Element und Risikoelement nur unidirektional erfolgen. Es ist aber durchaus möglich, dass ein Element bzw. im speziellen eine Prozessaktivität, sowohl von Risiken betroffen als auch Verursacher der Risiken ist. Dies sollte unterschieden werden können. Weiterhin wird mit MEMO eine aus Prozessmanagementsicht untypische Notation verwendet, so dass auf Anwenderseite ein zusätzlicher Lernaufwand erforderlich ist. Gleiches gilt für den Ansatz von Weiß und Winkelmann (2011), welcher auf der eher unbekannten SBPML[391] Notation aufbaut. Er unterstützt zwar viele Risikoaspekte, aber aufgrund der Spezialisierung auf den Bankensektor und der gewählten Notation, unterliegt der Ansatz aus allgemeiner Risikomanagementsicht einigen Restriktionen. Es ist bspw. nicht möglich logische Verknüpfungen zwischen den Risikoelementen zu modellieren und die Notation sieht nur sequentielle Prozessabfolgen vor. Somit sind komplexe Risiko-Ursache-Wirkungsketten nicht abbildbar.

Ansätze zur Unterstützung der Prozessdurchführungsphase

Die Ansätze von Conforti et al. (2013), Kang et al. (2009), Singh et al. (2008) und Wickboldt et al. (2011) zielen auf die Erkennung und Antizipation von Risiken während der Prozessdurchführung ab. Conforti et al. stellen einen Ansatz vor, der die Risikoüberwachung in IT-gesteuerten Geschäftsprozessen ermöglicht. Dazu führen sie eine eigene Sprache ein, welche die Definition von Regeln zur Überwachung der Geschäftsprozessrisiken erlaubt. Die Regeln werden in Form von Sensoren in einem eigenständigen IT-System (Sensormanagementsystem) implementiert, um die Prozessausführung zur Laufzeit zu überwachen. Ein Sensor ist dabei durch eine Wahrheitsfunktion definiert, welche die Erfüllung der zuvor festgelegten Bedingungen überprüft. Ist eine Bedingung erfüllt, wird der zuständige Prozessverantwortliche alarmiert. Die Sensoren beziehen Prozessinformationen aus historischen und aktuellen Prozessinstanzdaten und sind so während der Prozessausführung in der Lage, Prognosen zum weiteren Prozessverlauf bzw. zu einer risikobehafteten Situation zu machen. Weitergehende (automatisierte) Risikomanagementfunktionen sieht der Ansatz nicht vor. Kang et al. erzeugen aus Daten historischer Prozessverläufe einen Entscheidungsbaum, um Regeln und Wahrscheinlichkeiten für risikobehaftete Prozessverläufe aus den Daten abzuleiten. Mithilfe des erzeugten Entscheidungsbaumes prognostizieren sie das Risikoniveau einer Prozessinstanz

[391] Vgl. Becker et al. 2009.

bereits während der Ausführung neuer Instanzen, so dass Warnungen erzeugt werden können, wenn ein bestimmtes Risikoniveau überschritten wurde. Die zugrundeliegenden Logdateien mit den Daten der historischen Prozessverläufe besitzen jeweils pro Prozessinstanz Informationen über die eingetretenen Prozessereignisse mit ihren Attributen und eine Beurteilung, ob in der Instanz ein Risiko aufgetreten ist oder nicht. Wie die Beurteilung eines Risikos erfolgte, wird in dem Ansatz nicht deutlich. Ebenso bleibt unklar, wie mit verschiedenartigen Risiken umgegangen wird, da der Ansatz vereinfachend ein Risiko nur als einen normalen bzw. unnormalen Prozessverlauf charakterisiert. Es kann somit lediglich eine Aussage dazu getroffen werden, ob eine Prozessinstanz risikobehaftet ist oder nicht. Da dadurch nicht deutlich wird, welches Risiko den Prozess gefährdet, können auch keine zielgerichteten Risikosteuerungsmaßnahmen eingeleitet werden. Aus Sicht des Risikomanagements ist dieses Vorgehen nicht zufriedenstellend, da als einzige Steuerungsmaßnahmen die Akzeptanz des unbekannten Risikos oder der Abbruch der Prozessinstanz in Frage kommt. Singh et al. stellen einen Ansatz vor, der vorsieht laufende Prozessinstanzen zu überwachen und Risiken während der Laufzeit einer Prozessinstanz zu umgehen. Dabei geht der Ansatz explizit nur auf das Risiko fehlender Ressourcen ein, die im Prozess benötigt werden. Auf Basis historischer Daten wird dazu eine Verteilungsfunktion erzeugt, die Aussagen zur Wahrscheinlichkeit eines nicht erfolgreichen Prozessverlaufs aufgrund fehlender Ressourcen ermöglicht. Wenn ein zuvor definierter Schwellenwert durch Parameteränderungen während des Instanzdurchlaufs über- oder unterschritten wird, schlagen Singh et al. als Steuerungsmaßnahme vor, einen identischen Prozess zu starten („Sicherungsprozess“), welcher die geänderten Parameter antizipiert, so dass ausreichend Ressourcen dem originären Prozess bereitgestellt werden. Dadurch soll der Eintritt des Risikos eines nicht finalisierbaren, originären Prozesses aufgrund fehlender Ressourcen umgangen werden. Wie der Sicherungsprozess konkret ausgelöst wird, wird nicht beschrieben. Weiterhin berücksichtigt der Ansatz keine anderen Risiken, die das Prozessziel gefährden könnten. Weiterhin ist die Unterversorgung mit Ressourcen ein leicht zu antizipierendes Risiko, welches bereits im ursprünglichen Prozessdesign modelliert werden könnte. Wesentlich interessanter wäre eine dynamische Prozessanpassung bei Auftreten externer nicht direkt beeinflussbarer Risiken. Dies lässt sich mit dem vorgestellten Ansatz nicht realisieren. Wickboldt et al. stellen ebenfalls ein Verfahren zur Laufzeitanalyse von Prozessen vor. Auf Basis von Logdateien, die mit Risikoinformationen angereichert wurden, analysieren sie zunächst

die Ähnlichkeit aktueller und historischer Prozesse mittels einer Ähnlichkeitsfunktion. Sie stellen heraus, dass nicht alle Prozessinstanzen identisch ablaufen und daher zunächst der Grad der Ähnlichkeit zwischen einem aktuell laufenden Prozess und den historischen Prozessverläufen ermittelt werden muss. Darauf aufbauend bestimmen sie, unter Berücksichtigung des Ähnlichkeitsgrads und der historisch aufgetretenen Risiken, die Eintrittswahrscheinlichkeit und das Schadensausmaß von Risikoereignissen für jede Aktivität des aktuellen Prozesses. In Abhängigkeit von der ausgesetzten Bedrohung sieht das Verfahren anschließend eine Klassifikation aller Aktivitäten des aktuellen Prozesses vor. Die risikobehafteten Aktivitäten werden anschließend nach Bedrohungslage geordnet in einem Risikoreport aufgeführt. Der Ansatz sieht ebenfalls keinen aktiven Eingriff in den laufenden Prozess vor, sondern erfüllt eine rein risikoüberwachende Funktion. Weiterhin bleibt offen, wie die Logdateien konkret um Risikoinformationen angereichert werden. Dies manuell zu realisieren, erscheint aufgrund der vielfach großen Menge an Logeinträgen nicht praktikabel.

Ansätze zur Unterstützung der Prozessevaluationsphase

Jans et al. (2011) untersuchen die Anwendbarkeit von Process Mining im Rahmen der Innenrevision (siehe Kapitel 5.2.4). Dazu untersuchen sie den Beschaffungsprozess eines Finanzdienstleisters und identifizieren regelmäßige Abweichungen vom vorgesehenen Prozessmodell. So werden z. B. häufig Zahlungen an Lieferanten ohne vorherige Genehmigung ausgeführt. Die wesentliche Erkenntnis des Beitrags liegt in der nachweislichen Anwendbarkeit von Process Mining in der Innenrevision zur ex-post Aufdeckung von Risiken in Prozessen auf Basis historischer IT-Logdateien.

7.5. Erweiterung der BPMN um eine Risikosicht

7.5.1. Zielsetzung

Bestehende Ansätze zur Verbindung von Risikophänomenen mit Prozessmodellen weisen insgesamt Mängel auf. Bei allen Ansätzen der Prozessdesignphase erfolgt keine systematische Herleitung der Risikomanagementanforderungen, so dass vielfach wesentliche Aufgaben der einzelnen Risikomanagementphasen bei der Einbindung von Risikophänomenen in das Prozessmodell nicht berücksichtigt werden. Des Weiteren fehlt meist eine formale Beschreibung der vorgeschlagenen Risikokonstrukte, welche die Beziehungen der neu eingeführten Elemente untereinander eindeutig erläutert.[392] Letztlich besteht eine Forschungslücke darin, dass eine Notation fehlt, deren Risikokonstrukte sich sowohl für den Einsatz in der Prozessdesignphase als auch in der Prozessdurchführungsphase verwenden lassen.[393] Diese Lücken sollen im Folgenden geschlossen werden.

Damit die zu entwickelnde risikoorientierte Prozessnotation einerseits auf einer bereits etablierten Methode aufbauen kann und andererseits selbst von praktischer Relevanz ist, erscheint es sinnvoll, auf bestehenden Standards aufzubauen.[394] Im Rahmen der Geschäftsprozessmodellierung hat sich die BPMN in der Version 2.0 in den letzten Jahren weltweit durchgesetzt und wurde in ISO/IEC 19510:2013 zum Standard ernannt.[395] Der Standard enthält bisher keine Elemente zur vollständigen Beschreibung von Risikophänomenen in Geschäftsprozessen. Entsprechend wird die zu konzipierende risikoorientierte Prozessnotation auf Basis der BPMN entwickelt. Dabei soll möglichst auf bestehende BPMN Elemente zurückgegriffen werden und die Einführung neuer Elemente geringgehalten werden, um die Anwenderakzeptanz der neuen Erweiterung zu fördern.

7.5.2. Erweiterung

Die BPMN sieht bereits in der Spezifikation eine Erweiterbarkeit der Notation vor (siehe Kapitel 5.3.3). Diese ermöglicht ein Hinzufügen von neuen domänenspezifischen Aspekten (z. B. wie hier von Risikomanagementaspekten) unter Sicherstellung der Gültigkeit des

---

[392] Vgl. Suriadi et al. 2014, S. 950.
[393] Vgl. Suriadi et al. 2014, S. 951.
[394] Vgl. Bernasconi et al. 2013, S. 114.
[395] Vgl. https://www.iso.org/standard/62652.html; Chinosi und Trombetta 2012, S. 125; Yousfi et al. 2016, S. 55.

BPMN Kerns.[396] Die Elemente der BPMN werden grundsätzlich auf zwei Arten in der Spezifikation repräsentiert. Zum einen als ein Metamodel der MetaObject Facility Spezifikation (MOF)[397] zur Beschreibung der Sprachkonzepte und ihrer Beziehungen. Zum anderen durch ein Schemadokument im Extensible Markup Language (XML) Format, zur Beschreibung des Austauschformats der BPMN Modelle.[398] Letzteres stellt die Wiederverwendbarkeit der Modelle in unterschiedlichen BPMN Anwendungen (z. B. in Modellierungswerkzeugen) sicher. Zur Einführung einer Risikosicht in den BPMN Standard muss die Erweiterung entsprechend auf diese beiden Arten beschrieben werden. In der Spezifikation ist es jedoch nicht vorgesehen, dass eine Erweiterung der BPMN auf Metamodellebene frei definiert werden kann. Dies führt dazu, dass jedes Element einer Erweiterung grundsätzlich mit jedem BPMN Element des Standards verbunden werden kann und eine Erweiterung lediglich einzelner spezifischer BPMN Elemente somit nicht möglich ist.[399] Dazu wäre eine Definition der Erweiterung auf höherer Abstraktionsebene notwendig. Weiterhin fehlt in der Spezifikation ein systematisches Vorgehensmodell, wie eine Erweiterung zur BPMN hinzugefügt werden kann.[400] Stroppi et al. (2011) stellen daher ein Vorgehensmodell vor, welche diese Lücken schließt. Es besteht aus vier Schritten:

1) Konzeptualisierung der Erweiterung in der Unified Modeling Language (UML)[401]
2) Erzeugung eines BPMN+X Modells der Erweiterung
3) Transformation des BPMN+X Modells in ein XSD Modell der Erweiterung
4) Transformation des XSD Modells in ein XSD Dokument

Im ersten Schritt werden die Elemente der neu einzuführenden Erweiterung und ihr Zusammenspiel untereinander sowie mit den bestehenden BPMN Elementen beschrieben. Im vorliegenden Fall sind dies alle in der Prozessmodellierung zu berücksichtigenden Risikophänomene. Dies erfolgt mittels eines Klassenmodells in Notation der Unified Modeling Language (UML), auf welcher auch die BPMN aufbaut. Das erzeugte Klassenmodell wird von Stroppi

[396] Vgl. Object Management Group 2011, S. 44.
[397] Vgl. http://www.omg.org/mof/.
[398] Vgl. Stroppi et al. 2011, S. 61.
[399] Vgl. Stroppi et al. 2011, S. 61.
[400] Vgl. Stroppi et al. 2011, S. 59.
[401] Vgl. http://www.omg.org/spec/UML/.

et al. als „Conceptual Domain Model of the Extension“ (CDME) bezeichnet. Das CDME wird bewusst ohne Berücksichtigung der Restriktionen, die sich aus der BPMN Spezifikation ergeben, erstellt. Im zweiten Schritt wird unter Anwendung von neun Transformationsregeln aus dem CDME ein BPMN-konformes Klassendiagramm erzeugt, welches als BPMN+X Modell bezeichnet wird. Schritt drei und vier dienen der Erzeugung eines XML Schema Dokumentes der Erweiterung, welches letztlich die Austauschbarkeit der Erweiterung zwischen unterschiedlichen BPMN-konformen Anwendungssystemen erlaubt. Braun et al. (2015) modifizieren den Ansatz von Stroppi et al., indem sie der Erstellung des CDME eine systematische Prüfung („Domain Analysis and Equivalence Check“) voranstellen. Dieser Schritt dient der Überprüfung, welche Elemente der geplanten Erweiterung bereits mit bestehenden BPMN Elementen aus dem Standard realisiert werden können. Ziel ist es hierbei, nur so viele neue Elemente in die BPMN einzuführen, wie notwendig. Des Weiteren lassen Braun et al. die Transformation der Erweiterung in ein XML Schema Dokument aus[402] und ergänzen ihr Vorgehensmodell um einen Schritt, in welchem sie die konkrete Syntax der Erweiterung vorstellen. Aufgrund der Zielsetzung dieses Kapitels wird daher die Erweiterung der BPMN um eine Risikosicht mittels des Vorgehens von Braun et al. umgesetzt (siehe Abbildung 40).

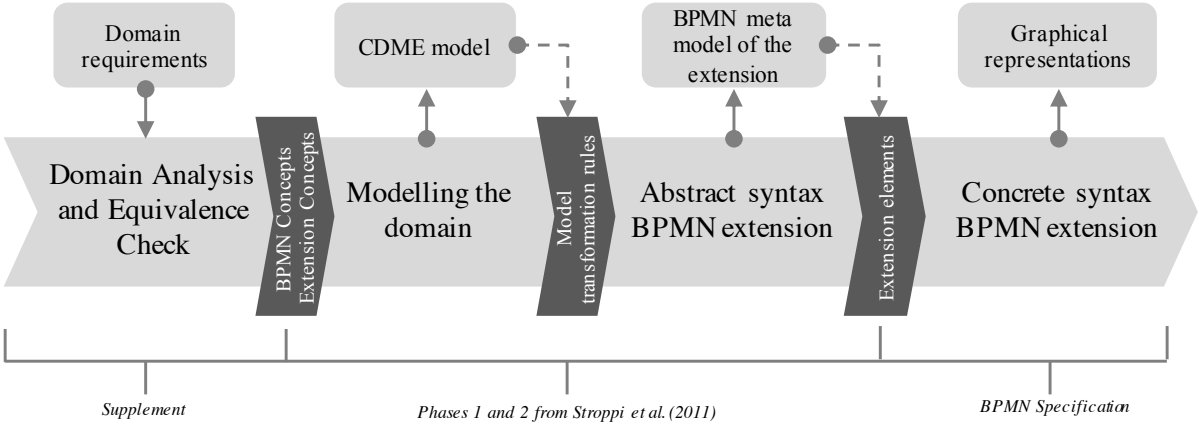


Abbildung 40: Vorgehensmodell zur Erweiterung der BPMN[403]

[402] Diese kann jederzeit auf Basis des BPMN+X Modells durchgeführt werden.
[403] In Anlehnung an Braun et al. 2015, S. 471.

7.5.2.1. Domänenanalyse und Äquivalenzprüfung

In Kapitel 7.2 und 7.3 wurden Anforderungen an eine risikoorientierte Prozessnotation formuliert (Domänenanalyse). Aus ihnen wurde abgeleitet, welche Konzepte eine Risikosicht in einem Prozessmodell abbilden muss. Sie sind daher der Ausgangspunkt für die Äquivalenzprüfung. Anhand einer tiefgehenden Analyse der BPMN Spezifikation wird dabei geprüft, ob das benötigte Konzept mit Elementen der BPMN modelliert werden kann. Ist dies der Fall wird im CDME das BPMN Konzept verwendet. Andernfalls wird ein neu einzuführendes Erweiterungskonzept im CDME definiert. Im Ergebnis werden nur so viele Erweiterungskonzepte wie notwendig neu eingeführt. Das Ergebnis der Äquivalenzprüfung ist in Abbildung 41 dargestellt.

Konzept	**Semantik**	**Äquivalenzprüfung**	**CDME**
Prozessziele	Ausgangspunkt der Risikoidentifizierung.	Keine Äquivalenz.	Erweiterungskonzept
Zielkennzahl und Bezugsobjekt	Messbare Größe für ein Ziel (Kosten, Durchlaufzeit, Qualität) bezogen auf ein Objekt (z. B. einen Zeitraum).	Keine Äquivalenz.	Erweiterungskonzept
Risiko	Risiko, welches auf einen Prozess einwirkt oder in diesem entsteht und das Erreichen eines oder mehrerer Ziele gefährdet.	Keine Äquivalenz.	Erweiterungskonzept
Risikocharakteristika	Definition von Name, Kategorie, Eintrittswahrscheinlichkeit, Schadensausmaß, Verteilungsfunktion und Schwellenwert.	Teilweise Äquivalenz → Text-Annotation; Aus Gründen der Übersichtlichkeit sollten die Charakteristika als Attribute des Risikoelements definiert werden.	Erweiterungskonzept
Risk Owner	Risikoverantwortliche Person oder Organisationseinheit.	Äquivalenz → Pools, Swimlanes.	BPMN Konzept

Konzept	Semantik	Äquivalenzprüfung	CDME
Risikofluss	Verbindungspfade zwischen Risiken sowie Risikosteuerungsmaßnahmen. Pfade müssen die Art des Zusammenhangs abbilden.	Teilweise Äquivalenz → Flows, diese bieten jedoch keine Unterscheidung der Art des Zusammenhangs (Ausmaß verstärkend etc.).	Erweiterungskonzept
Logikkonnektoren	Abbildung komplexer Risikoverbindungen (unter anderem Risiko-Ursache-Wirkungsketten).	Äquivalenz → Gateways.	BPMN Konzept
Risikokorrelationen	Korrelation zwischen Risiken ohne kausalen Zusammenhang.	Keine Äquivalenz.	Erweiterungskonzept
Risiko-Prozess-Bezug	Verknüpfung von Risiken mit Prozesselementen, zur Verdeutlichung der Zugehörigkeit.	Keine Äquivalenz.	Erweiterungskonzept
Risikolink	Verbindung zwischen Risiko-Ursache-Wirkungsketten über Lane-, Pool- und Prozessgrenzen hinweg.	Teilweise Äquivalenz → Link Ereignis; Laut Spezifikation darf das Link Ereignis allerdings nur innerhalb eines Prozesses verwendet werden.	Erweiterungskonzept
Risikosteuerungsmaßnahmen	Aktivitäten zur Steuerung von Risiken.	Keine Äquivalenz → Aufgaben haben keine spezifischen Marker.	Erweiterungskonzept
Maßnahmencharakteristika	Eigenschaften einer Maßnahme wie Maßnahmenschwellenwert, Wirkung auf Eintrittswahrscheinlichkeit, Wirkung auf Schadensausmaß.	Teilweise Äquivalenz → Text-Annotation; Zur Übersichtlichkeit sollten die Charakteristika als Attribute des Maßnahmenelements definiert werden.	Erweiterungskonzept

Abbildung 41: Ergebnis der Äquivalenzprüfung

7.5.2.2. Modellierung der Domäne

Auf Basis der Äquivalenzprüfung werden im CDME die Beziehungen neuer und bestehender BPMN Elemente mittels eines UML Klassendiagramms dargestellt (siehe Abbildung 43).[404] Eine Klasse beschreibt in der Objektorientierung die Struktur und das Verhalten einer Menge von Objekten, die identische Attribute und Methoden besitzen. Sie wird in der UML mittels eines Rechtecks, welches den Klassennamen enthält, dargestellt. Optional beinhaltet das Rechteck zusätzlich die Attribute und Methoden der Klasse. Die Beziehungen zwischen den Klassen werden mittels Kanten, den sogenannten Assoziationen, beschrieben. An die Kantenenden werden die Multiplizitäten geschrieben, welche ausdrücken, wie viele der Objekte einer Klasse in Relation zu den Objekten der anderen Klasse stehen (siehe Abbildung 42).

Beschreibung	**Multiplizität**
Kein oder ein Objekt.	0..1
Genau ein Objekt.	1
Kein, ein oder mehrere Objekt/e.	0..* (Kurzform: *)
Mindestens ein Objekt.	1..*

Abbildung 42: Arten von Multiplizitäten

Mittels einer Generalisierung wird eine gerichtete Beziehung zwischen einer Oberklasse und einer oder mehreren Unterklassen beschrieben. Die Unterklassen stellen Spezialisierungen der Oberklasse dar. Sie erben alle Attribute und Eigenschaften der Oberklasse und verfügen zusätzlich über eigene (spezielle) Attribute und Methoden. Die Generalisierung wird als durchgezogene Linie von der Unterklasse zur Oberklasse dargestellt. Am Ende der Linie befindet sich eine geschlossene, nicht ausgefüllte Pfeilspitze.

Im CDME werden zunächst alle BPMN Elemente modelliert, die eine Beziehung zu den Risikoelementen der Erweiterung besitzen. Dies sind Pools (inklusive Lanes), Prozesse, Flusselemente (Aktivitäten, Ereignisse, Operatoren) und Datenobjekte. Sie werden im CDME grau eingefärbt und als BPMN Concept ausgewiesen, da sie in dieser Form bereits im BPMN

[404] Auf die Darstellung von Attributen wird aus Gründen der Übersichtlichkeit verzichtet. Die jeweils wesentlichen Attribute eines Objekttyps sind in Kapitel 7 aufgeführt.

Metamodell vorhanden sind. Alle neu eingeführten Klassen bzw. Objekttypen der Risikoerweiterung werden in Weiß und als Extension Concept dargestellt.

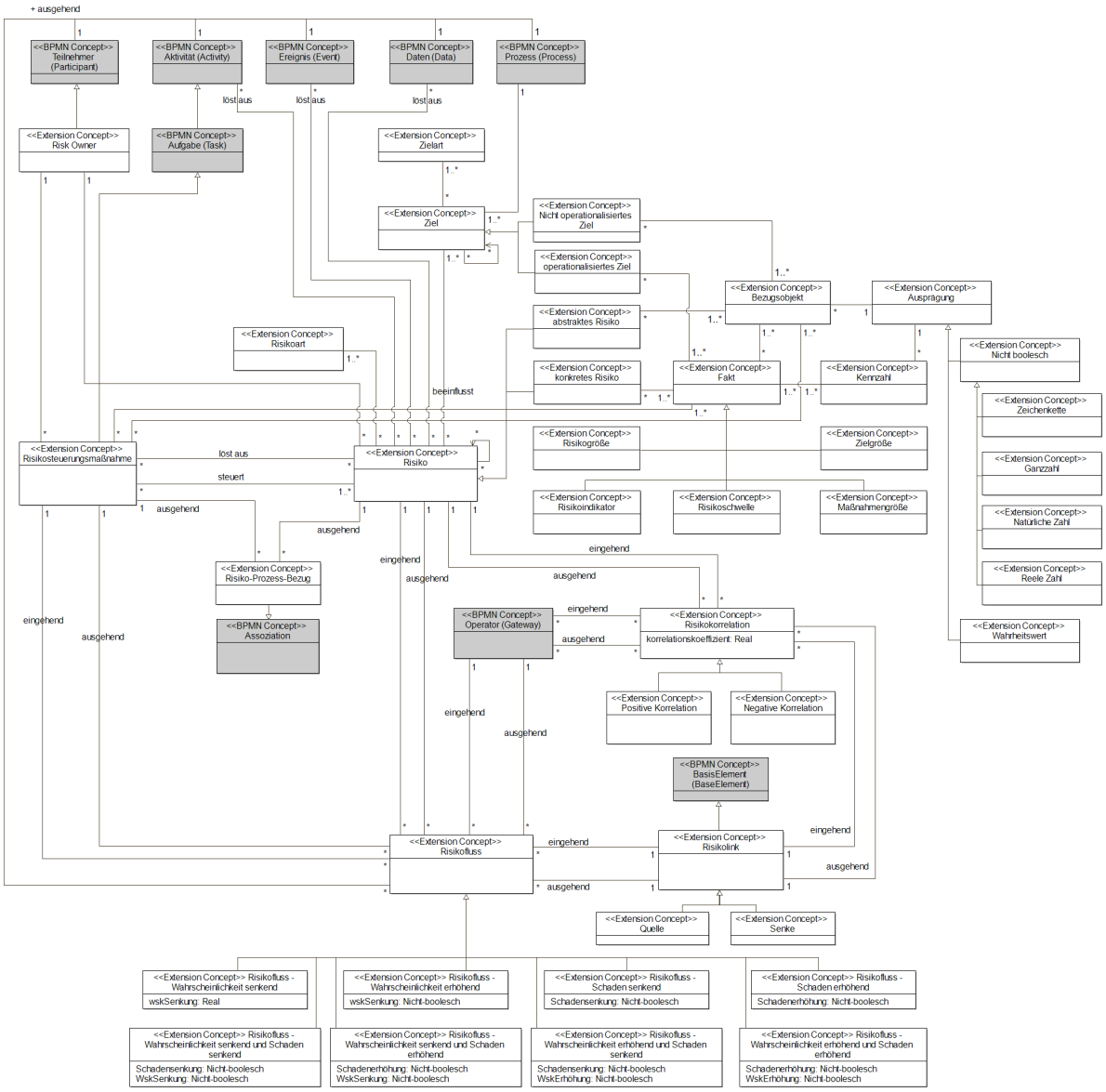


Abbildung 43: Metamodell der BPMN Erweiterung (CDME)[405]

Objekttyp Ziel

Da Risiken sich aus den Unternehmens- und Prozesszielen ableiten, sind diese zu definieren und die Notation muss ihre detaillierte Beschreibung ermöglichen (siehe Kapitel 7.2). Dazu

[405] Die Abbildung befindet sich in einer größeren Auflösung im Anhang dieser Arbeit.

wird ein Objekttyp *Ziel* in das CDME eingeführt und mit dem Objekttyp *Prozess* verbunden, da jeder Prozess mindestens ein Ziel verfolgt. Jedes Ziel verfügt über allgemeine Eigenschaften wie z. B. einen Namen und eine Beschreibung, welche als Attribute des Objekttyps *Ziel* modelliert werden können. Des Weiteren kann ein Ziel Eigenschaften besitzen, die es spezifizieren. Es lassen sich dabei konkrete und abstrakte Ziele unterscheiden. Die konkreten Ziele werden durch Fakten ausgedrückt (z. B. Anzahl der Kundenbeschwerden pro Woche < 50). Die abstrakten Ziele sind hingegen unscharf formuliert (z. B. Erhöhung der Kundenzufriedenheit). Konkrete Ziele mit Prozessbezug können weiterhin Instanz-bezogen (z. B. Durchlaufzeit <= 20 Minuten) oder Instanz-übergreifend (z. B. Prozessfehlerquote pro Quartal < 5 %) formuliert werden. Die Ziele müssen sowohl durch konkrete Kennzahlen und zugehörige Bezugsobjekte (z. B. einem Zeitraum), als auch abstrakt, ohne einen Kennzahlenbezug, spezifizierbar sein. Mit starren Attributen und im Vorfeld festgelegten Datentypen lassen sich solche Spezifizierungen nicht realisieren. Daher werden die Objekttypen *Fakt*, *Kennzahl*, *Bezugsobjekt* und *Ausprägung* in das CDME eingeführt.[406]

Zielgröße: Kundenzufriedenheit	**Kennzahl**	**Ausprägung**
	Anzahl	< 50
	Bezugsobjekt	**Ausprägung**
	Zielgegenstand	Kundenreklamationen
	Zeitraum	1 Monat

Abbildung 44: Darstellung einer konkret definierten Zielgröße

Ein konkretes Ziel wird durch einen Fakt *Zielgröße* repräsentiert (siehe Abbildung 44). Die Zielgröße wird durch eine Kennzahl mit einer bestimmten Ausprägung definiert und besitzt ein oder mehrere Bezugsobjekte. Ein Fakt repräsentiert somit eine eindeutige Kombination aus einer Kennzahl und einem oder mehreren Bezugsobjekten. Als Ausprägung lassen sich quantitative und qualitative Größen festlegen. Ein abstraktes Ziel lässt sich mittels dem Objekttyp *Bezugsobjekt* definieren (siehe Abbildung 45).

[406] Vgl. im Folgenden Rieke 2009, S. 192 ff.

Abstraktes Ziel	**Bezugsobjekt**	**Ausprägung**
	Kundenzufriedenheit	erhöhen

Abbildung 45: Darstellung eines abstrakten Ziels

Da zwischen Zielen eine hierarchische Beziehung bestehen kann, besitzt das Zielobjekt einen Selbstbezug (reflexive Assoziation). Durch den Objekttyp *Zielart* wird eine Kategorisierung der Ziele ermöglicht (z. B. leistungswirtschaftliches Ziel oder Finanzziel), um diese voneinander abzugrenzen.

Objekttyp Risiko

Die Risiken, als zentrales Element der Risikosicht, werden im CDME über den Objekttyp *Risiko* modelliert. Ein Ziel wird entweder von keinem, einem oder mehreren Risiken beeinflusst und ein Risiko kann wiederum ein oder mehrere Prozessziele gefährden. Sie sind daher direkt den Zielen zugeordnet, auf die sie einen Einfluss nehmen können. Analog zu den Zielen lassen sich Risiken, je nach Informationsstand, abstrakt oder konkret (quantitativ) beschreiben, so dass sie im CDME als abstraktes Risiko bzw. konkretes Risiko spezifiziert werden können. Die abstrakten Risiken lassen sich mithilfe des Objekttyps *Bezugsobjekt* darstellen. Die konkreten Risiken werden durch einen *Fakt* repräsentiert. Als risikospezifische Fakten kommen Risikogrößen, Risikoindikatoren und Risikoschwellen in Frage. Die Risikogröße beschreibt den Umfang des Risikos z. B. hinsichtlich Eintrittswahrscheinlichkeit, Schadensausmaß oder einem Risikomaß wie dem Value at Risk (siehe Abbildung 46).

Risiko: Auftragsrückgang (Bestandskunden)		
Risikogröße: Value at Risk	**Kennzahl**	**Ausprägung**
	VaR	4.000.000
	Bezugsobjekt	**Ausprägung**
	Einheit	€
	Zeitraum	1 Jahr
	Gültig ab	01.01.2018

Abbildung 46: Darstellung eines Fakts Risikomaß

Eine weitere Spezialisierung eines Fakts stellen Risikoindikatoren dar. Sie repräsentieren Anzeichen, die z. B. auf eine erhöhte Eintrittswahrscheinlichkeit des Risikos schließen lassen (siehe Abbildung 47).

Risiko: Auftragsrückgang (Bestandskunden)		
Risikoindikator: Kundenreklamationen	**Kennzahl**	**Ausprägung**
	Beschwerden	> 3
	Periode	Tag
	Bezugsobjekt	**Ausprägung**
	Zeitraum	2 Wochen

Abbildung 47: Darstellung eines Fakts Risikoindikator

Mittels eines Fakts *Risikoschwelle* wird eindeutig definiert, ab welchen Gegebenheiten ein Risiko als eingetreten angesehen wird (siehe Abbildung 48).

Risiko: Auftragsrückgang (Bestandskunden)		
Risikoschwellenbezug: Aufträge pro Jahr	**Kennzahl**	**Ausprägung**
	$(\frac{\text{Aufträge}_t}{\text{Aufträge}_{t-1}}) * 100$	<= 75
	Bezugsobjekt	**Ausprägung**
	Einheit	%
	Zeitraum	1 Jahr

Abbildung 48: Darstellung eines Fakts Risikoschwelle

Da analog zu den Zielen auch zwischen Risiken eine hierarchische Beziehung bestehen kann, wird das Risikoobjekt weiterhin mit einem Selbstbezug (reflexive Assoziation) versehen. Aus den Anforderungen an eine Risikoerweiterung der BPMN resultierend (siehe Kapitel 7.2) und analog zu den Zielen wird mittels des Objekttyps *Risikoart* die Kategorisierung von Risiken nach Risikoarten (z. B. Finanzrisiko, Absatzrisiko etc.) ermöglicht.

Objekttyp Risikosteuerungsmaßnahme

Zur Modellierung von Risikosteuerungsmaßnahmen wird auf das in der BPMN bereits vorhandene Aufgabenelement zurückgegriffen, da eine Maßnahme einer durchzuführenden Aufgabe gleicht. Das CDME berücksichtigt, dass ein Risiko von keiner, einer oder mehreren Risikosteuerungsmaßnahmen gesteuert werden kann. Da üblicherweise der jeweilige Risk Owner für die Durchführung einer Risikosteuerungsmaßnahme verantwortlich ist, wird zwischen den beiden Objekttypen entsprechend eine Verbindung geschaffen.

Jede Maßnahme hat allgemeine (Name, Status, Kosten, Beschreibung) und spezielle Eigenschaften. Die speziellen Eigenschaften können, ebenso wie bei den Zielen und Risiken, durch Fakten und Bezugsobjekte spezifiziert werden. Mittels eines Fakts *Maßnahmengröße* lassen sich messbare Eigenschaften einer Maßnahme definieren. So kann bspw. genau festgelegt werden, ab wann eine Steuerungsmaßnahme, abhängig von einer Kennzahl, eingeleitet oder beendet wird. Im Beispiel in Abbildung 49 wird der Maßnahmenstart in Abhängigkeit von einer operativen Kennzahl gesetzt. Für die Definition eines Maßnahmenendes wird ein weiterer Fakt „Maßnahmengröße“ der Risikosteuerungsmaßnahme zugewiesen.

Maßnahme: Vier-Augen-Prinzip in der Qualitätssicherung		
Maßnahmengröße: Maßnahmenstart	**Kennzahl**	**Ausprägung**
	Beschwerden/ pro Woche	>= 20
	Bezugsobjekt	**Ausprägung**
	Risikobezug	Auftragsrückgang
	Zeitraum	1 Woche

Abbildung 49: Darstellung eines Fakts Maßnahmengröße

Sind spezielle Eigenschaften einer Risikosteuerungsmaßnahme nicht eindeutig durch einen Fakt quantifizierbar, lassen sich diese, ähnlich den Zielen und Risiken (s. o.), mittels eines Bezugsobjekts abstrakt definieren.

Objekttyp Risikofluss

Wesentlich für die Modellierung von kausalen Abfolgen – wie Risiko-Ursache-Wirkungsketten, Risiko-Maßnahmen-Beziehungen und von Prozesselementen ausgehende Risiken – sind die zwischen den Elementen liegenden Verbindungen. Zur Abbildung solcher Beziehungsstrukturen wird die BPMN um einen Objekttyp *Risikofluss* ergänzt. Dieser ermöglicht die Modellierung von kausalen Zusammenhängen. Insgesamt lassen sich neun Arten von Risikoflüssen unterscheiden. Ein einfacher Risikofluss drückt aus, dass ein Risiko, ein Prozesselement (z. B. eine Aktivität) oder eine Risikosteuerungsmaßnahme, ein anderes Risiko bzw. eine andere Maßnahme auslöst. Dabei liegt kein Einfluss auf das Ausmaß vor und die Eintrittswahrscheinlichkeit des ausgelösten Objekts liegt bei 100 %. Die weiteren Arten von Risikoflüssen dienen der Spezifizierung des Umfangs des Einflusses auf die Eintrittswahrscheinlichkeit und das Schadensausmaß eines Risikos. Die jeweiligen Attribute der spezifischen Objekttypen des Risikoflusses können jeweils Werte der „Nicht booleschen"-Ausprägungen annehmen. Dies können entsprechend qualitative (z. B. Eintrittswahrscheinlichkeit: niedrig) oder quantitative Größen (z. B. Eintrittswahrscheinlichkeit: 80 %) sein.
Die Erweiterung des BPMN Metamodells erlaubt die logische Verknüpfung der Risikoflüsse mittels der bestehenden BPMN Operatoren (Gateways). Dadurch wird eine übersichtliche Modellierung komplexer Zusammenhänge ermöglicht. Eine Modellierung von Risikoflüssen

ist ausnahmslos nur zwischen kausal abhängigen Elementen möglich. Somit werden Risikoflüsse

- zwischen Risiken,
- zwischen Risikosteuerungsmaßnahmen
- sowie zwischen Risikosteuerungsmaßnahmen und Risiken bzw. umgekehrt verwendet.

Weiterhin können Prozesselemente wie bspw. Aktivitäten oder Daten zu einem Risiko führen, so dass von diesen ein Risikofluss ausgehen kann, der in einem Risiko mündet.
Für den umgekehrten Bezug von Risiken bzw. Risikosteuerungsmaßnahmen zu Prozesselementen werden keine Risikoflüsse verwendet, da ein Risikofluss per Definition dazu dienen kann, die Art einer Wirkung zu modellieren. Als Bezug von einem Risiko zu einem Prozesselement, wie z. B. einem Datenobjekt, kommt eine solche Verbindung nicht in Frage, da das Datenobjekt z. B. keine Wahrscheinlichkeit besitzt, die gesenkt oder erhöht werden könnte. Dennoch ist es von Interesse, den Bezug eines Risikos zu den Prozesselementen, bei denen es schlagend wird, zu veranschaulichen. Für die Abbildung dieses Zusammenhangs wird daher ein weiterer Beziehungstyp benötigt (siehe Risiko-Prozessbezug).

Objekttyp Risiko-Prozessbezug

Mittels des Objekttyps *Risiko-Prozessbezug* kann modelliert werden, an welcher Stelle im Prozess ein Risiko oder eine Risikosteuerungsmaßnahme einen Einfluss auf den Prozess hat. Über den Risiko-Prozessbezug lassen sich weiterhin durch Risiken oder Risikosteuerungsmaßnahmen ausgelöste alternative Prozessverläufe modellieren. Da in der BPMN mit dem Objekttyp *Assoziation* bereits die Möglichkeit gegeben ist, Informationen und Artefakte mit dem Prozessfluss zu verknüpfen, wird der Risiko-Prozess-Bezug als Spezialisierung dieses Objekttyps in Form einer gerichteten Assoziation realisiert, um dem Ziel gerecht zu werden, möglichst wenige neue Elemente in die BPMN einzuführen.

Objekttyp Risikokorrelation

Neben kausalen Beziehungen können zwischen Risiken auch lediglich Korrelationen ohne einen kausalen Zusammenhang bestehen. Diese können durch eine eigene Risikokorrelations-

kante modelliert werden, die über den Objekttyp *Risikokorrelation* im CDME berücksichtigt wird. Der Grad der Korrelation wird in Form des Korrelationskoeffizienten als Attribut der Kante erfasst. Falls die Richtung (das Vorzeichen des Koeffizienten) der Korrelation bekannt ist, können negative und positive Korrelationsbeziehungen mithilfe spezifischer Pfeilenden an der Risikokorrelationskante ausgedrückt werden.

Objekttyp Risikolink

Aus Gründen der Übersichtlichkeit existiert in der BPMN ein Linkereignis, welches eine Verbindung von einem Prozesselement zu einem anderen erlaubt, ohne zwischen diesen beiden eine durchgehende Kante zu modellieren. So können Prozessverläufe innerhalb eines Pools auch über Lanegrenzen hinweg realisiert werden. Entsprechend wird mit dem Element des Risikolinks diese Möglichkeit sowohl für lane-, pool- als auch für prozessübergreifende Risikozusammenhänge geschaffen. Insbesondere können so auch Risiko-Ursache-Wirkungsketten zwischen Prozessen modelliert werden, die auf Prozessebene voneinander unabhängig sind, deren Risiken aber einen kausalen Zusammenhang aufweisen. Der Risikolink kann für Risikoflüsse, Risikokorrelationen und für Risiko- bzw. Maßnahmen-Prozessbezüge genutzt werden. Eine Senke kann dabei eine oder mehrere Quellen haben und eine Quelle kann zu mehreren Senken führen, falls z. B. ein Risiko in mehreren anderen Prozessen weitere Risiken auslöst.

7.5.2.3. Abstrakte Syntax

Unter Anwendung der Transformationsregeln nach Stroppi et al. (2011) wird das CDME Domänenmodell in ein BPMN+X Modell transformiert und so zu einer UML-konformen Erweiterung des BPMN Metamodells umgewandelt (siehe Abbildung 50). Die Transformation teilt sich in zwei Phasen auf.

Phase 1

Zunächst werden alle ursprünglichen BPMN Klassen und Aufzählungstypen aus dem CDME Modell in das BPMN+X Modell übernommen und als BPMN Concept betitelt. Des Weiteren werden alle Aufzählungstypen der Erweiterung in das BPMN+X Modell übernommen und als Extension Concept betitelt.

Phase 2

Zur Transformation des CDME Modells in eine gültige BPMN Erweiterung in Form eines BPMN+X Modells werden in Phase 2 Transformationsregeln angewendet.

Dabei sei C eine Klasse im CDME Modell und p eine Eigenschaft dieser Klasse vom Typ t. Der Typ t kist entweder ein Attribut der Klasse C oder von dieser aus mittels einer Assoziation zu t navigierbar. Die Abbildung von C, p und t hängt davon ab, ob C ein BPMN Concept oder ein Extension Concept ist. Des Weiteren hängt sie davon ab, ob p eine bestehende (ursprüngliche) oder eine neue Eigenschaft von C ist und ob t ein BPMN Concept (Objekt einer anderen BPMN Klasse), ein Erweiterungskonzept (Objekt einer Erweiterungsklasse) oder ein Datentyp (primitiver Datentyp oder Aufzählungstyp) ist. P gilt als ursprüngliche Eigenschaft, wenn es bereits im BPMN Metamodell eine Klasse C mit der Eigenschaft p gibt. Sonst gilt p als neue Eigenschaft.

Regel 1

Regel 1 wird angewendet, wenn p ein ursprüngliches Attribut eines BPMN Concepts ist.

1a) Wenn t ein Datentyp ist, wird p als Attribut des BPMN Elements C repräsentiert.

1b) Wenn t ein BPMN Concept ist, wird p als eine von C nach t navigierbare Assoziation repräsentiert.

Regel 2

Regel 2 wird angewendet, wenn p eine neue Eigenschaft eines BPMN Concept ist. P wird dann als „Extension Attribute Definition“ in Form einer Eigenschaft einer „Extension Definiton“ spezifiziert. Ein „Extension Definition Element“ muss dazu erzeugt werden und über eine „Extension Relationship“ mit dem BPMN Concept C verbunden werden.

2a) Wenn t ein Datentyp ist, wird p als Attribut der Extension Definition repräsentiert.

2b) Wenn t ein BPMN Concept ist, wird p als navigierbare Assoziation vom erzeugten Extension Definition Element zum bestehenden BPMN Element t repräsentiert.

2c) Wenn t ein konkretes neues Erweiterungskonzept in dem Sinne ist, dass t ein neues Element darstellt, dann ist t ein neues Erweiterungselement und p ist eine Extension Attribute Definition, die als navigierbare Assoziation von der Extension Definition zum Erweiterungselement t dargestellt wird.

Regel 3

Wenn p ein neues Attribut eines BPMN Concept ist und t ein abstraktes Extension Concept, dann wird t als Extension Defintion repräsentiert und p als Extension Relationship vom BPMN Element C zur Extension Definition t.

Regel 4

Regel 4 wird angewendet, wenn p eine Eigenschaft eines Extension Concepts ist. Also einer Extension Definition oder eines Extension Element.

4a) Wenn t ein Datentyp ist, wird p als Attribut von C dargestellt.

4b) Wenn t ein BPMN Concept ist, wird p als navigierbare Assoziation vom BPMN Element C zum Element t dargestellt.

4c) Wenn t ein Extension Concept ist, wird t als Extension Element dargestellt und p mittels einer navigierbaren Assoziation vom Element C nach t.

Regel 5

G sei eine Generalisierungsbeziehung von einer Klasse C zu einer Superklasse S. Wenn G eine ursprüngliche Generalisierungsbeziehung von einem BPMN Concept zu einem anderen BPMN Concept ist, wird G als Generalisierungsbeziehung von C nach S dargestellt.

Regel 6

Wenn G eine neue Generalisierungsbeziehung von einem BPMN Concept zu einem anderen BPMN Concept ist, wird G als ungültig angenommen und im BPMN+X Model nicht berücksichtigt, da eine solche Generalisierung vom BPMN Erweiterungsmechanismus nicht unterstützt wird.

Regel 7

Regel 7 wird angewendet, wenn G eine Generalisierungsbeziehung von einem BPMN Concept zu einem Extension Concept ist. Der BPMN Erweiterungsmechanismus folgt dem Ansatz des „Extension by addition“. Er erlaubt somit nur die dömanenspezifische Erweiterung eines ursprünglich bestehenden BPMN Elements.

Der BPMN Erweiterungsmechanismus erlaubt keine taxonomische Verbindung eines spezifischen BPMN Concept und eines übergeordneten allgemeineren Extension Concept (7a) sowie anders herum (7b). G wäre dann ungültig. Jedoch kann das Extension Concept als Extension Definition repräsentiert werden und G als eine Extension Relationship vom BPMN Element zur Extension Definition. So können die zusätzlichen Eigenschaften des Extension Concept zum BPMN Concept hinzugefügt werden.

Regel 8

Regel 8 kommt zur Anwendung, wenn G eine Generalisierungsbeziehung von einem Extension Concept C zu einem anderen Extension Concept S ist. S muss zuvor als Extension Element oder Extension Definition definiert worden sein. Dies wird gewährleistet, indem die Regeln 2c, 3 oder 4c auf die Eigenschaften, die zu S gehören, angewendet werden und die Regeln 7 oder 8 auf die Generalisationsbeziehungen die S beinhalten. C wird als Extension Element (8a) oder Extension Definition (8b) repräsentiert, abhängig davon, ob S ein Extension Element oder eine Extension Definition ist. G wird dann als Generalisierungsbeziehung vom Element C zum Element S realisiert.

Unter Anwendung der Transformationsregeln ergibt sich aus dem CDME das in Abbildung 50 dargestellte BPMN+X Modell.

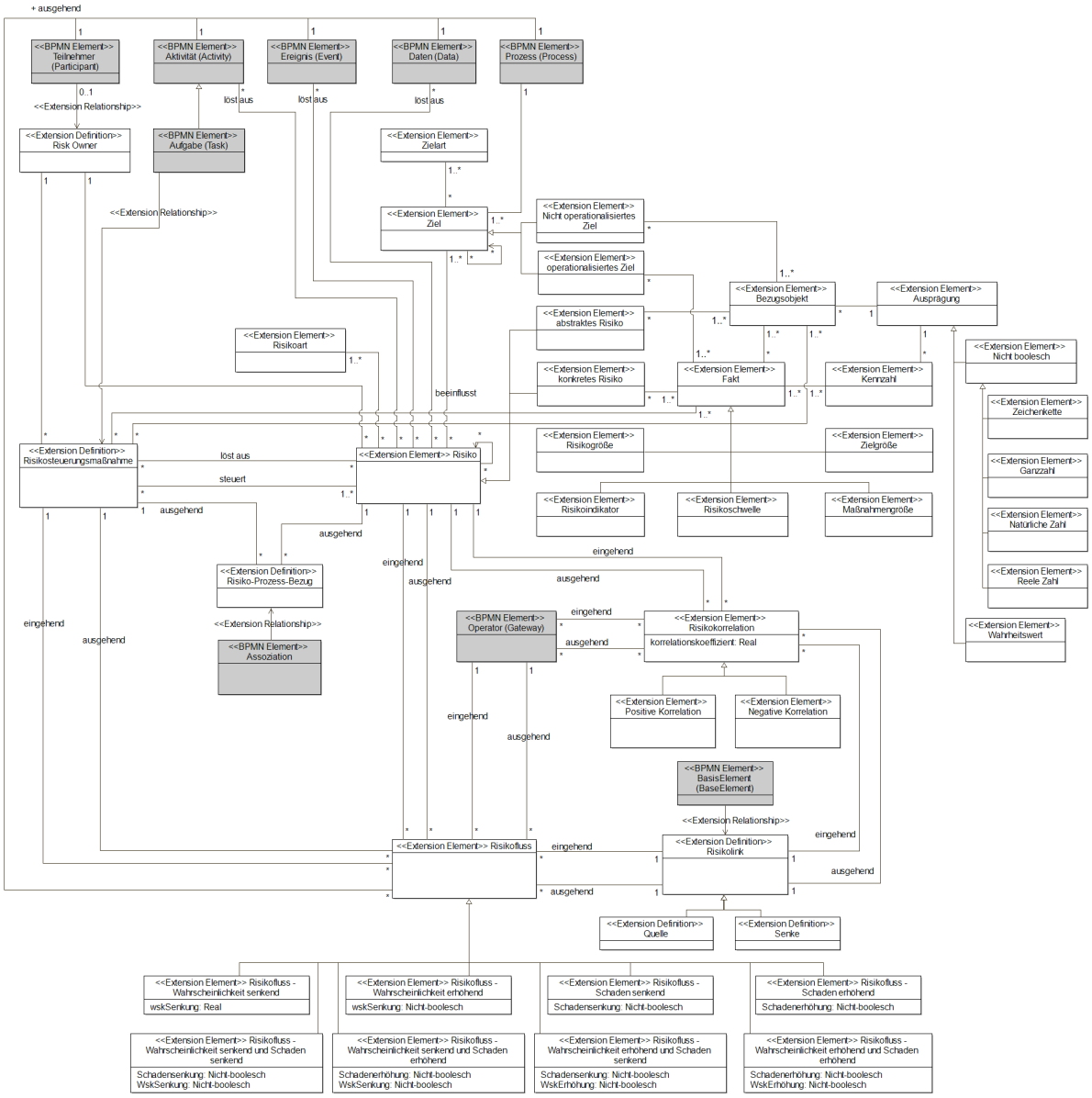


Abbildung 50: BPMN+X Modell der BPMN Erweiterung[407]

7.5.2.4. Konkrete Syntax

Damit grafische Modelle mit der vorgestellten Erweiterung erzeugt werden können, ist eine konkrete Syntax zu definieren, welche eine visuelle Repräsentation der neuen Risikoelemente im BPMN Prozessmodell ermöglicht. Im Wesentlichen wird die BPMN dazu um lediglich sechs neue Symbole, die eine Modellierung aller prozessbezogenen Risikophänomene erlauben, ergänzt. Es werden Symbole zur Modellierung von Risiken, Risikoflüssen, Risikokorre-

[407] Die Abbildung befindet sich in einer größeren Auflösung im Anhang dieser Arbeit.

lationen, Risikolinks und Risikosteuerungsmaßnahmen eingeführt (siehe Abbildung 51). Auf die grafische Darstellung der Prozessziele wird verzichtet, um das Prozessmodell nicht zu überladen. In einer informationstechnischen Umsetzung des Modells ist es z. B. denkbar, dass die Prozessziele über ein Kontextmenü des dargestellten Prozessmodells aufgerufen werden können.

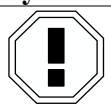
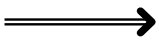
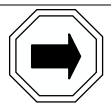
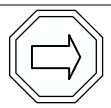
Bezeichnung	Symbol
Risiko	 Risiko
Risikofluss	
Risikokorrelation	
Risikolinkquelle	 Risikolink
Risikolinksenke	 Risikolink
Risikosteuerungsmaßnahme	 Maßnahme

Abbildung 51: Symbole der BPMN Erweiterung

Zur Modellierung von Risiken im Geschäftsprozessmodell, gemäß den in 7.2 und 7.3 spezifizierten Anforderungen, wird ein Risikosymbol eingeführt. Es wird durch ein Achteck mit gefülltem Ausrufezeichen nebst Risikobezeichnung repräsentiert. Ein Risiko wird innerhalb der BPMN Swimlane dargestellt, in welcher es initial Prozessflusselemente beeinflusst bzw. von diesen verursacht wird. Zur Abbildung von Beziehungsstrukturen dient der Risikofluss. Dieser ermöglicht die Modellierung von kausalen Zusammenhängen und wird mit einer gerichteten Doppellinienkante dargestellt. In Abhängigkeit der Wirkungsbeziehung kann ein Risiko-

fluss unterschiedliche Anfangs- und Endpfeiltypen annehmen, so dass insgesamt neun Typen von Risikoflüssen zu unterscheiden sind (siehe Abbildung 52).

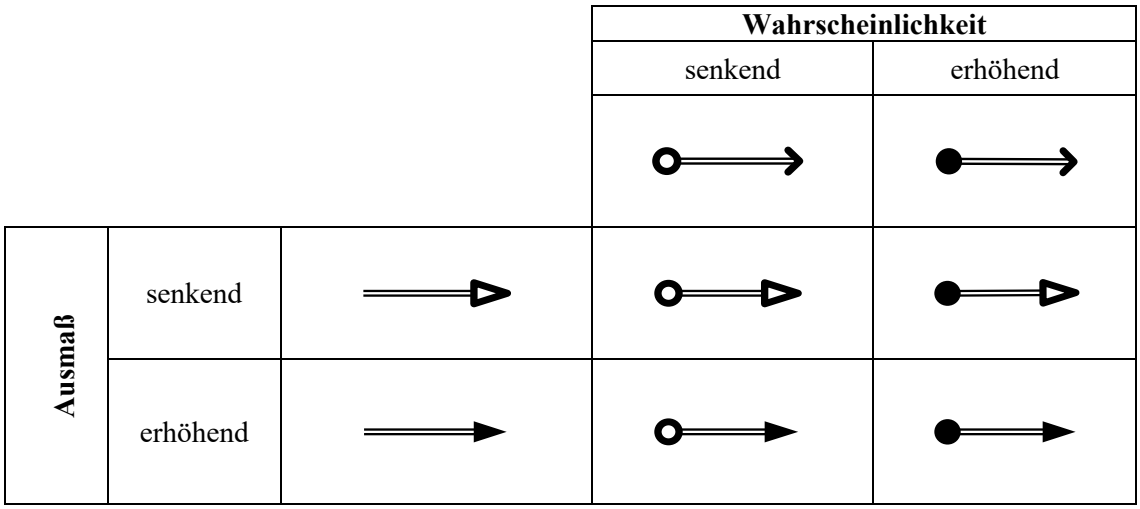


Abbildung 52: Mögliche Pfeiltypen eines Risikoflusses

Im Zusammenspiel der Risikoflüsse und Logikoperatoren ergeben sich die folgenden Modellierungsmöglichkeiten für Ursache-Wirkungsbeziehungen. Der in den Beispielen verwendete Standard Risikofluss stellt eine Sonderausprägung der Pfeiltypen mit 100 % Eintrittswahrscheinlichkeit des Folgerisikos dar.

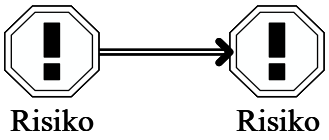


Abbildung 53: Ein Risiko löst ein weiteres Risiko aus.

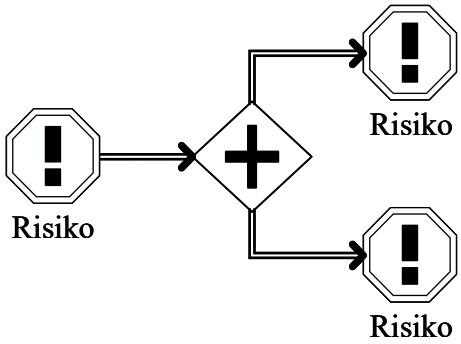


Abbildung 54: Ein Risiko löst zwei weitere Risiken aus.

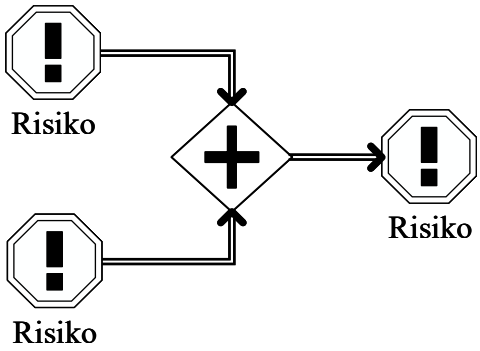


Abbildung 55: Zwei Risiken lösen zusammen ein drittes Risiko aus.

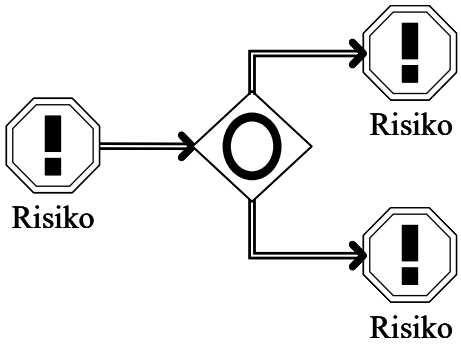


Abbildung 56: Ein Risiko löst entweder ein oder zwei weiteren Risiken aus.

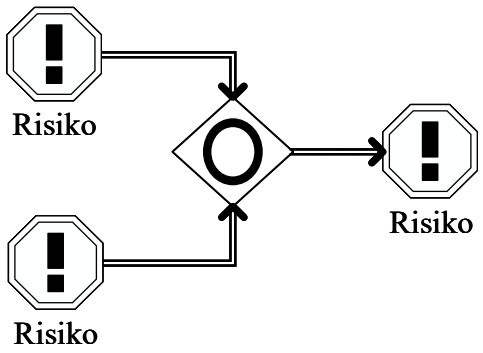


Abbildung 57: Ein Risiko allein oder zwei zusammen lösen ein drittes Risiko aus.

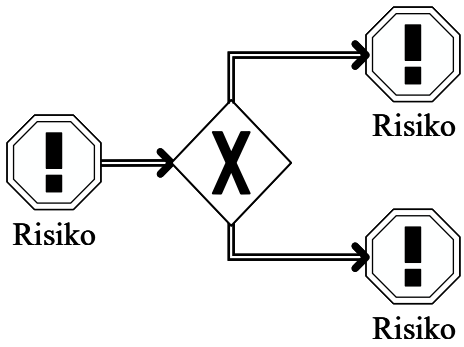


Abbildung 58: Ein Risiko löst entweder das eine oder das andere Risiko aus.

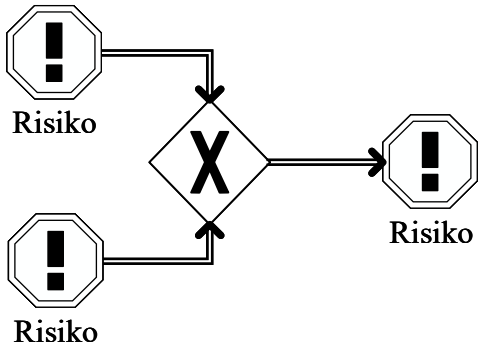


Abbildung 59: Entweder das eine oder das andere Risiko lösen ein drittes Risiko aus.

Zur Verdeutlichung der Wirkungsbeziehung eines Risikos oder einer Risikosteuerungsmaßnahme zu einem Prozesselement wird der Risiko- bzw. Maßnahmen-Prozessbezug eingeführt, der durch eine gepunktete, gerichtete Kante dargestellt wird (siehe Abbildung 60). Diese exis-

tiert in der BPMN bereits zur Darstellung von Assoziationen und ist daher kein neues Element der Erweiterung.

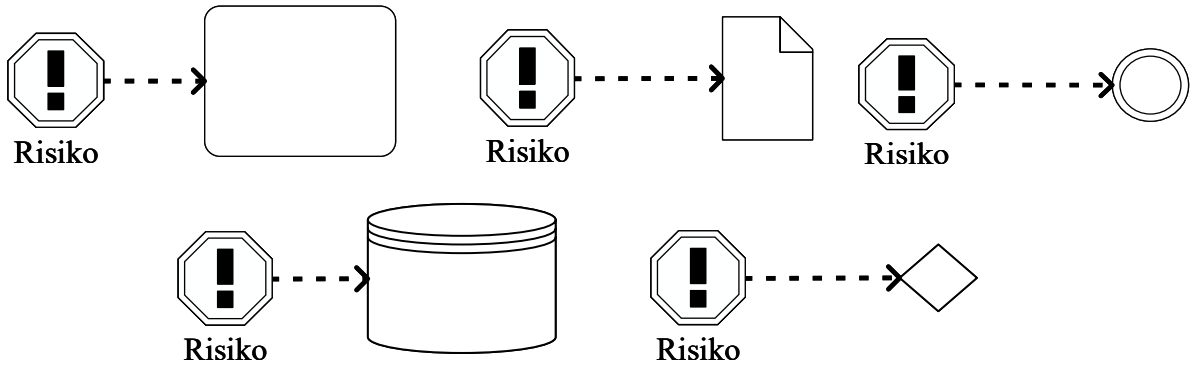


Abbildung 60: Bezug eines Risikos zu Prozessflusselementen[408]

Da ein Risiko aus einem Prozessflusselement heraus entstehen kann (z. B. aus einer Aktivität heraus), ist diese Beziehung ebenfalls modellierbar (siehe Abbildung 61).

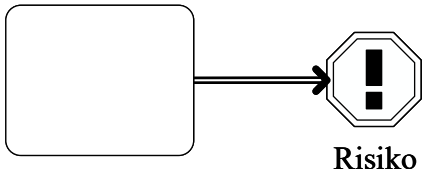


Abbildung 61: Prozessflusselement Aufgabe verursacht Risiko

Korrelationen zwischen Risiken werden mittels der Risikokorrelationskante repräsentiert. Diese wird durch eine gestrichelte Doppellinienkante visualisiert (siehe Abbildung 62).

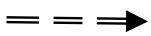
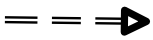
Positive Korrelation	Negative Korrelation
	

Abbildung 62: Mögliche Typen einer Risikokorrelation

Falls die Richtung der Korrelation bekannt ist, wird dies durch unterschiedliche Pfeilenden dargestellt (siehe Abbildung 62 und Abbildung 63).

[408] Zur Erläuterung der BPMN Elemente siehe Abbildung 23: Basiselemente der BPMN.

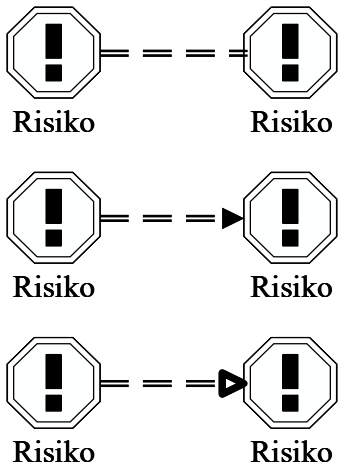


Abbildung 63: Darstellung von Risikokorrelationen

Der Risikolink zur Realisierung von Sprüngen im Prozess bzw. zwischen Prozessen wird durch ein Achteck mit einem nach rechts gerichtetem Pfeil dargestellt. Falls es sich um eine Risikolinkquelle handelt, ist der Pfeil schwarz gefüllt. Im Falle einer Risikolinksenke ist der Pfeil nicht gefüllt (siehe Abbildung 64). Die eindeutige Bezeichnung des Risikolinks wird sowohl an der Quelle als auch an der Senke per Textannotation vermerkt (hier im Beispiel *Risikolink*).

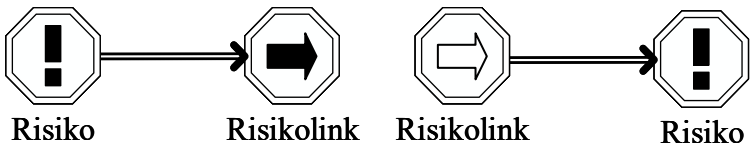


Abbildung 64: Darstellung einer Risiko-Ursache-Wirkungsbeziehung über Risikolink

Risikosteuerungsmaßnahmen basieren auf dem bestehenden Aufgabensymbol aus der BPMN. Dieses wird lediglich durch ein von einem Dreieck umrandetes Ausrufezeichen ergänzt, um die Aufgabe eindeutig als Risikosteuerungsmaßnahme zu spezifizieren.

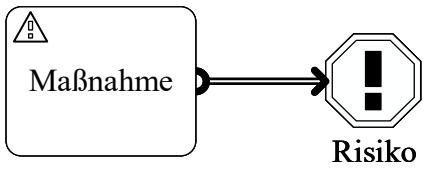


Abbildung 65: Risikosteuerungsmaßnahme senkt Eintrittswahrscheinlichkeit.

Idealerweise wirken Risikosteuerungsmaßnahmen auf die Risiken ein, indem die Eintrittswahrscheinlichkeit des Risikos (siehe Abbildung 65) oder das Schadensausmaß (siehe Abbildung 66) gesenkt werden.

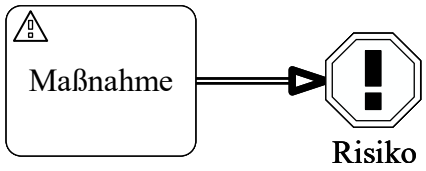


Abbildung 66: Risikosteuerungsmaßnahme senkt das Schadensausmaß.

Es ist jedoch auch denkbar, dass durch eine Risikosteuerungsmaßnahme neue Risiken ausgelöst werden (siehe Abbildung 67).

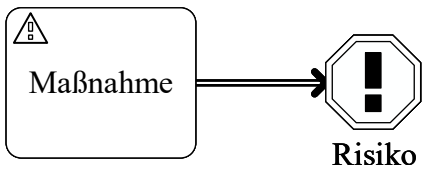


Abbildung 67: Risikosteuerungsmaßnahme löst neues Risiko aus.

Risikosteuerungsmaßnahmen liegen klare Start- und Endbedingungen zugrunde. Diese werden aus Gründen der Übersichtlichkeit in der konkreten Syntax nicht visualisiert.

7.5.3. Anwendungsbeispiel

Die Modellierung von Risikophänomenen auf Basis der eingeführten BPMN Erweiterung wird anhand eines Beispiels erläutert (siehe Abbildung 68). In diesem stehen der Wareneingangs- und der Fertigungsprozess eines produzierenden Unternehmens im Mittelpunkt.
Zunächst wird der Wareneingangsprozess betrachtet. Das Ziel des Prozesses ist die sachgemäße Verbuchung und Einlagerung qualitativ einwandfreier Warenlieferungen. Beim Eintref-

fen von neuen Warenlieferungen in der Warenannahme ist die Verpackung auf Beschädigungen zu prüfen. Sind keine äußeren Beschädigungen erkennbar, wird der Lieferschein mit der Warenlieferung abgeglichen. Sind äußere Beschädigungen erkennbar, erfolgt eine Prüfung des Inhalts hinsichtlich etwaiger Beschädigungen.

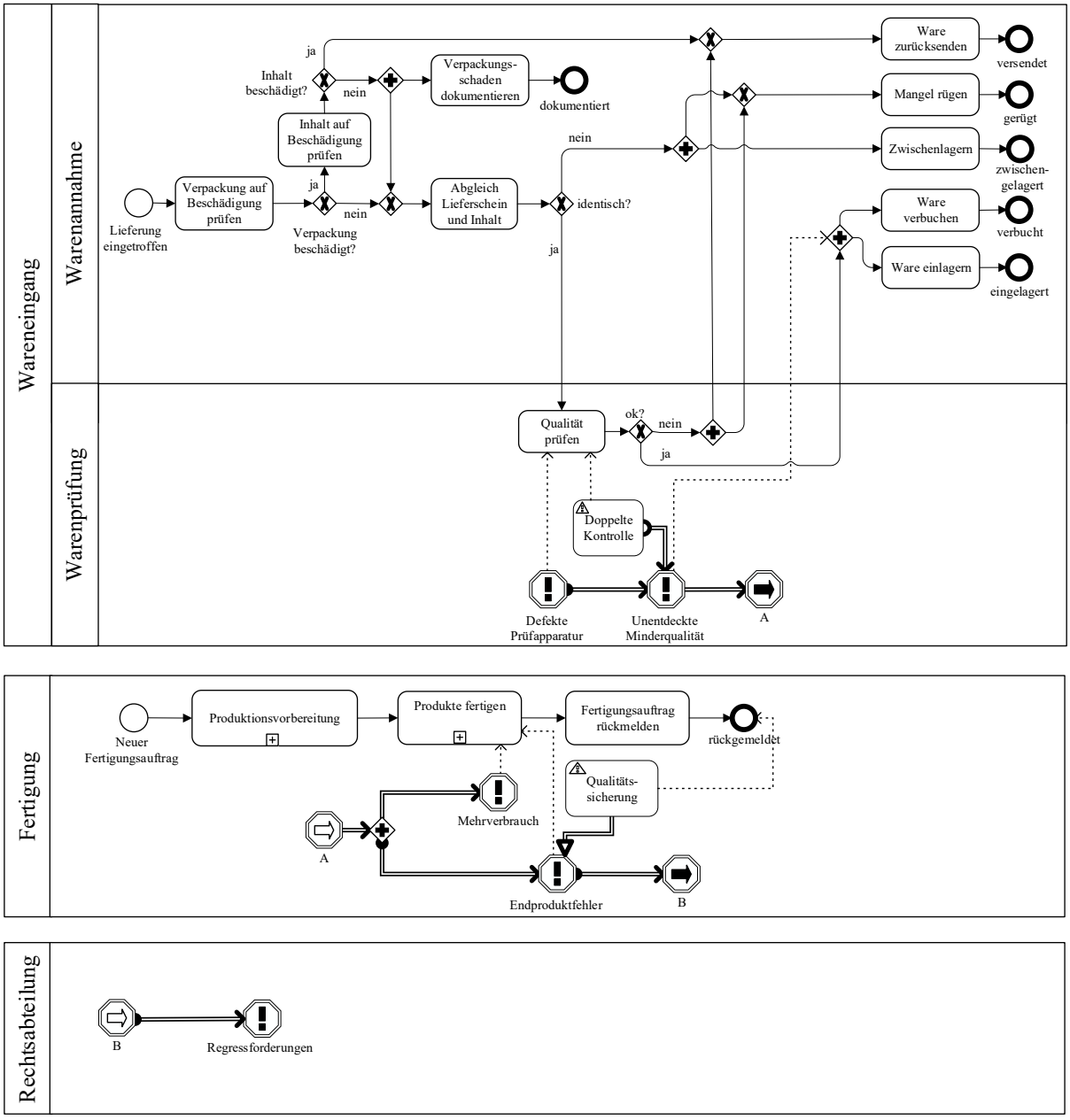


Abbildung 68: Prozess- und Risikosicht von Wareneingang und Fertigung

Falls die Ware beschädigt ist, wird diese zurückgesendet. Sind keine Schäden an der gelieferten Ware erkennbar, wird der Verpackungsschaden dokumentiert und es wird ein Abgleich zwischen Lieferschein und gelieferter Ware vorgenommen. Falls der Lieferschein mit der Lieferung nicht übereinstimmt, wird dieser Mangel gerügt und die Lieferung bis zur Klärung mit dem Lieferanten zwischengelagert. Sind Lieferschein und Lieferung identisch, erfolgt die Qualitätsprüfung. Gibt es Beanstandungen hinsichtlich der Qualität der Ware, so wird der Mangel gerügt und die Ware zurückgesendet. Entspricht die Ware den Qualitätsanforderungen, wird die Lieferung verbucht und eingelagert.

Ein potentielles Risiko besteht zunächst in einer defekten Prüfapparatur, welche im Rahmen der Qualitätsprüfung falsche Messwerte liefert. Da ein Prüfer von korrekten Messwerten ausgeht, erhöht dieses Risiko die Eintrittswahrscheinlichkeit des Risikos *Unentdeckte Minderqualität*. Zwischen den beiden Risiken besteht eine Ursache-Wirkungsbeziehung. Die Risiko-Prozessbezug Kante vom Risiko *Defekte Prüfapparatur* zur Prozessfunktion *Qualität prüfen* macht deutlich, dass dieses Risiko auf diese Funktion wirkt. Bleibt das Folgerisiko *Unentdeckte Minderqualität* unbemerkt, dann wirkt sich dieses Risiko darin aus, dass der Prozess fälschlicherweise mit dem Verbuchen und Einlagern der Ware fortgeführt wird, wenn das Risiko eintritt. Dies wird mittels der Risiko-Prozessbezug Kante von diesem Risiko zum Und-Gateway vor den Funktionen *Ware verbuchen* und *Ware einlagern* dargestellt. Weiterhin führt das Risiko *Unentdeckte Minderqualität* in einem späteren Fertigungsprozess, der eine qualitativ einwandfreie Fertigung von Produkten zu einem festen Selbstkostensatz zum Ziel hat, zu weiteren Risiken. Diese prozessübergreifende Risiko-Ursache-Wirkungskette wird mittels des Risikolinks mit der Bezeichnung *A* modelliert. Im Beispiel wird auf die Eintrittswahrscheinlichkeit des Risikos *Unentdeckte Minderqualität* durch die Risikosteuerungsmaßnahme *Doppelte Kontrolle* eingewirkt. Durch eine weitere ggf. stichprobenmäßige Kontrolle der Qualität mit einer anderen Prüfapparatur, zielt die Maßnahme auf die Minderung der Eintrittswahrscheinlichkeit des Risikos ab. Mittels des Maßnahmen-Prozessbezugs wird deutlich gemacht, dass die Maßnahme *Doppelte Kontrolle* sich auf das Prozessflusselement *Qualität prüfen* bezieht. Die Darstellung als Risikosteuerungsmaßnahme verdeutlicht, dass die Maßnahme während dieses Prozessschrittes als Risikomanagementaktivität losgelöst vom eigentlichen Prozess durchgeführt wird. Für alle Risikosteuerungsmaßnahmen ist anzumerken, dass diese in Abhängigkeit von bestimmten Bedingungen aktiviert werden können (z. B. bei Über-

schreiten eines Schwellenwertes oder in Abhängigkeit von einem Zeitpunkt). Das bedeutet, dass sie ggf. nicht bei jedem Prozessdurchlauf durchgeführt werden. Möchte man eine Maßnahme als dauerhaftes Risikosteuerungselement in einen Prozess integrieren, so empfiehlt sich eine Neugestaltung des Prozesses, in deren Zuge die Maßnahme als Teil des Prozesses in Standard BPMN Notation modelliert wird und nicht als Risikosteuerungsmaßnahme.

Wird die Minderqualität im Beispielprozess nicht erkannt, führt dies im Fertigungsprozess in jedem Fall zu einem Mehrverbrauch, der letztlich die Kosten der Fertigung erhöht, da mehr Material verbraucht wird. Des Weiteren erhöht sich durch die Minderqualität die Eintrittswahrscheinlichkeit, dass ein Endprodukt fehlerbehaftet ist und gegebenenfalls nicht in vorgesehener Weise funktioniert, so dass bei Verwendung durch den Kunden Fehler oder Schäden auftreten können. Aus dem Risiko kann ein Risiko *Regressforderungen* resultieren. Diesem wird im Beispiel nicht begegnet, so dass dieses Risiko akzeptiert wird. Eine mögliche Risikosteuerungsmaßnahme für dieses Risiko wäre der Abschluss einer Versicherung. Zur Reduzierung des Schadensausmaßes des Risikos *Endproduktfehler* werden zusätzliche Qualitätssicherungsmaßnahmen in der Fertigung durchgeführt. Der Risiko-Prozessbezug von der Maßnahme *Qualitätssicherung* zum Endereignis *rückgemeldet* macht deutlich, dass die Qualitätssicherungsmaßnahme nach Rückmeldung eines Fertigungsauftrags durchgeführt wird. Als Maßnahme des Risikomanagements erfolgt dies wiederum losgelöst vom eigentlichen Fertigungsprozess und somit ggf. nur stichprobenartig in Abhängigkeit von den zugrunde liegenden Start- und Endbedingungen der Maßnahme. Das Beispiel verdeutlicht insbesondere wie mit der risikoorientierten Prozessnotation prozessübergreifende Risiko-Ursache-Wirkungsketten modelliert werden können. Eine defekte Prüfapparatur kann über die Risiko-Ursache-Wirkungskette bis zu Regressforderungen führen.

Teil III: IT-gestütztes Risikomanagement

8. Risikomanagement-Informationssysteme

8.1. Überblick

In der Literatur werden uneinheitliche Bezeichnungen für Informationssysteme verwendet, die den Umgang mit Risiken unterstützen. Dabei werden zum einen die Begriffe Risikoinformationssystem und Risikomanagement-Informationssystem synonym für IT-gestützte Systeme zur Unterstützung des Risikomanagements verwendet. Zum anderen werden aber auch nicht IT-gestützte Systeme, die einen Überblick über die Risikolage ermöglichen, als Risikoinformationssystem bezeichnet.[409] Zum einheitlichen Verständnis wird im Rahmen dieser Arbeit ein IT-System, welches allein zur Unterstützung des Risikomanagements konzipiert wurde, als Risikomanagement-Informationssystem (RMIS) bezeichnet.

Im Allgemeinen zielt der Einsatz IT-gestützter betrieblicher Informationssysteme darauf ab, die unternehmensweite Erfassung, Verarbeitung und Speicherung von Daten zu erleichtern und diese effizient zur Verfügung zu stellen. Die Systeme sorgen für durchgängige Informationsströme entlang des Wertschöpfungsprozesses und somit über Funktionsbereiche hinweg. Sie stellen mit unterschiedlichen Detailierungsgraden eine Integration von mengen- und wertorientierten Sichten der operativen Bereiche hin zu Planungs- und Entscheidungsunterstützungssystemen dar.[410] Darüber hinaus ermöglichen insbesondere integrierte Informationssysteme, dass eine redundante Datenhaltung vermieden wird und das System sich zum Datenaustausch mit anderen unternehmensinternen und -externen Informationssystemen über Schnittstellen verbinden lässt.

Aus den Ausführungen in den Kapiteln 3 und 4 wird ersichtlich, dass eine IT-Unterstützung des Risikomanagements als nahezu unabdingbar erscheint. Insbesondere die Komplexität der Risikophänomene, die zum einen in jedem Funktionsbereich eines Unternehmens auftreten können und zum anderen nur schwer von einzelnen Personen in vollem Umfang organisationsweit überblickt werden können,[411] erfordert den Einsatz spezieller IT-Systeme. Vor allem in global tätigen Unternehmen ist die Informationsverarbeitung im Rahmen des Risikomanagements nur mithilfe einer geeigneten IT-Unterstützung zu leisten, da Risiken mit einer gro-

[409] Vgl. Yaraghi und Langhe 2011, S. 551 f.
[410] Vgl. Scheer 1994, S. 4 ff.
[411] Vgl. Erben und Romeike 2002, S. 561.

ßen und komplexen Datenmenge von Ereignissen einhergehen und unterschiedlichen Verantwortlichkeiten unterliegen.[412] Somit wird mit dem Einsatz von RMIS das Ziel verfolgt, die Aufgabenerfüllung des Risikomanagements effektiv zu unterstützen.

8.2. Anforderungen an Risikomanagement-Informationssysteme

Zur zielführenden Unterstützung der Aufgabenerfüllung des Risikomanagements sollte ein Risikomanagement-Informationssystem zum einen jede Phase des Risikomanagements möglichst umfänglich unterstützen und zum anderen organisatorische Aspekte abbilden können, damit es nahtlos in jegliches Unternehmen eingebunden werden kann. Zusätzlich muss es den technischen Anforderungen an moderne Informationssysteme genügen. Insgesamt lassen sich die Anforderungen an RMIS in

- methodisch-inhaltliche,
- organisatorische und organisationsrechtliche
- sowie technische Anforderungen

untergliedern.[413] Die methodisch-inhaltlichen Anforderungen umfassen die zur Unterstützung des Risikomanagements notwendigen Funktionen. Sie ergeben sich aus den Phasen des Risikomanagements. Die organisatorischen und organisationsrechtlichen Anforderungen beziehen sich auf Aspekte, die sich aus der Unternehmensstruktur[414] und gesellschaftsrechtlichen Vorgaben ergeben. Zu den technischen Anforderungen zählen die Anforderungen an das IT-System wie z. B. die Integrationsfähigkeit in die bestehende Systemlandschaft.[415]

8.2.1. Methodisch-inhaltliche Anforderungen

8.2.1.1. Anforderungen zur Unterstützung der Risikoidentifizierung

Wesentliche Aufgaben der Risikoidentifizierungsphase sind die frühzeitige und möglichst vollständige Entdeckung potentieller Risiken sowie die strukturierte Erfassung und Dokumentation ihrer Ursache- und Wirkungszusammenhänge untereinander.[416] Zur Erstellung eines

[412] Vgl. Barateiro und Borbinha 2012, S. 676.
[413] Vgl. Meletiadou et al. 2009, S. 4.
[414] Vgl. Jahnke und Thomas 2004, S. 21.
[415] Vgl. Erben und Romeike 2002, S. 568.
[416] Vgl. Hasenmüller 2009, S. 135 f.; Paetzmann 2012, S. 68.

Gesamtüberblicks über die Unternehmensrisiken, dem sogenannten Risikokatalog, wird ein Satz an Erkennungsmethoden benötigt, um Risiken effizient und einfach identifizieren und erfassen zu können (siehe Kapitel 4.2.2).[417] Analytische Methoden wie die Fehlermöglichkeits- und Einflussanalyse (FMEA) sind durch eine strukturierte und generisch anwendbare Vorgehensweise charakterisiert, die kein Risikospezialwissen benötigt. Kollektionsmethoden wie z. B. vordefinierte Checklisten benötigen hingegen ex ante viel Risikowissen.[418] Sie leiten die Anwender bei der Risikoerfassung an, indem sie einen bereits vordefinierten, umfassenden Katalog an Risiken, evtl. spezialisiert auf bestimmte Branchen, bereitstellen, aus dem von den Anwendern entsprechend der speziellen Unternehmenssituation die zutreffenden Risiken ausgewählt werden können. Insbesondere Kollektionsmethoden erscheinen für die Unterstützung der Risikoidentifizierung durch ein RMIS als sinnvoll, da sie für bestimmte Branchen und Risikoarten bereits vordefinierte potentielle Risiken zur Auswahl anbieten können. Für die anderen Methoden existieren vielfach bereits spezifische Programme, die für die Risikoidentifizierung genutzt werden können, oder sie sind nur bedingt für eine Softwareunterstützung geeignet (z. B. Brainstorming), so dass eine Unterstützung durch RMIS nicht notwendig bzw. nicht sinnvoll erscheint.

Da sich nicht alle Risiken überhaupt bzw. in angemessener Zeit mittels der aufgeführten Identifizierungsmethoden erkennen lassen, bietet es sich an, dass das RMIS Unterstützungsfunktionen bietet, welche die Analyse historischer Daten (z. B. aus einem ERP-System) mithilfe moderner Data und Process Mining Methoden ermöglichen. Auf diese Weise können Risikomuster (z. B. regelmäßig erhöhte Durchlaufzeit einer Aktivität, wenn bestimmte Ressourcen beteiligt sind) in den Datenbeständen entdeckt werden, die manuell gar nicht oder nur mit sehr hohem Aufwand erkannt werden können.[419]

Unabhängig von der gewählten Identifizierungsmethode sind die entdeckten Risiken am Ende der Risikoidentifizierungsphase mit ihren Stammdaten zu dokumentieren. Für diese Erfassung werden im RMIS Datenerfassungsfunktionen benötigt, welche die Stammdaten der Risiken so strukturiert abfragen, dass die ordnungsgemäße Speicherung aller bereits bekannten Charakteristika des Risikos sichergestellt ist. Dazu gehören u. a. eine eindeutige Risikobezeichnung, eine verbale Beschreibung, die Risikokategorie, der Risikoverantwortliche, die Risikoursa-

[417] Vgl. Wolf und Runzheimer 2009, S. 43.
[418] Vgl. Burger und Buchhart 2002, S. 88.
[419] Vgl. Caron et al. 2013, S. 464 ff.; Wu et al. 2014, S. 1 ff.

chen, die Risikowirkungen und bestehende Interdependenzen zwischen den Risiken.[420] Als strukturelle Hilfe sollten vom RMIS geeignete Datentypen vorgegeben und die Eingabe bestimmter Eigenschaften, wie bspw. die Risikobezeichnung, als Pflichteingaben erzwungen werden.

Da Risikoursachen in einem frühen Entwicklungsstadium erfolgsversprechender beeinflusst werden können,[421] sollte das Informationssystem über Erinnerungsfunktionen verfügen, die regelmäßig zur Risikoidentifizierung bzw. Erfassung auffordern. Weiterhin sollte das RMIS daran erinnern, die bereits erfassten Risiken regelmäßig auf ihre Aktualität hin zu überprüfen, da sich im Zeitverlauf Risiken gegebenenfalls verändern.[422] So kann von einem stets aktuellen Risikokatalog ausgegangen werden. Idealerweise ist der Erinnerungs-Turnus konfigurierbar.

Theoretische Anforderung	**Geforderte Funktionalität**
Vollständige Entdeckung potentieller Risiken unter Berücksichtigung einer wirtschaftlichen Erhebung	• Bereitstellung von Identifizierungsmethoden, insbesondere analytische Methoden z. B. FTA und FMEA sowie Kollektionsmethoden z. B. Checklisten • Data und Process Mining Analysen zur Unterstützung der Identifizierungsphase
Erfassung von Risiko-Ursachen, Risiko-Wirkungen und Wirkungszusammenhängen	• Strukturierte Erfassung der Risikostammdaten • Erfassung der Risikobeziehungen • Vorgabe von Datentypen und Pflichtfeldern
Frühzeitige und permanente Identifizierung von Risiken	• (Konfigurierbare) Erinnerungsfunktionen zur Sicherstellung einer regelmäßigen Identifizierung neuer Risiken und Aktualisierung des Risikokatalogs

Abbildung 69: Anforderungen zur Unterstützung der Risikoidentifizierung

[420] Vgl. Piaz 2002, S. 77 f.; Kajüter 2012, S. 163.
[421] Vgl. Siepermann 2008, S. 37 f.
[422] Vgl. Hornung et al. 1999, S. 320.

8.2.1.2. Anforderungen zur Unterstützung der Risikoquantifizierung

Jedes Risiko unterliegt im Grunde einer Wahrscheinlichkeitsverteilung, die jedem Schadensausmaß eine entsprechende Eintrittswahrscheinlichkeit zuordnet. Sind beide zahlenmäßig bekannt, kann zur Quantifizierung eines Einzelrisikos der Schadenerwartungswert als Produkt der beiden Größen berechnet werden.[423] Sind beide Größen nicht unmittelbar bekannt, können sie bei Vorliegen historischer Daten mittels zeitreihenanalytischer Prognosemodelle prognostiziert oder mittels Simulationsverfahren angenähert werden.[424] Liegt (dann) eine Wahrscheinlichkeitsverteilung vor, lassen sich Risiken über Risikomaße wie dem Value at Risk beschreiben und vergleichbar machen.[425] In einem RMIS sollten daher Schadensausmaß und Eintrittswahrscheinlichkeit als Moment einer Wahrscheinlichkeitsverteilung durch den Anwender für die jeweiligen Risiken definierbar sein, Verteilungsfunktionen frei definiert werden können sowie gängige Verteilungsfunktionen durch das RMIS zur Auswahl angeboten werden.[426] Die Bestimmung von Verteilungsfunktionen mittels Simulation und die aus ihnen zu berechnenden Risikomaße sollten ebenfalls unterstützt werden.

Da vielfach keine objektiven Verteilungsinformationen vorliegen, ist es notwendig, dass das RMIS im Rahmen der Quantifizierung auch Verfahren zur Erfassung und weiteren Verarbeitung von subjektiven Einschätzungen unterstützt. Dazu muss es möglich sein, sowohl für Eintrittswahrscheinlichkeit als auch Schadensausmaß qualitative Beschreibungen zu wählen. Um hierbei eine annähernde Quantifizierung zu erreichen, sollten die verbal beschriebenen qualitativen Einschätzungen einer Wertklasse zugeordnet werden können. Da zwischen Risiken Abhängigkeitsstrukturen bestehen können, muss es möglich sein diese Wechselwirkungen zu quantifizieren. Entsprechend sollten RMIS die Quantifizierung von Risikointerdependenzen ermöglichen. Zur quantitativen Darstellung des Gesamtrisikos eignen sich wieder Kennzahlen wie der Value at Risk,[427] auf dessen Basis dann die Beurteilung vorgenommen werden kann.

---

[423] Vgl. Burger und Buchhart 2002, S. 42.
[424] Vgl. Löhr 2010, S. 90.
[425] Vgl. Hoitsch und Winter 2004, S. 240 ff.
[426] Vgl. Gleißner und Romeike 2005a, S. 246.
[427] Vgl. Gleißner und Meier 1999, S. 926.

Theoretische Anforderung	Geforderte Funktionalität
Festlegen von Eintrittswahrscheinlichkeit und Schadensausmaß eines Risikos zur Quantifizierung von Einzelrisiken	• Explizite Werteingabe für Wahrscheinlichkeit und Schadensausmaß (Moment einer Verteilung) • Möglichkeit, bekannte Verteilungen zu definieren • Auswahlmöglichkeit gängiger Verteilungen (z. B. Normalverteilung) • Verteilungsbestimmung auf Basis historischer Daten des Unternehmens und per Monte Carlo Simulation • Unterstützung subjektiver Einschätzungen • qualitative Einschätzungen mittels Zuordnung verbaler Beschreibungen zu numerischen Werten (z. B. Klassenbildung oder Fuzzy-System[428]) • Vorgabe von Datentypen und Pflichtfeldern
Bestimmung geeigneter Risikokennzahlen[429]	Risikoerwartungswert, Maximum Possible Loss, Value at Risk, Cashflow at Risk, Durchschnittlicher Risikowert
Berücksichtigung von Wechselwirkungen	Durchführung von Sensitivitäts- und Szenarioanalysen, Monte Carlo Simulation unter intellektueller Angabe des Grades der wechselseitigen Beziehung[430]
Quantifizierung des Gesamtrisikos	Risikoaggregation mittels Monte Carlo Simulation[431], Bestimmung gemeinsamer Verteilungen[432]

Abbildung 70: Anforderungen zur Unterstützung der Risikoquantifizierung

[428] Vgl. Eickemeier 2002, S. 664 ff.
[429] Vgl. Siepermann 2008, S. 28.
[430] Vgl. Wolf 2003, S. 565 ff.
[431] Vgl. Wolf 2003, S. 565 ff.
[432] Vgl. Beck et al. 2006, S. 29 ff.

8.2.1.3. Anforderungen zur Unterstützung der Risikobeurteilung

Im Rahmen der Risikobeurteilung wird festgelegt, welche Risiken aufgrund ihres Gefährdungspotentials für die weitere Unternehmensentwicklung dringlicher betrachtet werden müssen als andere.[433] Die Beurteilung erfolgt in Kategorien (wie z. B. wesentlich, unwesentlich), um eine Rangordnung für die einzuleitenden Steuerungsmaßnahmen erstellen zu können.[434] Auf Basis dieser Einstellung werden Schwellenwerte in adäquaten Messgrößen definiert, die helfen das Risiko bei Überschreitung als wesentlich einzustufen.[435] Zur Unterstützung dieser Aufgaben muss ein RMIS notwendigerweise die Möglichkeit bieten, Wesentlichkeitsgrenzen zu definieren. Darauf aufbauend ist die Bildung von Kategorien bzw. Risikorangordnungen zu ermöglichen.

Aufgrund der Beliebtheit der Risikomatrix zur Visualisierung der Risikolage (siehe Kapitel 4.4.2) bietet es sich an, dass eines solche Darstellung von einem RMIS bereitgestellt wird und gegebenenfalls auf ihre eingeschränkte Aussagekraft hingewiesen wird.

Die einzelnen und aggregierten Risikogrößen sowie etwaige Risikokennzahlen wie der Value at Risk sollten ergänzend zur Risikomatrix anschaulich aufbereitet dargestellt werden, damit sie vom Anwender auf einen Blick verglichen und beurteilt werden können. Dies kann mithilfe sogenannter Dashboards erfolgen, welche die Risikoinformationen hoch verdichtet und übersichtlich visualisieren.

---

[433] Vgl. PwC 1999, S. 11; Rücker 1999, S. 109.
[434] Vgl. Diederichs et al. 2004, S. 192.
[435] Vgl. zur Definition von Schwellenwerten Burger und Buchhart 2002, S. 47 f.

Theoretische Anforderung	Geforderte Funktionalität
Bewertung von Einzelrisiken und Gesamtrisiko	• Definition von Schwellenwerten zur Ermöglichung einer Beurteilung • Möglichkeit der Bildung von Wesentlichkeitsklassen auf Basis der definierten Schwellenwerte (Priorisierung) • Übersichtliche Gegenüberstellung aller quantifizierten Risiken bzw. ermittelter Risikokennzahlen zur besseren Vergleichbarkeit • Dashboard und Risikomatrix zur Visualisierung • Manuelle Priorisierungsmöglichkeit von Risiken hinsichtlich ihrer Wesentlichkeit

Abbildung 71: Anforderungen zur Unterstützung der Risikobeurteilung

8.2.1.4. Anforderungen zur Unterstützung der Risikosteuerung

Ein RMIS kann die Risikosteuerung sinnvoll unterstützen, indem für die jeweiligen Steuerungsstrategien ein editierbarer Katalog mit vordefinierten Maßnahmen angeboten wird, der für unterschiedliche Gegebenheiten anpassbar ist. In einem solchen Katalog können die charakteristischen Eigenschaften jeder Maßnahme erfasst werden (z. B. Bezeichnung, Beschreibung, Maßnahmenkategorie, erwartete Wirkungen, verantwortliche Personen, Umsetzungsfrist).[436] Insbesondere ist auch die Quantifizierung der erwarteten risikoreduzierenden Wirkungen und der Aufwände der Maßnahmendurchführung von Interesse. Beide sind monetär zu bewerten, um in einer risikoorientierten betrieblichen Planung berücksichtigt werden zu können. Zur Quantifizierung und monetären Bewertung sind vom RMIS dieselben Methoden wie zur Risikoquantifizierung anzubieten. Aus den betrieblichen Informationssystemen bezogene Plandaten können dann mit den Risiko- und Maßnahmenkosten angereichert werden, um die Planung zu aktualisieren. Im Idealfall unterstützt das RMIS die Phase der Risikokontrolle durch weitestgehend automatisierte Kontrollen.[437] So könnte das RMIS bspw. selbstständig überprüfen, ob zuvor durch den Anwender definierte Schwellenwerte drohen überschritten zu

[436] Vgl. Kersten et al. 2016, S. 10.
[437] Vgl. Kajüter 2012, S. 201.

werden bzw. bereits überschritten wurden. Tritt eine Diskrepanz auf, muss das RMIS den Anwender darüber informieren. Falls bestimmte Kontrollen nicht automatisierbar sind, sollte das RMIS den Anwender an die Kontrolle erinnern. Die Kontrollzeitpunkte sollten konfigurierbar sein (z. B. Quartalsende).

Theoretische Anforderung	**Geforderte Funktionalität**
Zuordnung von Maßnahmen zu Risiken	• Editierbarer Katalog (ggf. mit vordefinierten Maßnahmen) • Erfassen von Maßnahmenmerkmalen • Zuweisung von Maßnahmen zu Risiken
Bestimmung der erwarteten Wirkungen auf die Risikogrößen	• Funktionen zur Bestimmung bzw. Erfassung der erwarteten (quantitativen) Wirkung auf das Risiko, die Risikokennzahlen, andere Maßnahmen und die Variablen der Unternehmensplanung (z. B. per Simulation)
Anwendung von Kontrollen und organisatorischen Sicherungsmaßnahmen	• Automatisierbare Kontrollen • Möglichkeit der Definition von Kontrollzeitpunkten • Erinnerungen zur Durchführung nicht automatisierbarer Kontrollen • Visualisierung und Benachrichtigung von (drohenden) Überschreitungen von Schwellenwerten

Abbildung 72: Anforderungen zur Unterstützung der Risikosteuerung und -kontrolle

8.2.1.5. Anforderungen zur Unterstützung des Risikoreporting

Zur Umsetzung eines verlässlichen Reporting sind vom RMIS Funktionen bereitzustellen, die zum Zweck einer zielgruppenspezifischen Kommunikation der Risikosituation anwenderspezifische Auswertungen der Risikolage bieten. Diese Risikoberichte müssen sich anhand unterschiedlicher Kriterien zusammenstellen lassen und auf einer frei wählbaren Aggregationsstufe generierbar sein. Berichtteile, die sich für eine visuelle Darstellung eignen, sollten durch entsprechende Grafiken ergänzt werden. Idealerweise werden die Berichte, neben einer Erzeugung auf Abruf, zu frei definierbaren Zeitpunkten automatisch erzeugt (z. B. quartalsweise und am Ende des Geschäftsjahres) und sicher vor unbefugtem Zugriff den Adressaten zugestellt.

Theoretische Anforderung	**Geforderte Funktionalität**
Zielgruppenspezifische Berichte über die Risikolage	• Zeitlich und inhaltlich individuelle Erzeugung von Risikoberichten • Beliebige Aggregationsstufen • Visualisierung der Risikolage • (Automatisierte) Erzeugung von Risikoberichten • Automatische Zustellung der Risikoberichte an die Zielgruppe mittels E-Mail oder Webportal • Dauerhafte Bereitstellung der Berichte

Abbildung 73: Anforderungen zur Unterstützung des Risikoreporting

8.2.2. Organisatorische und organisationsrechtliche Anforderungen

Die organisatorischen Anforderungen an ein RMIS unterteilen sich in aufbau- und ablauforganisatorische[438] sowie organisationsrechtliche Anforderungen aus dem Handels- und Gesellschaftsrecht. In verschiedenen Phasen des Risikomanagementprozesses wird vorausgesetzt, dass für ein Risiko eine verantwortliche Person oder Stelle, der sogenannte Risk Owner, existiert. Er ist vorrangig für die Gestaltung und Durchführung von Risikosteuerungsmaßnahmen, die Risikokontrolle und die Berichterstattung der ihm zugewiesenen Risiken verantwortlich.[439] Zur Abbildung der Risk Owner in einem RMIS ist es erforderlich, dass die Verantwortlichkeit für Risiken den Elementen der Aufbauorganisation (z. B. Personen oder Abteilungen) zugeordnet werden kann. Dazu ist im RMIS die Aufbauorganisation unter Berücksichtigung von Konzern- sowie Abteilungs- und Projektstrukturen abzubilden.[440]

Da Prozesse sowohl Ausgangspunkt von Risiken sind als auch Risiken in ihnen schlagend werden, sollte es im RMIS möglich sein, die Ablauforganisation in Form von Geschäftsprozessmodellen einzubinden.[441] Eine Visualisierung der Prozessstruktur schafft einen Überblick über die Zusammenhänge zwischen den Prozessfunktionen und den Prozessressourcen. So wird die Risikoidentifizierung erleichtert, da „durch die konzentrierte Sicht auf einen Prozessschritt und seine direkte Prozessumgebung […] es schnell und intuitiv möglich [ist], spezifische Risikoquellen einzelner Prozessschritte sowie Ursache-Wirkungs-Zusammenhänge zu erkennen“.[442] Werden bei komplett informationstechnisch unterstützten Prozessen zusätzlich die Daten einzelner Prozessinstanzen erfasst, können neben der Risikoidentifizierung auch die anderen Phasen des Risikomanagementprozesses sinnvoll unterstützt werden. Zu diesen Daten gehören bspw. Prozessinput- und Prozessoutputdaten, die Durchlaufzeit und Ausführungshäufigkeit von Prozessfunktionen, einzelnen Prozesspfaden und Prozessvarianten, die beteiligten Ressourcen je Prozessfunktion sowie prozessexterne Daten mit potentiellem Prozessbezug. Mithilfe moderner Mustererkennungsmethoden kann so ermittelt werden, welche Konstellation von Parametern regelmäßig zu schlagend werdenden Risiken wie z. B. Verzögerungen oder Prozessabbrüchen führt. Auf Basis der Prozessinstanzdaten können solche Risiken weiterhin quantifiziert und somit beurteilt werden. Im Rahmen des Risikoreporting

[438] Vgl. Jahnke und Thomas 2004, S. 21.
[439] Vgl. Perera 2005, S. 1; Viscelli 2014, S. 25.
[440] Vgl. Gleißner und Romeike 2005a, S. 246; Meletiadou et al. 2009, S. 5.
[441] Vgl. Anton et al. 2016, S. 46.
[442] Vgl. Diederichs und Imhof 2011, S. 174 f.

können auf Basis der ermittelten Prozessabweichungen Risikoprognosen mittels zeitreihenanalytischer Verfahren erstellt werden und in die Risikoberichte einfließen.

Je nach Rechtsform, Organisationsgröße und Unternehmenssitz (Kultur- und Rechtsraum) müssen unterschiedliche Regularien berücksichtigt werden.[443] Idealerweise lassen sich daher für jede rechtlich selbstständige Einheit spezifische Stammdaten wie z. B. die Rechtsform, und das Land des Unternehmenssitzes erfassen, damit geltende rechtliche Bestimmungen zum Risikomanagement dieser Gesellschaften berücksichtigt werden können. Die Vorgaben des KonTraG und die daraus abgeleiteten Rechnungslegungsstandards in Deutschland sowie die SOX Vorschriften und die COSO Regularien in den USA lassen sich beispielhaft für unterschiedliche (rechtliche) Vorgaben anführen. Das RMIS könnte in Abhängigkeit der erfassten Unternehmensstammdaten individuell auf die spezifischen risikorelevanten Anforderungen hinweisen und deren Einhaltung unterstützen sowie überprüfen.

Theoretische Anforderung	**Geforderte Funktionalität**
Risikomanagement auf verschiedenen Ebenen (Projekt-, Abteilungs-, Unternehmens-, Konzernebene)	• Abbilden der Aufbauorganisation • Festlegen von Risikoverantwortlichen • Risikoorientierte Prozessmodelle • Analyse IT-basierter Prozesse mittels Process- / Data-Mining
Berücksichtigung gesetzlicher und regulatorischer Vorgaben	• Erfassung von Rechtsform, Größe, Standort und Branche • Erinnerung an Fristen • Archivierung der Risikoberichte

Abbildung 74: Organisatorische / organisationsrechtliche Anforderungen an ein RMIS

[443] Vgl. Reichmann und Kißler 2012, S. 241.

8.2.3. Technische Anforderungen

Die technischen Anforderungen an ein RMIS lassen sich aus den methodisch-inhaltlichen und den organisatorischen Anforderungen sowie aus allgemeinen Anforderungen an integrierte betriebliche Informationssysteme ableiten. Sie umfassen Kommunikations-, Flexibilitäts- und Informationssicherheitsanforderungen an das IT-System. Kommunikationsanforderungen richten sich an die Schnittstellen des Systems zum Datenaustausch mit anderen IT-Systemen und Anforderungen zur Realisierung automatisierter Benachrichtigungen von Anwendern (siehe Kapitel 8.2.1). Ein RMIS ist zunächst auf die Versorgung mit vielen unternehmensinternen und -externen Informationen angewiesen, damit Risiken mit ihren Merkmalen erfasst und quantifiziert werden können. Dies sind bspw. Daten aus betrieblichen Informationssystemen wie Produktionsplanungs- und Steuerungssystemen oder aus externen Informationssystemen wie bspw. einem Börseninformationssystem. Daher muss das RMIS grundsätzlich mit einer großen Menge an heterogenen Daten aus verschiedenen Quellsystemen umgehen können und diese zusammenführen.[444] Damit aktuelle Unternehmensdaten ins RMIS importiert werden können, benötigt es standardisierte Schnittstellen. Über diese können Daten von betrieblichen Informationssystemen, wie z. B. einem ERP-System, angefordert oder an diese übermittelt werden.[445] Im Falle eines ERP-Systems können dies z. B. Daten der Ist- und der Plan-Bilanz sowie der entsprechenden (Plan-) Gewinn- und Verlustrechnung sein. Weiterhin muss der manuelle Im- und Export von Daten über gängige Dateiformate möglich sein, um auch Daten anderer Informationssysteme, wie bspw. externer Schadensdatenbanken, in das RMIS einspeisen zu können. Für den Nachrichtenversand an Anwender ist eine Anbindung an einen Messagingserver notwendig, um z. B. im Rahmen der Risikoidentifizierung und der Risikokontrolle E-Mail Nachrichten mit Erinnerungen oder Alarmierungen an zuständige Anwender zu versenden. Zur automatischen Abwicklung solcher Arbeitsschritte ist die Definition automatisierter Abfolgen vom RMIS zu ermöglichen.

Flexibilitätsanforderungen betreffen die Datenhaltung und die Erweiterbarkeit des RMIS. Ein RMIS sollte aufgrund regelmäßiger Neuerungen flexibel aufgebaut sein.[446] So können neue Funktionen und Analysemethoden, z. B. in Form einzelner Softwaremodule, entwickelt und dem bestehenden System durch Upgrades hinzugefügt werden. Damit solche Erweiterungen

[444] Vgl. Hornung et al. 1997, S. 41.
[445] Vgl. Jahnke und Thomas 2004, S. 23; Meletiadou et al. 2009, S. 5.
[446] Vgl. Gleißner und Romeike 2005a, S. 244 f.

der Software auch unternehmensintern vorgenommen werden können, ist die Bereitstellung von Entwicklertools vorteilhaft.

Letztlich muss das RMIS den Schutzzielen der Informationssicherheit genügen, da im Rahmen des Risikomanagements sensible Daten erhoben und erzeugt werden. Insbesondere sollte die gesamte Kommunikation zwischen Client und Server, zwischen Datenbank und Anwendung sowie mit externen Systemen nach aktuellen Sicherheitsstandards verschlüsselt sein.[447] Des Weiteren sollten die Daten nicht allen Anwendern ohne Einschränkungen zugänglich sein. Dazu ist es notwendig, dass ein RMIS eine rollenbasierte Zugriffsverwaltung unterstützt, über welche die Anwenderzugriffe mithilfe eines Berechtigungskonzeptes gesteuert werden. Jede Rolle hat dabei andere Berechtigungen und jeder Organisationseinheit bzw. jedem Anwender können eine oder mehrere Rollen zugewiesen werden. Die Rollen können im Idealfall wahlweise unter Beachtung der Organisationshierarchie vererbt werden. So kann z. B. einer Abteilung eine Rolle zugewiesen werden, die dann automatisch für alle Mitglieder der Abteilung übernommen wird. Die Zugriffsverwaltung kann entweder im RMIS als Benutzerverwaltung mit Rollenkonzept realisiert oder über Schnittstellen angebunden werden. Letztlich erfordern gesetzliche Anforderungen, dass das RMIS über Funktionalitäten verfügt, die eine revisionssichere Datenarchivierung ermöglichen.[448]

[447] Vgl. Kersten et al. 2013, S. 158 f.
[448] Vgl. § 257 HGB.

Theoretische Anforderung	Geforderte Funktionalität
Kommunikationsanforderungen	• Standardisierte Schnittstellen zur Anbindung betrieblicher Informationssysteme (z. B. SAP PI) • API-Unterstützung für vor- und nachgelagerte Systeme • Manueller Im- und Export von Daten über gängige Dateiformate • Messagingserver-Anbindung • Automatisierte Alarmierungs- bzw. Erinnerungsfunktionalität
Flexibilitätsanforderungen	• Datenbankbasierte Datenhaltung • Modularer Aufbau • Entwicklertools
Informationssicherheitsanforderungen	• Erfüllung der Schutzziele der Informationssicherheit • Verschlüsselte Datenübertragung • Rollenbasierte Zugriffsverwaltung • Backup- und Archivierungsmechanismen

Abbildung 75: Technische Anforderungen an ein RMIS

8.3. Arten von Risikomanagement-Informationssystemen

Auf dem Markt steht eine Vielzahl an Informationssystemen für das Risikomanagement zur Verfügung, die sich bezüglich Zielsetzung, Konzeption und Funktionsumfang sehr unterscheiden. Das Angebot reicht von eher finanzwirtschaftlich orientierten Add-ons für Standard-Office Anwendungen bis hin zu voll integrierten Risikomanagement-Informationssystemen. Erstere gibt es z. B. für Tabellenkalkulationsprogramme, die nur Teilaspekte des Risikomanagements abdecken.[449] Letztere sind rein für das Risikomanagement ausgelegt und mit umfassenden Funktionsumfang ausgestattet.[450] Weiterhin existieren Systeme mit Fokus auf der Unterstützung des Governance- und Compliancemanagement[451] sowie Tools für das Forderungs- und Versicherungsmanagement.[452] Diese decken vielfach Teilfunktionen des Risikomanagementprozesses ab. Bestehende Kategorisierungen von RMIS unterscheiden die Systeme entweder anhand ihrer technischen Gestaltung oder ihres Funktionsumfangs und erlauben so nur eine eindimensionale Einordnung.[453] Im Sinn einer klaren Abgrenzung der unterschiedlichen RMIS werden im Folgenden sowohl funktionale Aspekte als auch organisatorische und technische Eigenschaften berücksichtigt. Aus den ermittelten Anforderungen an RMIS ergibt sich so das in Abbildung 76 dargestellte Schema. Die Einordung der RMIS erfolgt anhand des Grades des risikomanagementspezifischen Funktionsumfangs und des Grades der Integration. Ersterer bildet ab, wie viele der geforderten Risikomanagementfunktionen das RMIS unterstützt. Letzterer spiegelt wider, wie gut sich ein Informationssystem in die Organisation und die bestehende Systemlandschaft eines Unternehmens integrieren lässt. Durch diese Vorgehensweise werden einigermaßen homogene Kategorien gebildet, deren dort eingeordnete RMIS sich direkt miteinander vergleichen lassen.

Innerhalb des Schemas lassen sich mit Bezug auf die Unterstützung des Risikomanagements zunächst zwei Gruppen von Informationssystemen unterscheiden. Die Systeme der Gruppe I (Quadrant Q1 und Q2) bieten Funktionen an, die sich zur Unterstützung einzelner Aufgaben im Risikomanagement verwenden lassen. So lassen sich mit ihnen z. B. Risiken lediglich erfassen oder sie eignen sich zur Quantifizierung von Risiken. Ihr Hauptanwendungsfokus liegt

---

[449] Vgl. z. B. @risk (http://www.palisade.com/risk/de); RiskAMP (http://www.riskamp.com).
[450] Vgl. z. B. enrisma (http://www.enrisma.de); Opture (http://www.opture.com); RiMIS (http://www.antares-is.de/rimis).
[451] Vgl. z. B. Compliance 360 (https://www.saiglobal.com); GRC Cockpit (http://www.grc-cockpit.de).
[452] Vgl. z. B. RiskConsole (http://www.ventivtech.com); Tinubu Square (http://www.tinubu.com).
[453] Vgl. Gleißner und Romeike 2005b, S, 159; Jonen et al. 2006, S. 31 ff.; Meletiadou et al. 2009, S. 7 ff.; Lackes et al. 2010, S. 63 ff.; Weuster 2014, S. 25 ff.

aber vielfach in anderen Bereichen. Häufig sind diese Systeme für Spezialaufgaben des Risikomanagements prädestiniert, aber sie können nicht alle Phasen des Risikomanagements begleiten.

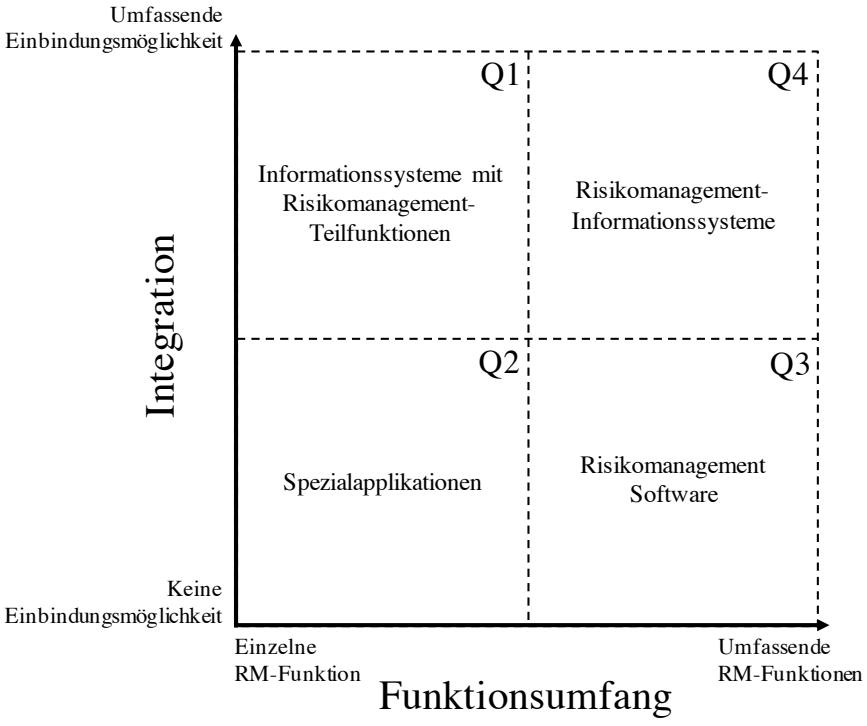


Abbildung 76: Kategorisierung von RMIS

Eine solche Software kann z. B. eine Anwendung für das Prozessmanagement sein, welche neben der Erfassung und Analyse von Geschäftsprozessen auch die Abbildung von einzelnen Risiken innerhalb der Prozesse ermöglicht. Wenn ein solches RMIS über umfassende Einbindungsmöglichkeiten in bestehende Organisationsstrukturen und IT-Systeme verfügt, gilt es gemäß dem eingeführten Kategorisierungsschema als *Informationssystem mit Risikomanagement-Teilfunktionen*. Je weniger es sich integrieren lässt, desto eher handelt es sich um eine *Spezialapplikation*. Ein Beispiel für eine Spezialapplikation wäre eine Tabellenkalkulation, welche eine Monte Carlo Simulation ermöglicht. Die Systeme der Gruppe II (Quadrant Q3 und Q4) unterstützen nahezu jede Phase des Risikomanagements. Sie zeichnen sich durch einen großen risikomanagementbezogenen Funktionsumfang aus. Bietet ein solches Informationssystem zusätzlich eine umfassende Einbindungsmöglichkeit in bestehende Organisatio-

nen und ihre Systemlandschaften, wird es der Kategorie *Risikomanagement-Informationssystem* zugeordnet. Es ermöglicht eine unternehmensweite Nutzung durch mehrere Anwender, die standardmäßige Anbindung an ERP-Systeme, die Berücksichtigung von Rollenkonzepten und einen webbasierten Zugang. Ein Informationssystem für das Risikomanagement, das über wenige oder keine umfassende Integrationsmöglichkeit in bestehende Organisationsstrukturen und Systemlandschaften verfügt, wird der Kategorie *Risikomanagement Software* zugeteilt. Solche Lösungen findet man häufig in Form von Einzelarbeitsplatzlösungen oder in Form von webbasierten Mehrbenutzerlösungen ohne weitergehende Anbindung an betriebswirtschaftliche IT-Systeme vor.

8.4. Status Quo des Angebots an Risikomanagement-Informationssystemen

8.4.1. Marktstudie

Eine Unterstützung des Risikomanagements durch geeignete Informationssysteme ist nicht nur ratsam, sondern aufgrund der Komplexität der Risiken und der Fülle unterschiedlicher risikorelevanter Daten auch geboten.[454] Obwohl auf dem Markt seit Jahren eine Vielzahl an Informationssystemen für das Risikomanagement bereitsteht, werden solche Systeme jedoch nur von einer Minderheit an Unternehmen genutzt.[455] Das vorherrschende Instrument des Risikomanagements ist auch knapp 20 Jahre nach Verabschiedung des KonTraG noch immer die Standard-Tabellenkalkulation, obwohl Unternehmen die Bedeutung einer umfassenden Informationsversorgung für das Risikomanagement durchaus bewusst ist.[456] Die Verwendung klassischer Tabellenkalkulationsprogramme kann für einzelne Teilaufgaben des Risikomanagements, wie z. B. bei der Risikoquantifizierung, durchaus sinnvoll sein, führt aber in der Regel zu einer fragmentierten Sicht auf die Risikosituation aus dem Blickwinkel einzelner Abteilungen und behindert so die Kommunikation von Risikoaspekten innerhalb eines Unternehmens, die Wiederverwendung risikorelevanter Informationen an verschiedenen Stellen und somit letztlich eine ganzheitliche Sicht auf die Risikolage.[457] Doch selbst wenn Risikomanagement-Informationssysteme eingesetzt werden, werden deren Möglichkeiten wie die

[454] Vgl. Zhao et al. 2015, S. 922.
[455] Vgl. Risk and Insurance Management Society 2009; Henschel 2010, S. 89; Bundesverband der Deutschen Industrie und PricewaterhouseCoopers 2011; Funk RMCE et al. 2011; Kajüter 2012, S. 284; gtnews 2013; Theuermann und Ebner 2014; PricewaterhouseCoopers 2015.
[456] Vgl. Deloitte 2015.
[457] Vgl. Barateiro und Borbinha 2011.

Anbindung an bestehende betriebliche Informationssysteme aktuell noch nicht ausgeschöpft.[458]

Damit das aktuelle Angebot an RMIS adäquat beurteilt werden kann, wurde im Rahmen dieser Arbeit eine empirische Untersuchung durchgeführt.[459] Mittels Literatur- und Internetrecherche wurden weltweit 378 RMIS-Anbieter identifiziert.[460] Anbieter von RMIS für Banken und Versicherungen wurden aus dieser Datenbasis entfernt, da Banken und Versicherer zusätzlichen gesetzlichen Vorgaben unterliegen und daher spezifische Anforderungen an das Risikomanagement haben, so dass sich RMIS für diese Zielgruppe funktional von allgemeinen RMIS Lösungen unterscheiden.[461] Von denen zur Teilnahme eingeladenen 192 Unternehmen haben final 99 Firmen an der Umfrage teilgenommen. Letztlich haben davon 36 Anbieter den Fragebogen mit 144 Fragen finalisiert.[462] Der Fragebogen wurde sowohl in Deutsch als auch in Englisch angeboten. Die Fragen bezogen sich auf allgemeine, funktionsbezogene und technische Aspekte des jeweiligen RMIS. Weiterhin wurden vertriebliche Informationen und das sonstige Leistungsangebot der Anbieter erhoben. Die Abbruchquote von 64 % liegt gegebenenfalls in der Anzahl der Fragen begründet. Da es das Ziel der Studie war, einen umfassenden Marktüberblick mit einer detaillierten Betrachtung des Leistungsangebots der Softwaresysteme zu erlangen, wird der Fragenumfang als gerechtfertigt angesehen. Die Fragen waren überwiegend Multiple Choice Fragen, um die Beantwortung zu vereinfachen und dem vorzeitigen Abbruch entgegenzuwirken. Die von den Teilnehmern gemachten Angaben basieren auf den Eigendarstellungen der Unternehmen und wurden nicht verifiziert. Insgesamt verteilen sich die untersuchten RMIS auf die in Abbildung 77 dargestellten vier Kategorien wie folgt:

---

[458] Vgl. Lackes et al. 2010, S. 69; PricewaterhouseCoopers 2015.

[459] Vgl. Anton et al. 2018.

[460] Teile dieser Marktstudie beruhen auf Ergebnissen aus der Bachelor Thesis von Müller, Tobias: Systematische Analyse des Marktes für Risikoinformationssysteme, Lehrstuhl für Wirtschaftsinformatik, TU Dortmund, 2015. Beide Studien basieren auf demselben Fragebogen. In dieser Dissertation wurde jedoch eine eigenständige Nacherhebung und eine eigenständige Gesamtanalyse durchgeführt. In der Bachelorthesis wurden insgesamt 69 Anbieter angeschrieben, von denen 22 teilnahmen. Für die in dieser Arbeit durchgeführte Studie wurden weitere 309 Anbieter identifiziert und von diesen nach Bereinigung von Banken- und Versicherungslösungen sowie Abzug der 69 Teilnehmer aus der Bachelor Thesis, 123 weitere Anbieter zur Teilnahme im Rahmen der Nacherhebung eingeladen. Die Nacherhebung wurde im August 2016 durchgeführt. Sofern bekannt, wurden die jeweiligen Verantwortlichen, ansonsten die Zentrale der Unternehmen per E-Mail mit einem Link zu einem Onlinefragebogen zur Teilnahme eingeladen.

[461] Vgl. Jonen et al. 2006, S. 35; Weuster 2014, S. 26 f.

[462] Davon sind 22 Anbieter aus der o.g. Thesis mit in die Analyse in dieser Dissertation einbezogen worden.

Informationssysteme mit Risikomanagement-Teilfunktionen (Q1)	Spezialapplikationen (Q2)	Risiko-management Software (Q3)	Risikomanagement-Informationssysteme (Q4)
2 (6 %)	6 (17 %)	12 (33 %)	16 (44 %)

Abbildung 77: Kategorienverteilung der untersuchten RMIS

Aufgrund der geringen Anzahl von Systemen in den Kategorien Q1 und Q2 (Gruppe I) ist die Aussagekraft der Ergebnisse für diese beiden Kategorien grundsätzlich eingeschränkt. Für das Ziel der Studie ist dies nicht weiter relevant, da das Interesse der Untersuchung sich im Wesentlichen auf RMIS richtet. Somit stehen die Systeme aus den Kategorien Q3 und Q4 (Gruppe II) im Fokus der Analyse.[463]

[463] Eine Übersicht der teilnehmenden Anbieter und der jeweiligen RMIS Funktionen befindet sich im Anhang dieser Arbeit.

8.4.2. Ergebnisse

Risikoidentifizierung

Im Rahmen der Unterstützung der Risikoidentifizierungsphase werden von den RMIS der Gruppe II insbesondere Checklisten mit über 75 % Erfüllungsgrad als Identifizierungsmethode unterstützt (siehe Abbildung 78).

	Q1	**Q2**	**Q3**	**Q4**
Methoden zur Risikoidentifizierung				
Checklisten	50 %	67 %	75 %	100 %
FMEA	50 %	33 %	33 %	31 %
Fehlerbaumanalyse	0 %	17 %	25 %	50 %
Risikostammdaten				
verbale Beschreibung	100 %	83 %	83 %	94 %
Risikokategorie	50 %	100 %	92 %	100 %
Risk Owner	50 %	83 %	83 %	100 %
Ursachen	100 %	67 %	83 %	94 %
Wirkungen	50 %	100 %	83 %	100 %

Abbildung 78: Unterstützung der Risikoidentifizierung und -erfassung

Dies ist bei den Systemen der Kategorie Q3 verbesserungswürdig, da insbesondere Checklisten durch den RMIS-Anbieter vorkonfiguriert für jede Branche bereitgestellt werden könnten. Sie helfen Anwendern einen Grundstock an branchenspezifischen Risiken zu erfassen und verhindern, dass diese nicht übersehen werden. Eine vollständige Erfassung der wesentlichen Risikostammdaten, wie z. B. der Risikoursachen, bieten nicht alle der RMIS der Gruppe II an, obwohl die Kenntnis der Risikostammdaten bedeutend für die folgenden Phasen des Risikomanagementprozesses, insbesondere für die Risikoquantifizierung und die Risikosteuerung, ist. Moderne Methoden der Datenanalyse zur Unterstützung der Identifizierung von Anomalien in risikorelevanten Daten werden von keinem der Systeme angeboten. In diesem Bereich

sind andere unterstützende Informationssysteme bereits weiterentwickelt und es besteht bei den RMIS der Gruppe II entsprechender Nachholbedarf.[464]

Risikoquantifizierung

Die RMIS der Gruppe II ermöglichen im Rahmen der Risikoquantifizierung mehrheitlich eine qualitative Erfassung von Eintrittswahrscheinlichkeit und Schadensausmaß eines Risikos und lediglich 50 % bzw. 81 % bieten eine quantitative Bemessung an (siehe Abbildung 79).

	Q1	**Q2**	**Q3**	**Q4**
Bestimmung der Wahrscheinlichkeitsverteilung				
Festlegung der Wahrscheinlichkeitsverteilung	0 %	50 %	75 %	81 %
Historische Simulation	0 %	17 %	8 %	31 %
Monte Carlo Simulation (selbst generierte Verteilung)	0 %	50 %	50 %	50 %
Einfache Quantifizierungsmethoden				
Wahrscheinlichkeit & Ausmaß qualitativ	50 %	67 %	92 %	88 %
Wahrscheinlichkeit & Ausmaß quantitativ	100 %	83 %	50 %	81 %
Komplexe Quantifizierungsmethoden				
Sensitivitätsanalyse	0 %	33 %	42 %	44 %
Fuzzy-basierte Verfahren	0 %	0 %	0 %	6 %
Risikomaße				
Cashflow at Risk Berechnung	0 %	17 %	25 %	50 %
Value at Risk Berechnung	0 %	50 %	42 %	63 %

Abbildung 79: Unterstützung der Risikoquantifizierung

Eine angemessene monetäre Ermittlung des potentiellen Schadensausmaßes kann somit mit einem beachtlichen Teil der RMIS der Gruppe II nicht erfolgen. Komplexere Methoden wie

[464] Vgl. z. B. https://www.sap.com/product/technology-platform/process-mining.html im Bereich Prozessmanagement oder https://www.zapliance.com im Bereich Interner Kontrollsysteme.

Sensitivitätsanalysen zur Quantifizierung von Ursache-Wirkungs-Zusammenhängen werden nur von einem kleinen Teil der Systeme angeboten, obwohl diese Zusammenhänge aufgrund ihres Bedrohungspotentials eine besondere Aufmerksamkeit erfahren sollten. Ebenso wird von wenigen der Systeme (6 % aus Q4) eine auf qualitativen Einschätzungen aufbauende Quantifizierung z. B. mittels eines Fuzzy-Systems unterstützt. Somit ist es überwiegend nicht möglich, qualitativ erhobene Angaben zumindest ansatzweise zu quantifizieren. Weiterhin können gängige Risikokennzahlen nur von maximal 42 % (Q3) bzw. 63 % (Q4) berechnet werden, obwohl eine dazu notwendige Wahrscheinlichkeitsverteilung bei 75 % (Q3) bzw. 81 % (Q4) festgelegt werden kann. Insgesamt wird eine umfassende Unterstützung der Quantifizierung von den Systemen vernachlässigt, so dass hierfür andere Tools verwendet werden müssen.

Risikobeurteilung

Die notwendigen Funktionen im Rahmen der Risikobeurteilung sind bei den RMIS der Gruppe II überwiegend vorhanden (siehe Abbildung 80). Auffällig ist, dass bis zu 8 % der RMIS der Gruppe II die Definition von Schwellenwerten nicht ermöglichen. Ohne eine solche Wesentlichkeitsgrenze kann das RMIS nicht automatisiert entscheiden, welche Risiken als kritisch anzusehen sind. Die Beobachtung der Risikomessgröße und die darauf aufbauende Beurteilung eines Risikos müssen demnach in jedem Einzelfall manuell durch einen Anwender erfolgen. Dieser Zusatzaufwand ist im Sinne einer Unterstützung durch das RMIS nicht anwenderfreundlich und zudem fehleranfällig. Weiterhin können nur bei 75 % der Systeme aus Kategorie Q3 Risiken hinsichtlich einzuleitender Steuerungsmaßnahmen priorisiert werden. Diese Möglichkeit sollte bei RMIS grundsätzlich bestehen, da ein Entscheider ein Risiko ggf. aus strategischen Gründen hinsichtlich einzuleitender Steuerungsmaßnahmen höher priorisieren möchte als gleichwertig quantifizierte Risiken.

	Q1	Q2	Q3	Q4
Risikobeurteilung				
Schwellenwerte	50 %	50 %	92 %	94 %
Visualisierung in Risikomatrix	50 %	50 %	75 %	88 %
Priorisierung von Risiken	0 %	83 %	75 %	94 %

Abbildung 80: Unterstützung der Risikobeurteilung

Risikosteuerung und -kontrolle

Die Definition und Zuweisung von Risikosteuerungsmaßnahmen wird vom Großteil der RMIS der Gruppe II mit 92 % bei den Systemen der Kategorie Q3 und 94 % in der Kategorie Q4 unterstützt (siehe Abbildung 81). Weitergehende Unterstützung, wie ein vordefinierter Maßnahmenkatalog, wird von einem Viertel (Q3) bzw. der Hälfte (Q4) der Systeme angeboten. Ein vorkonfigurierter Maßnahmenkatalog, welcher sich z. B. nach Maßnahmenstrategien gliedert, könnte bereits herstellerseitig mitgeliefert werden. Häufig ähneln sich die Prozesse und Betätigungsfelder und somit auch die Risiken der Unternehmen einer Branche, so dass durch eine branchenspezifische Vorkonfiguration des Maßnahmenkatalogs den Anwendern Arbeit abgenommen werden kann. Die Mehrheit der RMIS der Gruppe II (75 % der Kategorie Q3 und 81 % der Kategorie Q4) ermöglichen eine Quantifizierung der Maßnahmenwirkungen auf Schadensausmaße und Wahrscheinlichkeiten der Risiken. Wie diese sich konkret gestaltet, wurde nicht erhoben.

	Q1	Q2	Q3	Q4
Unterstützung der Risikosteuerung				
Vordefinierte Maßnahmendatenbank	0 %	67 %	25 %	50 %
Zuordnung von Maßnahmen zu Risiken	50 %	67 %	75 %	88 %
Quantifizierung der Maßnahmenwirkung				
Einfluss von Maßnahmen auf betriebsw. Kennzahlen	0 %	33 %	58 %	69 %
Einfluss von Maßnahmen auf Risiken	50 %	50 %	75 %	81 %
Einfluss von Maßnahmen auf Unternehmensplanung	0 %	50 %	42 %	69 %

	Q1	Q2	Q3	Q4
Unterstützung der Risikokontrolle				
Abweichungsanalyse mit Benachrichtigung	50 %	50 %	67 %	88 %
Ampelfunktion	100 %	83 %	50 %	94 %
Definition von Kontrollzeitpunkten	100 %	67 %	75 %	94 %
Erinnerungsfunktion	50 %	67 %	92 %	94 %

Abbildung 81: Unterstützung der Risikosteuerung und -kontrolle

Bei der Risikokontrolle leisten die RMIS schwerpunktmäßig Unterstützung in der Organisation der Kontrollaufgaben (siehe Abbildung 81). So können mehrheitlich Kontrollzeitpunkte definiert und Erinnerungen an durchzuführende Kontrollen eingestellt werden. Die Unterstützung bei der Durchführung der Kontrollaufgaben, z. B. in Form von systemseitigen Abweichungsanalysen, ist mit 67 % bei den Systemen der Kategorie Q3 noch ausbaufähig.

Organisatorische und organisationsrechtliche Anforderungen

Im Rahmen der Erfüllung der organisatorischen Anforderungen ermöglichen alle betrachteten Systeme die Abbildung von Verantwortlichkeiten zu Elementen der Aufbauorganisation (siehe Abbildung 82). Insbesondere zeigt sich, dass bei den besser integrierten RMIS der Kategorie Q4 die Risiken nahezu allen wesentlichen Elementen der Aufbauorganisation zugewiesen werden können. Die Granularität in der Zuordnung endet allerdings bei einigen der RMIS auf Abteilungsebene. Einzelnen Personen bzw. Rollen innerhalb von Abteilungen kann die Verantwortung für ein Risiko somit nicht direkt zugeordnet werden. Eine genauere Zuordnung wäre im Sinne eindeutiger Verantwortlichkeiten sinnvoll. Die ablauforganisatorischen Anforderungen erfüllt nur eine Minderheit der RMIS, die es ermöglicht risikoorientierte Prozessmodelle darzustellen. Die Analyse von Prozessinstanzdaten im Kontext des Risikomanagements bietet keines der Systeme der Gruppe II. In der Literatur wird darauf verwiesen, dass meist der Aufwand, der mit einer Risikoanalyse auf Prozessinstanzebene einhergeht, gescheut wird und eine Risikoanalyse sich lediglich auf die allgemeine Gestaltung der Prozesse be-

schränken sollte.[465] Mittlerweile können allerdings moderne Methoden der Datenanalyse die Anwender unterstützen aus großen Prozessinstanzdatenmengen wertvolle Erkenntnisse abzuleiten. Hierhingehend ist die Unterstützungsleistung der RMIS noch ausbaufähig.

	Q1	**Q2**	**Q3**	**Q4**
Aufbauorganisatorische Integration				
Risikozuordnung zu Konzernstrukturen	50 %	83 %	83 %	100 %
Risikozuordnung zu Abteilungen	50 %	67 %	92 %	100 %
Risikozuordnung zu Personen	0 %	67 %	75 %	88 %
Risikozuordnung zu Projekten	50 %	83 %	83 %	100 %
Ablauforganisatorische Integration				
Risikozuordnung zu Geschäftsprozessen	50 %	67 %	50 %	100 %
Geschäftsprozessabbildung mittels EPK	50 %	17 %	0 %	19 %
Geschäftsprozessabbildung mittels BPMN	50 %	17 %	0 %	25 %
Beachtung regulatorischer Vorgaben				
COSO ERM	0 %	33 %	58 %	69 %
ISO 31000	0 %	67 %	75 %	69 %
DRS 20	0 %	33 %	33 %	38 %
IDW PS 340	0 %	33 %	33 %	44 %

Abbildung 82: Erfüllung organisatorischer und organisationsrechtlicher Anforderungen

Die Beachtung regulatorischer Vorgaben wird für die Mehrheit der RMIS der Gruppe II als erfüllt angegeben. Da Gesetzestexte und Rahmenwerke überwiegend keine detaillierten Vorschriften hinsichtlich der Ausgestaltung des Risikomanagementsystems machen, ist dies nicht verwunderlich. Teilweise werden die Anforderungen jedoch bereits durch die aus den methodisch-inhaltlichen und technischen Anforderungen abgeleiteten Funktionen, wie z. B. die Erinnerung an Fristen oder das Backup von Risikoberichten, abgedeckt.

[465] Vgl. Becker et al. 2005, S. 715 f.

Technische Anforderungen

Hinsichtlich der technischen Anforderungen fällt im Bereich der Kommunikation auf, dass ein dateibasierter Im- und Export von Daten häufiger unterstützt wird als ein Echtzeitaustausch über APIs (siehe Abbildung 83). Das Risikomanagement kann ohne Echtzeitaustausch von Daten nur verzögert auf Änderungen in der Informationslage reagieren und ist auf die manuelle Pflege des Datenbestandes angewiesen. Dies führt neben dem erhöhten Aufwand für Anwender zu einer verzögerten Einleitung geeigneter Maßnahmen.

	Q1	**Q2**	**Q3**	**Q4**
Kommunikation				
API	100 %	50 %	25 %	88 %
Dateibasierter Im-/ Export in Comma-separated values	100 %	67 %	83 %	94 %
Dateibasierter Im-/ Export in Excel	100 %	83 %	92 %	94 %
Dateibasierter Im-/ Export in XML	50 %	100 %	92 %	94 %
Microsoft Dynamics Schnittstelle	0 %	17 %	8 %	56 %
Oracle Enterprise Manager Schnittstelle	0 %	0 %	8 %	50 %
SAP Schnittstelle	100 %	33 %	17 %	81 %
Flexibilität				
Entwicklertools	100 %	83 %	8 %	50 %
Sicherheit				
Automatisches Backup	50 %	67 %	58 %	75 %
Manuelles Backup	50 %	17 %	17 %	25 %
Verschlüsselter Datenaustausch	0 %	83 %	100 %	94 %
Zugriffsverwaltung Microsoft Active Directory	100 %	50 %	75 %	38 %
Zugriffsverwaltung Novell eDirectory	50 %	17 %	17 %	19 %
Zugriffsverwaltung IBM Notes (Lotus Notes)	50 %	17 %	8 %	25 %

Abbildung 83: Erfüllung technischer Anforderungen

Eine durchgehende Verschlüsselung der Kommunikationswege, so dass sensible Daten anforderungsgemäß sicher ausgetauscht werden können, wird, insbesondere von den auf einer Client-Server-Architektur aufbauenden Systemen, nicht vollumfänglich erfüllt. Des Weiteren sind nicht bei allen Systemen notwendige Backupmechanismen vorhanden, so dass eine Sicherung der bedeutsamen Daten, wie z. B. bereits erzeugter Risikoberichte, bei manchen RMIS nur mit erhöhtem Aufwand und entsprechendem Fachwissen möglich ist.

8.4.3. Diskussion der Ergebnisse

Die Analyse der RMIS zeigt, dass insbesondere die Phasen der Risikoidentifizierung und der Risikokontrolle sowie die aufbauorganisatorische Integration umfänglich und zufriedenstellend unterstützt werden. Die notwendige Stammdatenerfassung im Rahmen der Risikoidentifizierung wird insbesondere von den Risikomanagement-Informationssystemen (Kategorie Q4) umfassend ermöglicht. Ebenso bieten diese Systeme mehrheitlich Checklisten zur Unterstützung der Risikoidentifizierung an. Hinsichtlich der Fähigkeit heutzutage gängige Datenanalysealgorithmen zur Risikoidentifizierung zu verwenden oder entsprechende Tools anzubinden, sind jedoch alle Systeme ausbaufähig. Die zunehmende Digitalisierung in den Unternehmen und die steigende Automation erzeugen immer mehr große, heterogene Datenmengen, deren rein intellektuelle Auswertung zur Identifizierung von Bedrohungspotentialen nicht mehr handhabbar ist. Hier können Data-Mining Methoden, z. B. durch den Hinweis auf häufig von der Norm abweichende Ereignisse, die Anwender unterstützen.[466] Dies ist zwar nicht die Kernaufgabe eines RMIS, zumindest sollten aber Schnittstellen die Nutzung solcher Methoden in anderen Programmen ermöglichen.

Bezüglich der Risikoquantifizierung leisten die Systeme vor allem bei der qualitativen Erfassung von Risikoeintrittswahrscheinlichkeiten und Schadensausmaßen eine profunde Unterstützung, weniger jedoch bei der Ermittlung quantitativer Werte. Das kann daran liegen, dass die Quantifizierung von Risiken generell eine anspruchsvolle Aufgabe für die Risikomanagementverantwortlichen ist. Eine exakte Risikoquantifizierung wird von diesen häufig nicht vorgenommen,[467] da Anwendern die Wahrscheinlichkeitsverteilungen nicht bekannt sind oder ihnen das Fachwissen fehlt, um diese einzuschätzen. Eine subjektive und nur näherungsweise Bemessung von Risiken überwiegt somit in der Praxis. Hier ergibt sich für RMIS das Potenti-

[466] Vgl. Caron et al. 2013, S. 465 ff.
[467] Vgl. Bömelburg et al. 2012, S. 1165; PricewaterhouseCoopers 2015, S. 34.

al, mithilfe geeigneter Funktionen wie Analysen historischer Daten oder Simulationsverfahren diesen Schritt für die Anwender zu erleichtern. Die Ergebnisse dieser Studie zeigen jedoch, dass dieses Potential nicht genutzt wird.

Funktionen der Risikobeurteilung werden zwar von allen untersuchten RMIS angeboten, jedoch ist die eigentlich einfach zu realisierende Definition von Schwellenwerten nicht bei allen Systemen möglich. Dabei sind für die Beurteilung der Risiken Referenzwerte in Form von Schwellenwerten und deren Dokumentation im RMIS unabdingbar. Findet keine Hinterlegung solcher Wesentlichkeitsgrenzen im RMIS statt, muss jedes quantifizierte Risiko von den Anwendern individuell interpretiert werden, was zu Inkonsistenzen in der Beurteilung führen kann. Darüber hinaus können einzelne Zielgruppen, wie z. B. Mitglieder des Aufsichtsrats, ohne dokumentierte Schwellenwerte die Bedeutung eines Risikowerts gegebenenfalls nicht korrekt interpretieren.

In der Risikosteuerung werden insbesondere die Aufgaben der Risikokontrolle durch die betrachteten RMIS unterstützt. Viele der Systeme bieten übersichtliche Ampelfunktionen zur Risikolage und Erinnerungsfunktionen zur Wahrnehmung der Aufgaben der Risikokontrolle an. Es fällt jedoch auf, dass die Systeme im Rahmen der Identifizierungsphase zum Großteil die Unterstützung durch Checklisten anbieten, aber im Rahmen der Risikosteuerung nur wenige einen vordefinierten Maßnahmenkatalog für die in den Checklisten aufgeführten Risiken bereitstellen. Des Weiteren können die Auswirkungen eingeleiteter Maßnahmen auf die betriebswirtschaftlichen Planwerte und Kennzahlen bei über 30 % der Risikomanagement-Informationssysteme (Q4) nicht bestimmt werden, obwohl bis zu 81 % dieser RMIS eine direkte Verbindung zu ERP-Systemen unterstützen, über welche die Planwerte abgerufen werden können. Diesbezüglich bleiben die Systeme eindeutig hinter ihren Möglichkeiten zurück. Dabei ergäben sich hier Synergieeffekte, da für die Bemessung der Maßnahmenwirkung dieselben Methoden verwendet werden können wie für die Risikoquantifizierung. Beide Phasen werden so nicht optimal unterstützt.

Eine starke aufbauorganisatorische Integration ermöglichen insbesondere Systeme der Kategorie Q4. Schwächen zeigen sich jedoch bei der Erfüllung der ablauforganisatorischen Anforderungen. Auf Geschäftsprozessebene können Risikoaspekte überwiegend nur textuell erfasst werden. Eine Integration von Geschäftsprozessmodellen (z. B. nach dem BPMN 2.0 Standard) wird kaum unterstützt. Viele Risiken basieren jedoch auf der Ablauforganisation und

entstehen erst zum Ausführungszeitpunkt. Daher bietet es sich an, dass die in Unternehmen vielfach bereits vorhandenen Prozessdokumentationen im RMIS abgebildet bzw. in dieses importiert werden[468], damit sie als Unterstützung für das Management operativer Risiken genutzt werden können.

Hinsichtlich technischer Aspekte erlauben RMIS der Kategorien Q3 und Q4 zwar zu einem großen Teil den Im- und Export von Dateien aus Tabellenkalkulationen. Eine im Sinne eines holistischen Risikomanagements umfassende Integration in bestehende Systemlandschaften wird jedoch nur teilweise ermöglicht. Die Potentiale einer solchen Integration können daher nicht vollumfänglich ausgeschöpft werden, indem bspw. Plandaten aus anderen IT-Systemen im RMIS verwendet werden oder vorhandene Benutzerverwaltungen genutzt werden können.

Zusammenfassend ist festzuhalten, dass die analysierten RMIS zwar wie zu erwarten den gesetzlichen Anforderungen gerecht werden, weiterführende Analyse- und Unterstützungstools, wie z. B. Simulations- und Datenanalysetools, jedoch meist fehlen. Vor allem bei Systemen, die über Schnittstellen zu bestehenden ERP-Systemen verfügen, wird so eine Chance vertan. Auffällig ist auch, dass oftmals einfache Funktionen wie die Definition von Schwellenwerten oder die Bereitstellung von Maßnahmenkatalogen nicht realisiert sind, obwohl diese leicht zu implementieren wären. Darüber hinaus ist die nur rudimentär vorhandene Integration von Geschäftsprozessen zu bemängeln, wo gerade deren Bedeutung für das Risikomanagement vielfach besonders hervorgehoben wird.[469]

Da es sich bei den betrachteten Systemen nur um einen kleinen Ausschnitt des Gesamtmarktes handelt, wurde im Nachgang zur Befragung eine Kurz-Analyse aller Systeme durchgeführt, um zu überprüfen, ob die Ergebnisse der Studienstichprobe dem Leistungsstand der RMIS auf dem Gesamtmarkt entsprechen. Dazu wurden die Internetseiten und Produktkataloge der 156 nicht an der Studie teilnehmenden Anbieter analysiert. Auf Basis der dort verfügbaren Informationen wurden die RMIS anschließend nach RMIS-Arten kategorisiert (siehe Anhang). Wenn eine Information nicht auffindbar war, wurde vereinfachend angenommen, dass die entsprechende Eigenschaft vom jeweiligen RMIS nicht abgedeckt wird. Nur wenige der RMIS konnten der Kategorie Q4 (1 %) zugeordnet werden. Die Hauptgruppe bilden RMIS der Kategorie Q3 (65 %), die einen hohen Funktionsumfang aufweisen, sich allerdings

[468] Der Import ist z. B. bei XML-basierten maschinenlesbaren Prozessmodellierungssprachen wie WS-BPEL oder BPMN 2.0 möglich.

[469] Vgl. Rikhardsson et al. 2006, S. 4 f.; Conforti et al. 2011, S. 100; Diederichs und Imhoff 2011, S. 174 ff.

nur gering in bestehende Organisationsstrukturen und Systemlandschaften integrieren lassen. Dem Integrationsaspekt scheint demnach seitens der RMIS-Anbieter eine geringe Bedeutung beigemessen zu werden. Ebenso existiert eine große Anzahl an Spezialapplikationen (33 %). Unter diesen sind überwiegend Tools, die Funktionen zur Risikoquantifizierung bereitstellen. Die hohe Anzahl an Speziallösungen zur Unterstützung der Risikoquantifizierung und die Ergebnisse der vorliegenden Studie zeigen, dass es eine Lücke zwischen der Nachfrage an komplexen Quantifizierungsmethoden und deren Bereitstellung in bestehenden RMIS gibt. Dies führt allerdings zu einem Bruch in der integrierten Informationsverarbeitung innerhalb des Risikomanagementprozesses und erschwert einen ganzheitlichen Blick auf die Risikosituation. Die Quantifizierung erfordert zwar in erster Linie einen entsprechenden Kompetenzaufbau seitens der Anwender, aber auch die RMIS könnten durch entsprechende Hilfestellungen diese Aufgabe zielführender unterstützen, so dass der Einsatz von Speziallösungen obsolet wird.

8.4.4. Limitationen

Die Studie unterliegt einigen Einschränkungen. Zunächst ist zu bedenken, dass die RMIS nicht einem einheitlichen Testszenario unterzogen wurden, sondern die Studie auf einem Fragebogen basiert, der von den Anbietern selbst ausgefüllt wurde. Dadurch sind Verzerrungen durch falsch verstandene Fragen oder fehlerhafte Antworten möglich, die nicht ohne weiteres identifiziert werden konnten. Außerdem ist bei dieser Methodik zu bedenken, dass lediglich das Vorhandensein bestimmter Funktionalitäten abgefragt wurde, nicht aber die Qualität ihrer Implementierung beurteilt werden kann. Darüber hinaus haben knapp ein Fünftel aller RMIS Anbieter weltweit an der Studie teilgenommen. Der Anteil der Anbieter von RMIS mit umfassender Risikomanagementfunktionalität (Kategorie Q3 und Q4) lag dabei bei ca. 27 %. Daher kann eine Verallgemeinerung der Erkenntnisse zunächst nur bedingt erfolgen. Um diesem Problem der Stichprobengröße zu begegnen, wurde daher auf Basis der im Internet zu findenden Informationen eine Vollerhebung durchgeführt, die die Erkenntnisse der Studie jedoch bestätigt. Zuletzt ist die Vorgehensweise zur Erstellung des Anforderungskatalogs zu nennen. Vorteilhaft ist zwar, dass dieser, wenn auch nicht vollkommen vollständig, so doch möglichst umfassend gestaltet werden konnte. Jedoch wurden an einzelne Bereiche hohe Anforderungen gestellt, die zwar aus wissenschaftlicher Sicht geboten erscheinen, in der Praxis möglicherweise aber zum Teil eine geringere Relevanz besitzen. In zukünftigen Untersuchun-

gen könnte daher überprüft werden, inwieweit die in dieser Studie theoretisch bestimmten Anforderungen an RMIS den Anforderungen aus Unternehmenssicht entsprechen und inwiefern Unternehmen mit dem bestehenden Marktangebot an RMIS zufrieden sind.

9. Entwurf eines Risikomanagement-Informationssystems

9.1. Überblick

Die in dieser Arbeit entwickelte Erweiterung der BPMN zur Modellierung von Risiken in Geschäftsprozessmodellen überwindet einen Großteil der Mängel bestehender Ansätze. Zum einen setzt sie auf einer systematischen Herleitung der Anforderungen an eine Risikoerweiterung für Prozessmodelle auf, zum anderen liegt ihr eine formale Beschreibung der Beziehungen zwischen prozessbezogenen Risikophänomenen und Prozesselementen zugrunde (Metamodell) und sie lässt sich in der Prozessdesign- sowie Prozessdurchführungsphase (Maschinenlesbarkeit) nutzen. Die in Kapitel 8.4 aufgezeigten Verbesserungspotentiale der informationstechnischen Unterstützung des Risikomanagements sollen im Folgenden durch ein Risikomanagement-Informationssystem adressiert werden, welches Geschäftsprozesse und Prozessrisiken in den Fokus des Risikomanagements stellt. Mithilfe des Informationssystems sollen Geschäftsprozesse und ihre inhärenten Risiken auf Basis der BPMN und der konzipierten Risikoerweiterung modelliert und verwaltet werden können. Bei der Konzeption werden die Anforderungen an Risikomanagement-Informationssysteme berücksichtigt (siehe Kapitel 8.2).

9.2. Aufbau des Informationssystems

9.2.1. Beschreibung der Systemarchitektur

Die Beschreibung des im Folgenden konzipierten RMIS orientiert sich an den Sichten der Architektur für Integrierte Informationssysteme (ARIS) und erfolgt auf Fachkonzeptebene.[470]
Die Beschreibung des RMIS erfolgt durch Darstellung der Funktionssicht, der Datensicht und der Steuerungssicht. Die Funktionssicht stellt die Funktionen des Informationssystems mithilfe von Funktionsbäumen dar. Die Datensicht beschreibt mittels Datenschemata die logische Datenstruktur des RMIS. Die Steuerungssicht zeigt mittels Prozessmodellen die Zusammenhänge zwischen den Sichten auf. Die Beschreibung der Datensicht erfolgt, im Gegensatz zu ARIS, nicht mit einem Entity Relationship Model (ERM), sondern, aufgrund seiner Vorteile,[471] mit einem Strukturierten Entity Relationship Model (SERM). Zur Modellierung der Steuerungssicht wird anstelle der bei ARIS vorgesehenen EPK die BPMN genutzt, um die

[470] Vgl. Scheer 1992.
[471] Vgl. Ferstl und Sinz 2013, S. 158 f.

Konsistenz innerhalb dieser Arbeit zu wahren. Dabei beschränkt sich die Modellierung der Steuerungssicht auf die Risikomanagement-bezogenen Prozesse, die das RMIS unterstützt. Die Prozessmodellierung grundlegender Administrationsprozesse wird vernachlässigt, da diese im Wesentlichen in jedem Informationssystem abzubilden sind und daher keine Besonderheit darstellen (z. B. ein Prozess „*Benutzer verwalten“*).

9.2.2. Detailsichten für die Grundfunktionen

Funktionssicht

Zu den administrativen Grundfunktionen gehört die *Benutzer- und Rollenverwaltung*, welche eine individuelle Zugriffsregelung auf die Funktionen des Informationssystems für jeden Anwender erlaubt (siehe Abbildung 84). Über die *Unternehmenszielpflege* können strategische Ziele und zugehörige Plangrößen definiert werden. Mittels des *Schnittstellenmanagements* können Schnittstellen für den Datenaustausch mit anderen Informationssystemen eingerichtet werden. Die Daten, die über diese Schnittstellen in das RMIS eingespeist werden, können über das *Schnittstellenmanagement* mit den zugehörigen Datenfeldern des RMIS verknüpft werden. Zur Erfassung der Aufbau- und Ablauforganisation bietet das System Funktionen zur Abbildung der Organisationsstrukturen und der Geschäftsprozesse an. Eine zentrale Rolle nimmt die Definition der Geschäftsprozesse ein, da diese für die spätere Risikomodellierung auf Basis der in dieser Arbeit entwickelten Notation benötigt werden. Das RMIS erlaubt einerseits den Import von Geschäftsprozessmodellen, die bereits in anderen Tools nach dem BPMN Standard modelliert wurden. Anderseits besitzt das RMIS einen eigenen Editor zur BPMN konformen Modellierung von Geschäftsprozessen. Jedem importierten oder modellierten Prozess sind konkrete Prozessziele zuzuordnen, die sich aus den strategischen Unternehmenszielen bzw. den daraus resultierenden Plangrößen ableiten lassen, damit eine darauf aufbauende Risikoidentifizierung gemäß der in dieser Arbeit zugrunde gelegten Definition (siehe 2.3) erfolgen kann. Diese Definition der Prozessziele erfolgt über die Funktion *Prozesszieldefinition*.

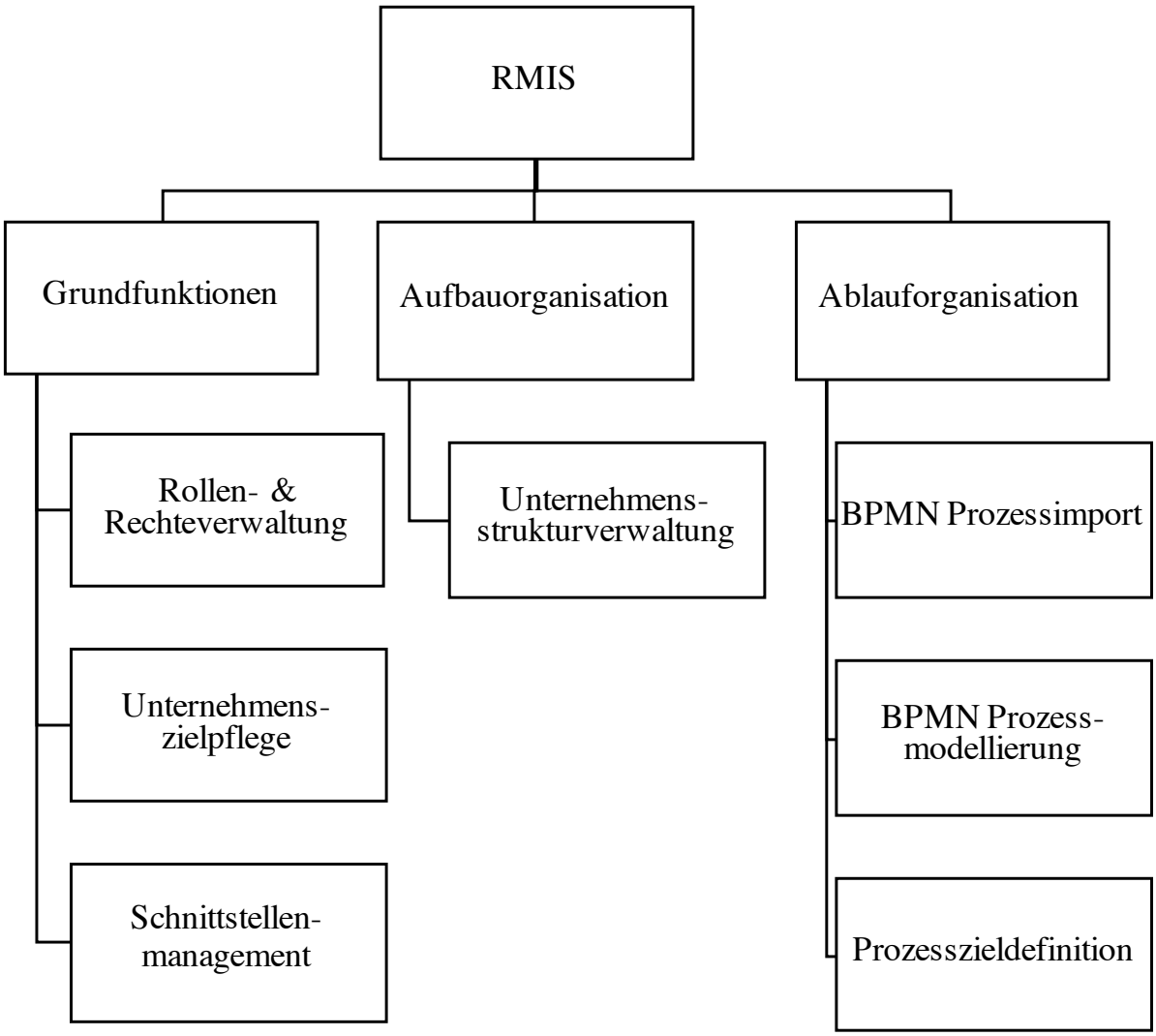
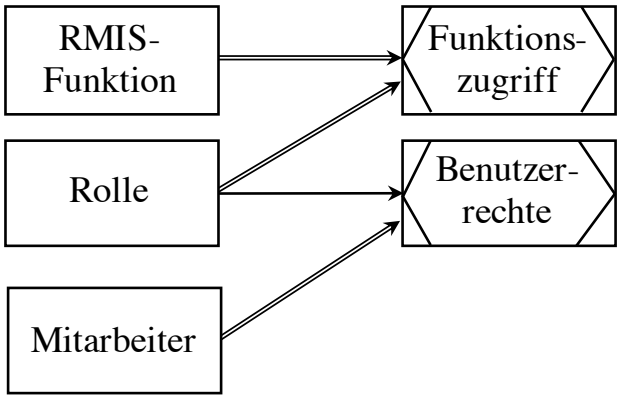


Abbildung 84: Funktionsbaum Grundfunktionen und Organisation

Datensicht[472]

Das Datenmodell zur Rollen- und Rechteverwaltung ist in Abbildung 85 dargestellt. Das RMIS verfügt über Rollenprofile, denen jeweils eine unterschiedliche Anzahl an nutzbaren Funktionen zugewiesen sind. Die Kapselung in Rollen ermöglicht eine flexible Zugriffssteuerung für die unterschiedlichen Anwendergruppen des RMIS. Zur Steuerung der Zugriffsrechte eines Mitarbeiters werden diesem ein oder mehrere Rollenprofile zugewiesen. Beispielhafte Rollen sind die *Administrator* oder die *Risk Owner* Rolle. Ein Mitarbeiter mit zugewiesener Administratorrolle darf üblicherweise auf jegliche Funktionen des Systems zugreifen und diese ausführen. Ein Mitarbeiter, der über die Risk Owner Rolle verfügt, hat entsprechend weniger Befugnisse.



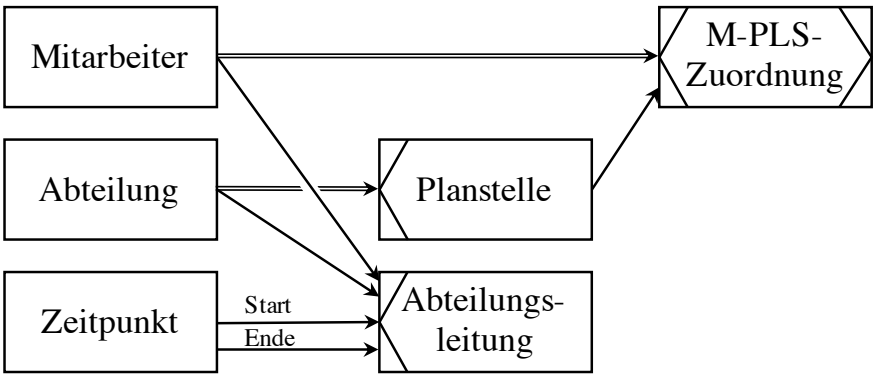
RMIS-Funktion (F-ID, Bezeichnung)
Funktionszugriff (F-ID, Rollen-ID)
Rolle (Rollen-ID, Bezeichnung)
Benutzerrechte (M-ID, Rollen-ID)
Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)

Abbildung 85: Datenmodell Rechteverwaltung

Abbildung 86 zeigt das SER Modell zur Beschreibung der aufbauorganisatorischen Elemente. Das Datenmodell ermöglicht die Erfassung von Abteilungen und ihnen zugeordneten Planstellen, welche durch keinen, einen oder mehrere Mitarbeiter besetzt sein können. Durch die

[472] Die Datenmodelle werden in den folgenden Kapiteln aus Gründen der Übersichtlichkeit entlang der Struktur der Unterkapitel beschrieben und in Teilen nach und nach ergänzt. So kann es vorkommen, dass Attribute erst einem Objekttyp hinzugefügt werden, wenn sie für die in den jeweiligen Unterkapiteln beschriebenen Funktionen benötigt werden. Im Anhang dieser Arbeit befinden sich Übersichtsdarstellungen in denen die einzelnen SER Modelle im Zusammenhang dargestellt werden.

Zuordnung der Mitarbeiter zu den Planstellen über den R-Typ *M-PLS-Zuordnung*, wird deren Abteilungszugehörigkeit abgebildet. Dabei ist es möglich, dass ein Mitarbeiter mehreren Abteilungen angehört, da er z. B. in zwei Abteilungen je eine 50-Prozent-Stelle besetzt. Das SERM berücksichtigt, dass jede Abteilung maximal einen Abteilungsleiter hat. Das Modell sieht vor, dass eine Abteilung vorübergehend keinen Abteilungsleiter und auch keinen Vertreter hat. Da die Dauer der Abteilungsleitungsfunktion gegebenenfalls unbefristet ist, kann das Attribut *Ende-Z-ID* kein Teil des Primärschlüssel des Objekts *Abteilungsleitung* sein. Entsprechend muss das Objekt *Abteilungsleitung* als ER-Typ modelliert werden. Weiterhin kann ein Mitarbeiter theoretisch mehrere Abteilungen leiten (z. B. kommissarisch).

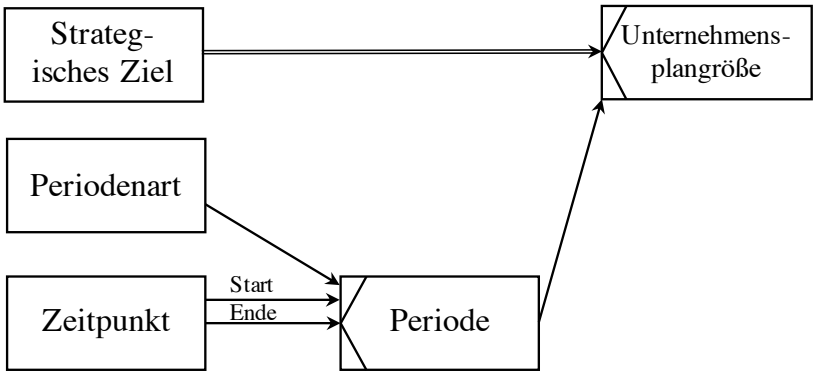


Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Abteilung (A-ID, Bezeichnung)
Planstelle (PLS-ID, A-ID, Bezeichnung)
M-PLS-Zuordnung (M-ID, PLS-ID)
Zeitpunkt (Z-ID, Zeitpunkt)
Abteilungsleitung (A-ID, M-ID, Start-Z-ID, Ende-Z-ID)

Abbildung 86: Datenmodell Aufbauorganisation

Zu den Grundfunktionen des RMIS gehört die Erfassung von strategischen Zielen. Aus ihnen leiten sich konkrete Unternehmensplangrößen ab, die zahlenmäßig ausgedrückt werden und monetär zu bewerten sind (siehe Abbildung 87). An den Unternehmensplangrößen, die jeweils für eine bestimmte Periode gültig sind, orientieren sich im weiteren Verlauf die prozessbezogenen Plangrößen. Eine Periode besteht aus einem Start- und einem Endzeitpunkt und die Periodenart legt fest, ob es sich um ein Jahr, einen Monat usw. handelt.[473]

[473] Vgl. Siepermann 2008, S. 182.

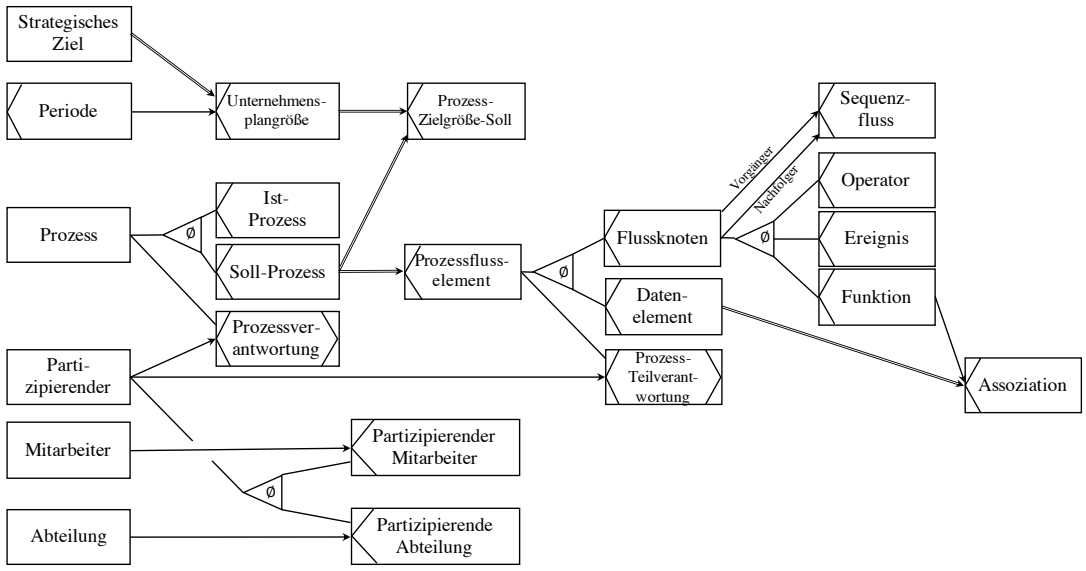


Strategisches Ziel (SZ-ID, Bezeichnung)
Unternehmensplangröße (PG-ID, PE-ID, SZ-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Periodenart (PA-ID, Art)
Zeitpunkt (Z-ID, Zeitpunkt)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)

Abbildung 87: SERM Plangrößenerfassung

Zur Erfassung der Soll-Prozesse im RMIS lassen sich BPMN-Modelle aus einer .bpmn-Datei, die in einer anderen Anwendung erstellt und gemäß dem BPMN Standard gespeichert wurde, im Prozesseditor des RMIS öffnen, modellieren und speichern. Alternativ können die BPMN Modelle von Grund auf im Prozesseditor des RMIS modelliert werden. Die so entstehenden Soll-Prozessmodelle werden als E-Typ *Prozess* im Datenschema repräsentiert und als Soll-Prozess spezialisiert (siehe Abbildung 88).[474] Soll-Prozesse stellen die geplanten Prozessverläufe dar. Ein Soll-Prozess besteht aus mehreren Prozessflusselementen, die im BPMN Standard innerhalb einer Swimlane Darstellung angeordnet sind. Jede Swimlane ist entweder ein Pool oder eine Lane, die sich innerhalb eines Pools befindet (siehe Abbildung 23). Ein Pool kann weiterhin aus mehreren Lanes bestehen und eine Lane ist immer ein Bestandteil genau eines Pools.

[474] Die ebenfalls als Spezialisierung des Prozesses dargestellten Ist-Prozesse sind die tatsächlich ausgeführten Prozessvarianten einer Periode, die sich bei Vorliegen historischer Prozessdaten rekonstruieren lassen (siehe Kapitel 5.2.4). Sie sind im Rahmen der Risikoidentifizierung bzw. -analyse von Interesse und werden daher im SERM in Abbildung 93 näher beschrieben.



Strategisches Ziel (SZ-ID, Bezeichnung)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Unternehmensplangröße (PG-ID, PE-ID, SZ-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozess (P-ID, Bezeichnung)
Ist-Prozess (IP-ID, P-ID)
Soll-Prozess (SP-ID, P-ID)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozessflusselement (PFE-ID, P-ID, SP-ID, Bezeichnung)
Flussknoten (FLK-ID, PFE-ID)
Datenelement (D-ID, PFE-ID, Bezeichnung, Typ)

Sequenzfluss (Vorgänger-FLK-ID, Nachfolger-FLK-ID, Bezeichnung)
Operator (FLK-ID, Bezeichnung, Junktor)
Ereignis (FLK-ID, Bezeichnung, BPMN-Ereignisart)
Funktion (FU-ID, FLK-ID, Bezeichnung, BPMN-Funktionstyp)
Assoziation (D-ID, FU-ID, Bezeichnung)
Partizipierender (PART-ID)
Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Abteilung (A-ID, Bezeichnung)
Partizipierender Mitarbeiter (PART-ID, M-ID)
Partizipierende Abteilung (PART-ID, A-ID)
Prozessverantwortung (PART-ID, P-ID)
Prozess-Teilverantwortung (PART-ID, PFE-ID)

Abbildung 88: Datenmodell BPMN Soll-Prozess

Sowohl Pools als auch Lanes stellen letztlich Verantwortlichkeiten bzw. Teilverantwortlichkeiten innerhalb eines Prozesses dar. Die Verantwortung wird von Prozesspartizipierenden übernommen (E-Typ *Partizipierender*). Dies kann ein einzelner Mitarbeiter oder eine Abteilung sein. Je Prozess gibt es maximal einen Hauptverantwortlichen, der im R-Typ *Prozessverantwortung* festgehalten wird und im BPMN Diagramm einem Pool entspricht. Das SERM berücksichtigt hierbei auch, dass gemäß BPMN Standard kein Prozess über mehrere Pools verlaufen kann, indem ein Prozess maximal einem Partizipierenden zugeordnet werden kann. Des Weiteren kann es innerhalb eines Prozesses Teilverantwortliche für einzelne Prozessflusselemente, wie z. B. eine Aufgabe, geben. Diese Verantwortlichkeiten werden im R-Typ *Prozess-Teilverantwortung* festgehalten. Existieren innerhalb eines Prozesses mehrere Teilverantwortliche, werden diese im BPMN Diagramm von der Anwendungslogik entsprechend als

Lanes innerhalb des prozesszugehörigen Pools (R-Typ *Prozessverantwortung*) dargestellt. Falls die gesamte Prozessverantwortung und jegliche Teilverantwortung für alle Prozessflusselemente einem Partizipierenden zugeordnet sind, wird der Prozess von der Anwendungslogik BPMN konform gesamthaft innerhalb eines Pools ohne Unterteilung in Lanes dargestellt. Da es vorkommen kann, dass zur Prozessdesignzeit die Verantwortlichkeiten noch nicht klar definiert sind, erlaubt das SERM, dass sowohl der E-Typ *Prozess* als auch der ER-Typ *Prozessflusselement* mit einer (0, 1)-Beziehung über den jeweiligen R-Typen zum E-Typ *Partizipierender* verbunden sind und somit auch kein Verantwortlicher definiert werden darf.
Zur Abbildung der BPMN Prozessflusselemente, lässt sich der ER-Typ *Prozessflusselement* weiter spezifizieren. Ein Prozessflusselement ist entweder ein Datenobjekt oder ein Flussknoten. Die Flussknoten werden als Funktionen, Ereignisse oder logische Operatoren spezifiziert. Sie sind jeweils durch Sequenzflüsse miteinander verbunden. Datenelemente werden in der BPMN über Assoziationen den Funktionen, in denen sie entstehen oder benötigt werden, zugeordnet. Dies wird durch den ER-Typ *Assoziation* realisiert, der gemäß BPMN mit einer eigenen Bezeichnung versehen werden kann. Laut BPMN sind Datenspeicher und Datenobjekte zu unterscheiden (siehe Abbildung 23). Diese Unterscheidung wird über das Attribut *Typ* des ER-Typs *Datenelement* realisiert. Jeder Prozess hat weiterhin mindestens eine konkrete Zielgröße, die sich aus einer Unternehmensplangröße ableitet und im ER-Typ *Prozess-Zielgröße-Soll* messbar quantifiziert wird. Prozesszielgrößen sind häufig Größen wie z. B. die Verringerung der Durchlaufzeit eines Prozessdurchlaufs um x Zeiteinheiten oder leistungsorientierte Größen wie z. B. eine feste zu produzierende Menge pro Prozessdurchlauf. Da die Prozesszielgrößen sich direkt aus den monetär bewerteten Plangrößen der Unternehmung ergeben, sind sie trotz ihres nicht-monetären Charakters für die spätere Risikoanalyse monetär zu bewerten.

9.2.3. Detailsichten für die Risikoidentifizierung

Funktionssicht

Im Rahmen der Risikoidentifizierung muss zunächst ein Prozess ausgewählt werden, für welchen die Identifizierung von Risiken durchgeführt werden soll. Das RMIS sieht vor, dass Risiken entlang des Soll-Prozessmodells dokumentiert werden. Entsprechend werden über die Funktion *Prozess auswählen* die zuvor importierten oder modellierten BPMN Soll-Prozesse zur Auswahl bereitgestellt.

Im nächsten Schritt können über die Funktion *Risiken identifizieren* die Risiken entlang des ausgewählten Soll-Prozessmodells identifiziert bzw. erfasst werden.

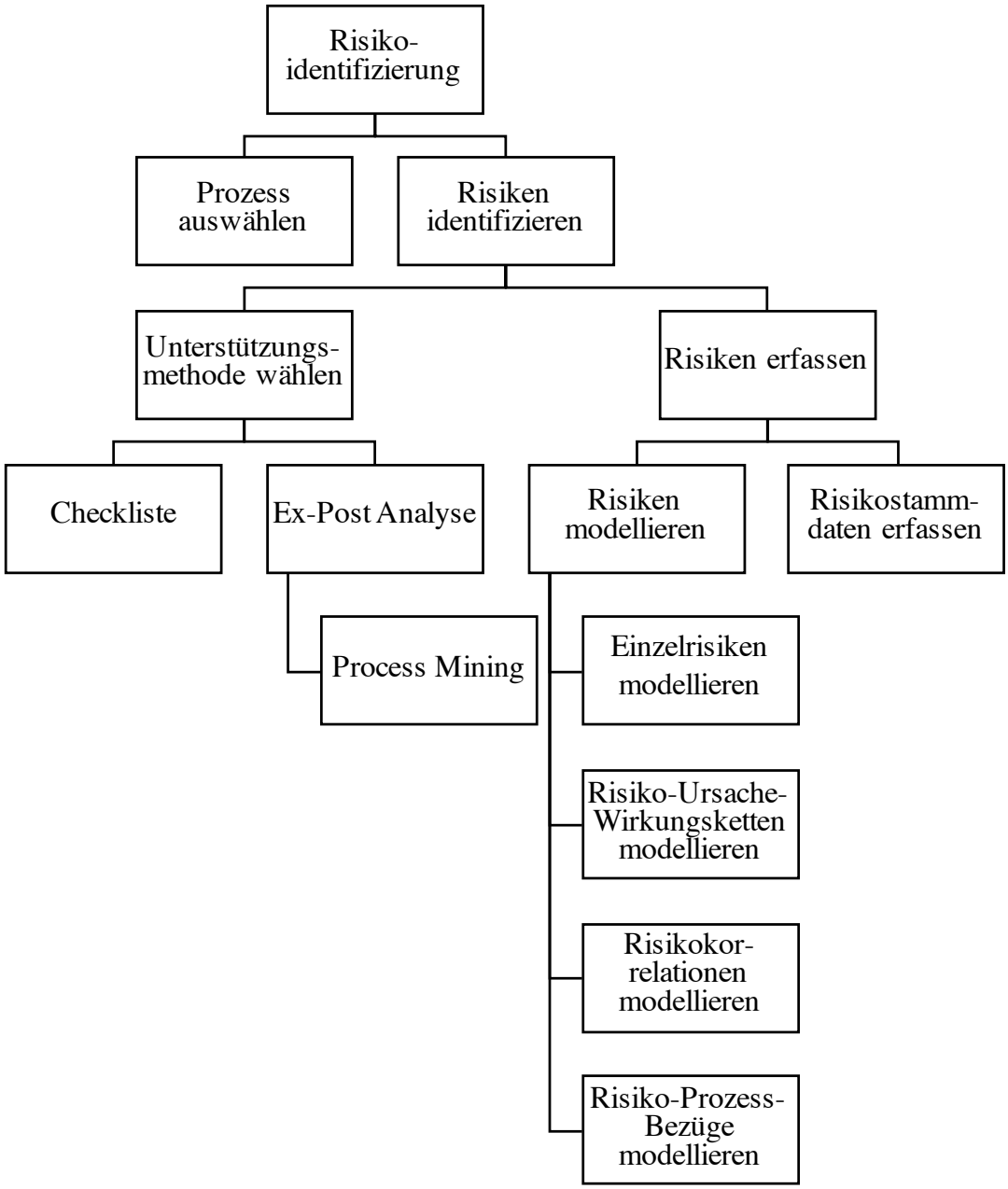


Abbildung 89: Funktionsbaum Risikoidentifizierung

Sind die Risiken nicht unmittelbar bekannt, kann auf Unterstützungsmethoden zur Risikoidentifizierung zurückgegriffen werden. Als klassisches Hilfsmittel bieten gängige RMIS branchenspezifische Checklisten an. Als innovative Methode zur Unterstützung der Risi-

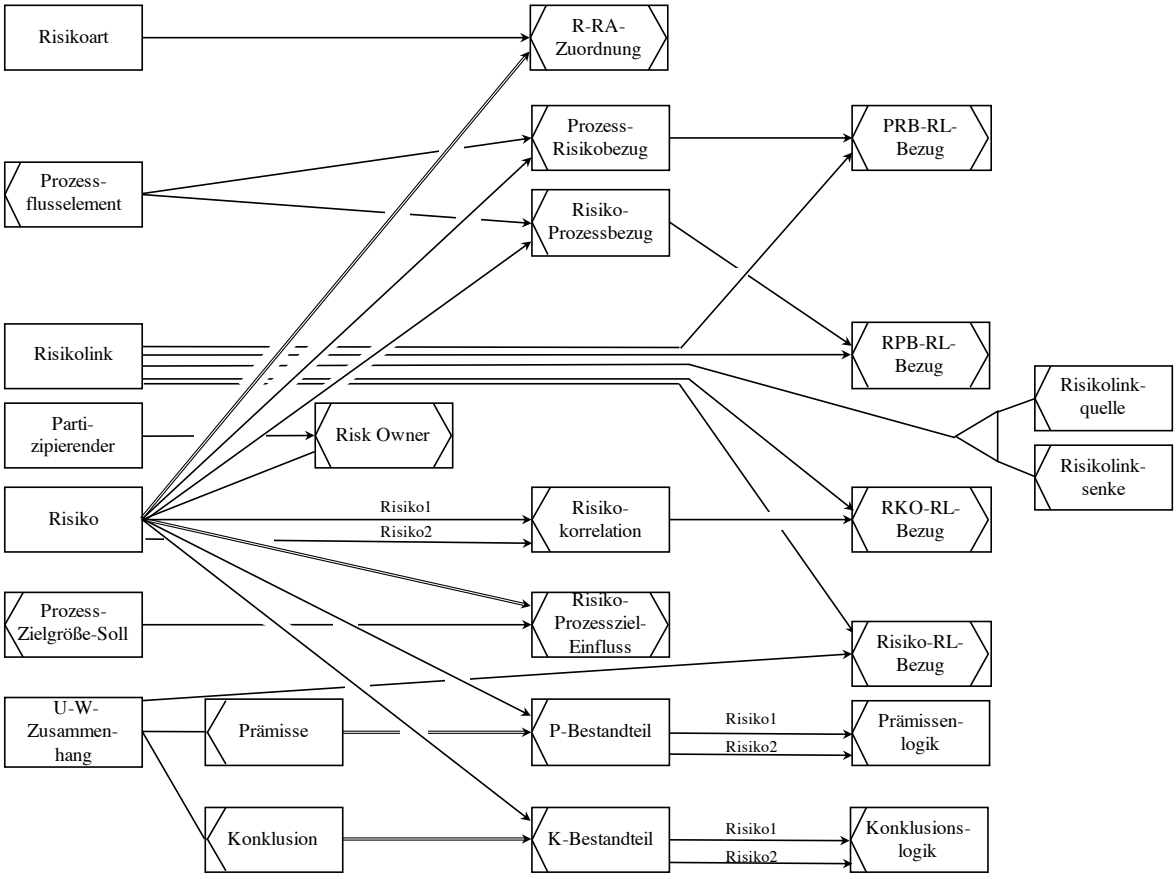
koidentifizierung sieht das hier beschriebene RMIS die Analyse historischer Belegdaten, die einen Prozessbezug aufweisen, vor. Auf Basis dieser Daten können mit modernen Algorithmen aus dem Bereich des Process Mining (siehe Kapitel 5.2.4) die tatsächlichen Prozessverläufe rekonstruiert werden. Dabei kann es vorkommen, dass unterschiedliche Prozessverlaufsvarianten identifiziert werden. Es können z. B. Prozessvarianten existieren in denen einzelne Prozessschritte des Soll-Prozesses in den Ist-Prozessverläufen der Realität häufig übersprungen wurden. Des Weiteren tauchen gegebenenfalls neue Aktivitäten im Ist-Prozess auf und verlangsamen diesen, obwohl sie im Soll-Prozess nicht modelliert sind. Durch die Process Mining Analysen können solche Phänomene, die dazu führen, dass Prozessziele nicht erreicht wurden, ermittelt werden und visuell (z. B. Abweichungen vom Soll-Prozessverlauf) sowie kennzahlenbasiert (z. B. Abweichung von durchschnittlichen Durchlaufzeiten) dargestellt werden. Indem ein Soll-Ist Abgleich zwischen dem modellierten Soll-Prozess und den tatsächlichen Ist-Prozessverläufen durchgeführt wird, können risikobehaftete Prozessflusselemente identifiziert werden. Entweder werden diese Erkenntnisse dann direkt durch Änderung des Soll-Prozessdesigns umgangen oder eingeplant, indem das Soll-Prozessmodell im RMIS mithilfe der in dieser Arbeit entwickelten Risikonotation für Geschäftsprozessmodelle um die identifizierten Risikophänomene erweitert wird. Dazu wird über die Funktion *Risiken erfassen* ein Editor bereitgestellt, der die Modellierung der Risikonotationssymbole entlang der BPMN Soll-Prozessmodelle erlaubt.

Datensicht

Das Datenschema, welches die Speicherung im Prozessmodell modellierter Risikophänomene auf Basis der risikoorientierten Prozessnotation (ROPN) erlaubt, ist in Abbildung 90 dargestellt. Es spiegelt die risikobezogenen Beziehungen wider, die ein Anwender im Editor des hier vorgestellten RMIS modellieren kann. So wird die Erfassung aller Elemente der risikoorientierten Prozessnotation aus Kapitel 7.5.2.4., die zur Modellierung der Risiken, der Beziehungen zwischen den Risiken und der Beziehungen zwischen Risiken und den Prozesselementen benötigt werden, ermöglicht.

Ein Risiko hat üblicherweise einen Verantwortlichen. Entsprechend wird dem E-Typ *Risiko* über den R-Typ *Risk Owner* ein Partizipierender des Prozesses zugewiesen. Dieser wird durch diese Zuordnung zum *Risk Owner* für dieses Risiko. Da es vorkommen kann, dass zum Zeit-

punkt der Erfassung des Risikos noch keine Verantwortlichkeiten definiert wurden, wird die Verbindung als (0, 1)-Kante modelliert. Je Risiko kann weiterhin maximal ein Verantwortlicher benannt werden, da sonst die Verantwortung nicht eindeutig ist und gegebenenfalls einzuleitende Risikosteuerungsmaßnahmen aufgrund unklarer Zuständigkeit nicht ausgeführt werden. Ein Partizipierender kann für kein, ein oder mehrere Risiken verantwortlich sein.



Risiko (R-ID, Bezeichnung, Beschreibung)
Risikoart (RA-ID, Bezeichnung)
R-RA-Zuordnung(R-ID, RA-ID)
Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Partizipierender (PART-ID)
Risk Owner (PART-ID, R-ID)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit)
Risiko-Prozessziel-Einfluss (R-ID, PZGS-ID)
Prozessflusselement (PFE-ID, P-ID, SP-ID, Bezeichnung)
Prozess-Risikobezug (PRB-ID, PFE-ID, R-ID)
Risiko-Prozessbezug (RPB-ID, R-ID, PFE-ID)
Risikokorrelation (RKO-ID, Risiko1-ID, Risiko2-ID)

Risikolink (RL-ID, Name)
Risikolinkquelle (RL-ID, RLQ-ID)
Risikolinksenke (RL-ID, RLS-ID)
PRB-RL-Bezug (PRB-ID, RL-ID)
RPB-RL-Bezug (RPB-ID, RL-ID)
RKO-RL-Bezug (RKO-ID, RL-ID)
Risiko-RL-Bezug (UWZ-ID, RL-ID)
U-W-Zusammenhang (UWZ-ID, Bezeichnung)
Prämisse (PR-ID, UWZ-ID)
P-Bestandteil (PR-ID, R-ID)
Prämissenlogik (PR-ID, Risiko1-ID, Risiko2-ID, Junktor)
Konklusion (KO-ID, UWZ-ID)
K-Bestandteil (KO-ID, R-ID)
Konklusionslogik (KO-ID, Risiko1-ID, Risiko2-ID, Junktor)

Abbildung 90: Datenmodell Risikomodell und Risiko-Prozessbezüge

Die Prozesselemente und Risiken die zunächst keinem Partizipierenden zugeordnet werden, sind von der Anwendungslogik in einer Lane darzustellen, die keine Information über die Verantwortlichkeit enthält.

Falls das Risiko Einfluss auf Prozessflusselemente, wie z. B. eine Funktion, ausübt, wird dies in der risikoorientierten Prozessnotation (ROPN) mittels der Risiko-Prozess-Bezüge (siehe Abbildung 60) modelliert. Diese Beziehungen werden im ER-Typ *Risiko-Prozessbezug* festgehalten. Wenn ein Prozessflusselement ein Risiko verursacht, wird dies in der ROPN über Prozess-Risikobezüge dargestellt und im SERM mittels des ER-Typs *Prozess-Risikobezug* abgebildet. Etwaig modellierte Korrelationsbeziehungen zwischen Risiken werden im ER-Typ *Risikokorrelation* erfasst.[475] Da ein Risiko immer auf mindestens ein oder mehrere Prozessziele wirkt, sind diese Beziehungen über den R-Typ *Risiko-Prozessziel-Einfluss* realisiert.

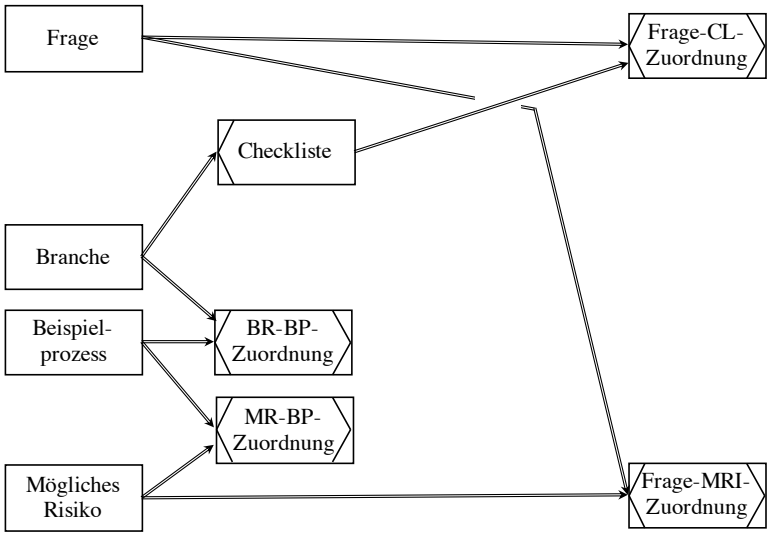
Die in der ROPN modellierten Ursache-Wirkungs-Zusammenhänge zwischen zwei oder mehreren Risiken (Risiko-Ursache-Wirkungsketten) werden im Datenmodell in Form von Prämissen und Konklusionen modelliert. Ein Risiko kann dabei Bestandteil ein oder mehrerer Prämissen bzw. Konklusionen sein. Soll lediglich zwischen zwei Risiken ein Ursache-Wirkungszusammenhang abgebildet werden, so existiert für das ursächliche Risiko als Element des ER-Typs *P-Bestandteil* kein Eintrag im ER-Typ *Prämissen-Logik*. Sollen mehr als zwei Risiken in einer Risiko-Ursache-Wirkungskette abgebildet werden, kann über die ER-Typen *Prämissenlogik* und *Konklusionslogik* jeglicher logische Zusammenhang von Ursachen und Wirkungen flexibel beschrieben werden.

Im Rahmen der Risikostammdatenerfassung wird jedes Risiko mindestens einer Risikoart zugewiesen. Dieser Zusammenhang wird im R-Typ *R-RA-Zuordnung* erfasst.

Der in der ROPN eingeführte Risikolink zur pool- und prozessübergreifenden Verbindung von Risikoflüssen, Risikokorrelationen oder Risiko-Prozess-Bezügen (siehe Abbildung 64), wird über einen eigenen E-Typ *Risikolink* repräsentiert. Ein Risikolink besteht immer aus einer Risikolinkquelle und einer -senke, die jeweils mit mehreren unterschiedlichen Verbindungspfaden (Risikoflüssen, Risikokorrelationen, etc.) verbunden sein können. Diese Verbindungen werden über entsprechende R-Typen (z. B. *PRB-RL-Bezug*) modelliert. Ein Ursache-

[475] Gemäß dem o.g. sukzessiven Aufbau der Datenmodelle in diesem Kapitel werden dieser und weitere Objekttypen im weiteren Verlauf der Arbeit um neue Attribute (z. B. zur Risikoquantifizierung) ergänzt.

Wirkungs-Zusammenhang zwischen zwei Risiken kann auf diese Weise auch prozessübergreifend modelliert werden (*Risiko-RL-Bezug*).



Checkliste (CL-ID, B-ID, Bezeichnung, Beschreibung)
Branche (B-ID, Bezeichnung)
Frage-CL-Zuordnung (Frage-ID, CL-ID)
Frage (Frage-ID, Fragetext)
Beispielprozess (BP-ID, Prozessname, Beschreibung)
BR-BP-Zuordnung (B-ID, BP-ID)
Mögliches Risiko (MRI-ID, Name)
MR-BP-Zuordnung (MRI-ID, BP-ID)
Frage-MR-Zuordnung (Frage-ID, MRI-ID)

Abbildung 91: SERM Checkliste

Die Bereitstellung von Checklisten als simple Methode zur Unterstützung der Risikoidentifizierung, wird durch den E-Typ *Checkliste* realisiert (siehe Abbildung 91). Eine Checkliste ist immer genaue einer Branche zugeordnet und besteht aus mehreren Fragen, die sich jeweils auf branchentypische potentielle Risiken beziehen. Des Weiteren sind die potentiellen Risiken branchenüblichen Beispielprozessen zugeordnet. Als Ergebnis der Beantwortung einer Checkliste kann ein Anwender für ihn relevante Risiken erkennen. Anhand der Beispielprozesszuordnung wird für ihn ersichtlich, wo sich die erkannten Risiken üblicherweise auswirken können. Dies kann er bei der Modellierung der eigenen Prozesse und Risiken im risikoorientierten Prozessmodell berücksichtigen. Die Objekttypen der Checklistenfunktionalität stehen in keinem direkten Bezug zu den übrigen Objekttypen des RMIS, da die Checkliste

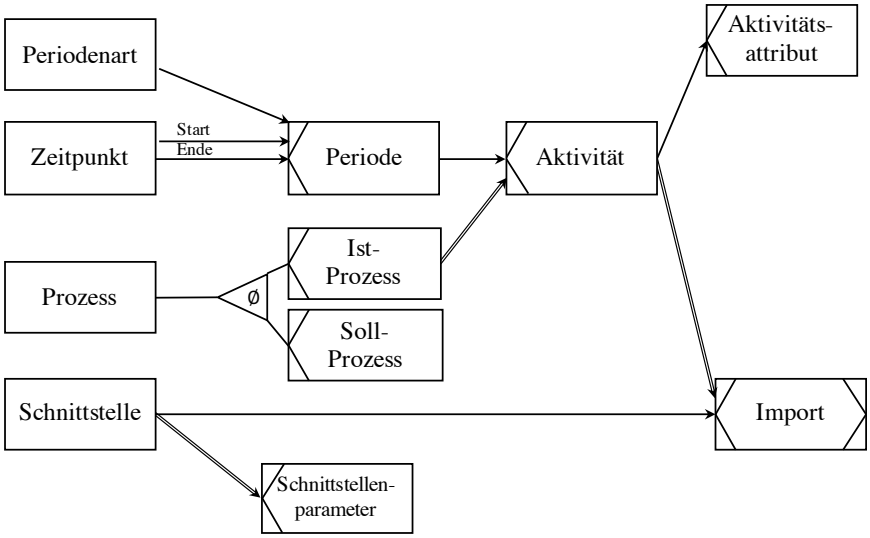
lediglich eine Identifizierungshilfe für den Anwender darstellt, die keine Integration mit dem Gesamtmodell erfordert.

Neben der Erfassung intellektuell identifizierter Risiken bietet das RMIS die Möglichkeit moderne Methoden der Datenanalyse auf tatsächliche Geschäftsvorfälle anzuwenden, um risikobehaftete Geschäftsprozesse zu erkennen. Da Prozesse bei jedem Durchlauf in unterschiedlicher Art und Weise ablaufen können, existieren gegebenenfalls unterschiedliche Varianten eines Ist-Prozesses. Die maschinelle Analyse der Prozesse der Vergangenheit ist daher von Interesse, um häufig auftretende Varianten, die risikoreiche Abweichungen vom geplanten Sollverlauf darstellen, aufzudecken. Jeder Prozess besteht aus mehreren Aktivitäten, den sogenannten Prozessschritten. Bei einem Kreditorenprozess gibt es z. B. die Aktivitäten:

1. Scanne Rechnung.
2. Buche Rechnung.
3. Bezahle Rechnung.

Sind diese Aktivitäten mit ihrer Zugehörigkeit zu einem Durchlauf des Prozesses (sog. Prozessinstanz) und mit mindestens einem Start-Zeitstempel digital erfasst (z. B. in einem ERP System), können mittels Process Mining Verfahren die tatsächlichen Prozessverläufe vom RMIS analysiert und gespeichert werden (siehe Kapitel 4.2.2). Das zugehörige Datenschema zum Import von Prozessaktivitäten ist in Abbildung 92 dargestellt. Zunächst muss das RMIS die Möglichkeit bieten, die digital erfassten Aktivitätsbelege sowie ihre Zugehörigkeit zu einem Prozessdurchlauf zu importieren. Dazu können im RMIS Schnittstellen zu externen Informationssystemen definiert werden. Eine Schnittstelle kann z. B. eine API-Anbindung an ein ERP System sein. Schnittstellenspezifische Parameter wie z. B. eine URL, Zugangsdaten und Aufrufparameter sowie ihre jeweiligen Werte, werden über den ER-Typ *Schnittstellenparameter* erfasst. Die Aktivitätsbelege können nur per Import und nicht manuell in das RMIS aufgenommen werden, da die Verwaltung der Belege in den dafür vorgesehenen Informationssystemen und nicht im RMIS erfolgen soll. Jede importierte Aktivität muss weiterhin mindestens über einen Startzeitpunkt verfügen, damit Process Mining Verfahren angewendet werden können. Zur genaueren Analyse ist der Import des jeweiligen Endzeitpunktes wün-

schenswert, da ansonsten der Startzeitpunkt der nächsten Aktivität als Endzeitpunkt der vorhergehenden Aktivität vom Process Mining Verfahren angenommen wird. Entsprechend ist der ER-Typ *Aktivität* vom ER-Typ *Periode* abhängig. Sollten weitere Daten zu den Aktivitäten vorliegen, die für das Process Mining von Interesse sein können (z. B. die ausführende Ressource der Aktivität), können diese Daten im ER-Typ *Aktivitätsattribut* abgebildet werden.

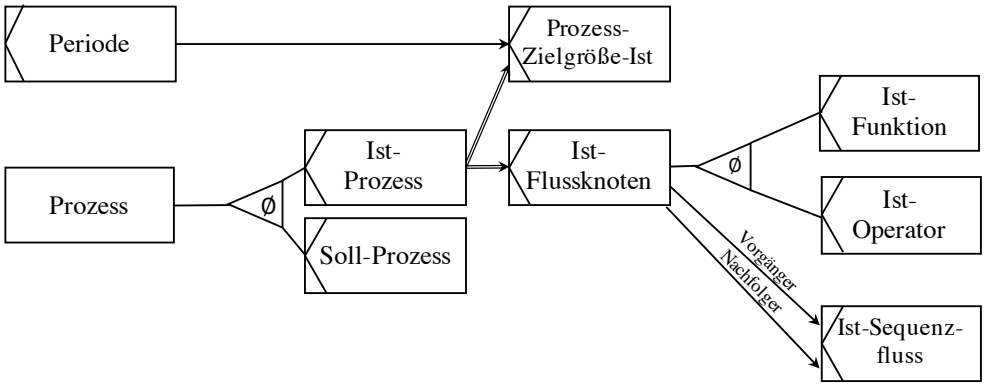


Periodenart (PA-ID, Art)
Zeitpunkt (Z-ID, Zeitpunkt)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Prozess (P-ID, Bezeichnung)
Ist-Prozess (IP-ID, P-ID)
Soll-Prozess (SP-ID, P-ID)
Aktivität (AK-ID, IP-ID, PE-ID, Bezeichnung)
Aktivitätsattribut (AKA-ID, AK-ID, Bezeichnung, Wert)
Schnittstelle (SST-ID, Bezeichnung)
Schnittstellenparameter (SST-P-ID, SST-ID, Bezeichnung, Wert)
Import (SST-ID, AK-ID)

Abbildung 92: Datenmodell Aktivitätsimport

Durch die Anwendung des Process Mining auf die importierten Aktivitätsdaten können nun alle tatsächlichen Prozessvarianten der Vergangenheit ermittelt werden. Diese werden im Datenmodell in Abbildung 93 erfasst. Pro Variante eines Prozesses lassen sich die tatsächlichen Ausprägungen von Zielgrößen wie z. B. die Durchlaufzeit ermitteln. Diese werden im ER-Typ *Prozess-Zielgröße-Ist* festgehalten. Falls Kosteninformationen Teil des Importvorgangs

waren, kann zudem eine monetäre Bewertung der Ist-Zielgröße erfolgen. Die vom Process Mining Verfahren ermittelte Zusammensetzung von Prozesselementen, wird über die ER-Typen *Ist-Flussknoten, Ist-Funktion* und *Ist-Operator* abgebildet. Jede Kombination dieser Elemente stellt einen Ist-Prozess bzw. eine Variante des Ist-Prozesses dar. Vom RMIS können die am häufigsten vorkommenden Prozessvarianten und auffällige Ist-Prozessvarianten dem Anwender visuell hervorgehoben dargestellt werden. Weiterhin ist ein visueller Vergleich mit den zughörigen modellierten Soll-Prozessen möglich und ein Vergleich der Soll- und Ist-Prozess-Zielgrößen. Auf diese Weise können Soll-Ist Abweichungen erkannt werden und somit der Identifizierung potentieller Risiken im Prozess dienen. Diese Erkenntnisse können anschließend für die Umgestaltung der Soll-Prozesse oder die Modellierung der erkannten Risiken im risikoorientierten Prozessmodell genutzt werden.



Prozess (P-ID, Bezeichnung)
Ist-Prozess (IP-ID, P-ID)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Ist-Funktion (IFLK-ID, IP-ID, PE-ID, Bezeichnung)
Ist-Operator (IFLK-ID, Junktor)
Ist-Sequenzfluss (IFLK-ID, Vorgänger-IFLK-ID, Nachfolger-IFLK-ID)

Abbildung 93: Datenmodell Process Mining

Steuerungssicht

Die Phase der Risikoidentifizierung folgt im RMIS dem folgenden Ablauf. Der verantwortliche Risk Owner beginnt die Risikoidentifizierung für einen ihm zugewiesenen Prozess. Diesen wählt er zunächst aus dem Pool bestehender Prozessmodelle aus. Entweder bedient er sich einer Unterstützungsmethode zur Risikoidentifizierung oder er identifiziert das Risiko direkt

im Prozessmodell aufgrund seines Erfahrungswissens. Im Anschluss modelliert er das Risiko im Prozessmodell mittels der ROPN. An die Modellierung schließt sich die Erfassung der Risikostammdaten an. Entweder werden dann weitere Risiken identifiziert und modelliert oder die Risikoidentifizierung beendet.

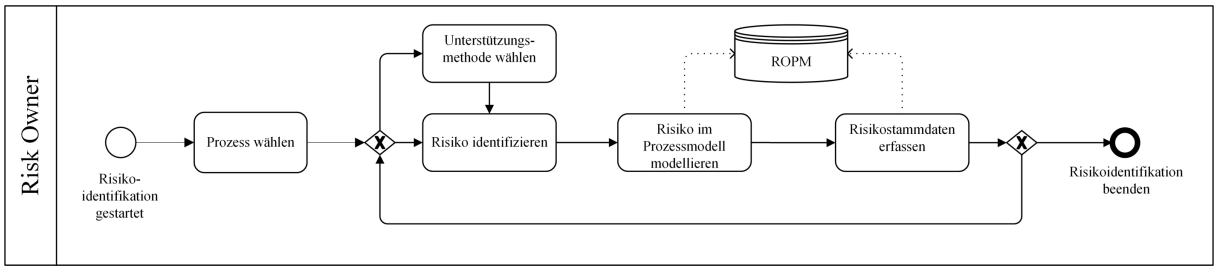


Abbildung 94: Prozessmodell Risikoidentifizierung

9.2.4. Detailsichten für die Risikoquantifizierung

Funktionssicht

Damit Risiken adäquat quantifiziert werden können, verlangt das RMIS grundsätzlich für jedes Risiko die Zuordnung einer Verteilungsfunktion. Dem Anwender werden dazu gängige Verteilungsfunktionen vom RMIS zur Auswahl angeboten und die jeweiligen Verteilungsparameter erfragt. Liegt seitens der Anwender keine Information über die Verteilung vor, bietet das RMIS Funktionen an, um diese anzunähern. Dies erfolgt für ein Einzelrisiko entweder auf Basis historischer Daten mittels einer Historischen Simulation, mittels einer Monte Carlo Simulation oder durch Expertenbefragung unter Anwendung eines Fuzzy-Regelsystems.[476] Wurden Verteilungsinformationen festgelegt oder angenähert, kann das RMIS anschließend gängige Risikomaße wie z. B. den Value at Risk berechnen und Risiken so mit anderen Risiken direkt vergleichbar machen. Die Quantifizierung von Risikowechselwirkungen erfolgt über den Korrelationskoeffizienten. Dieser wird entweder geschätzt oder rechnerisch auf Basis der historischen Ausprägungen der Risiken, für welche die Korrelationsbeziehung beschrieben wird, bestimmt. Zur Ermittlung des Gesamtrisikoausmaßes unterstützt das RMIS jegliche verteilungsbasierten Aggregationsverfahren (siehe Kapitel 4.3.2.4).

[476] Für die Bestimmung der Verteilungsfunktion eines Einzelrisikos können durchaus dieselben Verfahren genutzt werden, die auch im Rahmen der Risikoaggregation zur Bestimmung einer Gesamtverteilung mehrerer Einzelrisiken genutzt werden (siehe Kapitel 4.3.2.4).

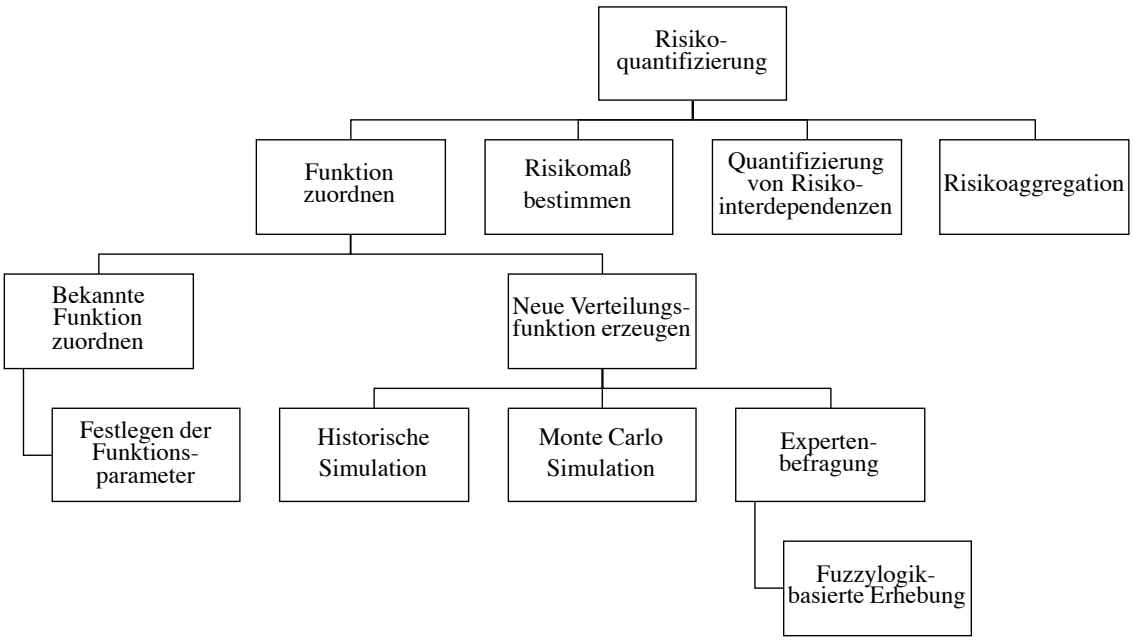
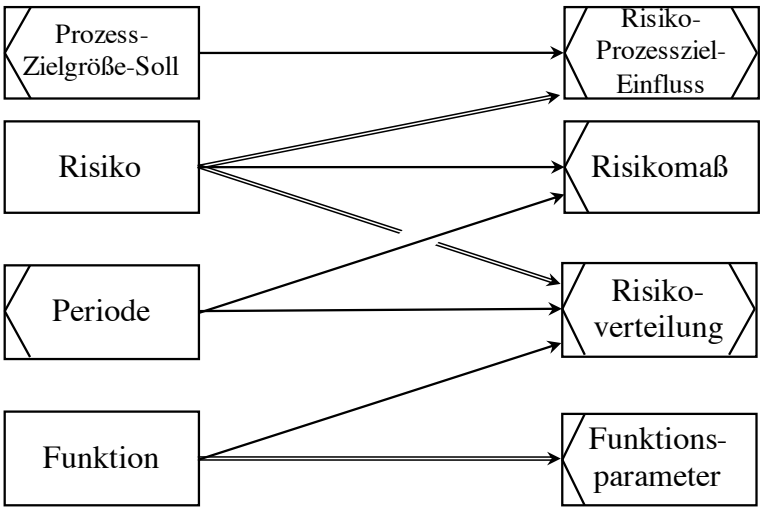


Abbildung 95: Funktionsbaum Risikoquantifizierung

Datensicht

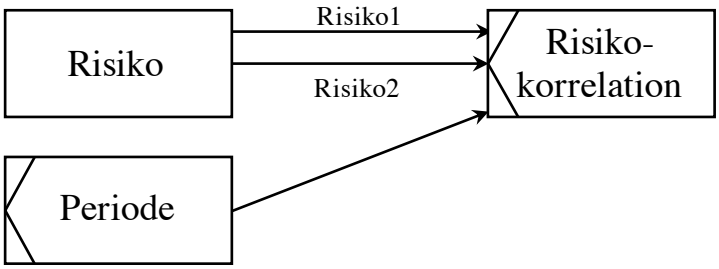
Im SERM zur Risikoquantifizierung (siehe Abbildung 96) wird jedem Risiko im R-Typ *Risikoverteilung* für eine Periode genau eine Verteilungsfunktion zugeordnet, welche einem Schadensausmaß eine Eintrittswahrscheinlichkeit zuordnet. Eine Verteilungsfunktion wird mittels des E-Typs *Funktion* beschrieben. Sie besitzt gegebenenfalls mehrere Verteilungsparameter wie z. B. einen Erwartungswert der im ER-Typ *Funktionsparameter* erfasst werden kann. Durch die Zuweisung beliebig vieler Funktionsparameter, lassen sich mit dem E-Typ *Funktion* beliebige Verteilungsfunktionen oder auch andere Funktionen flexibel beschreiben. Damit dem quantifizierten Risiko eine Plangröße (ER-Typ *Prozess-Zielgröße-Soll*), die es beeinflusst, zugeordnet werden kann, erfolgt über den R-Typ *Risiko-Prozessziel-Einfluss* eine Verbindung zu den quantifizierten Prozesszielgrößen. Dabei beeinflusst ein Risiko mindestens eine Zielgröße, da es ansonsten nicht modelliert werden müsste bzw. kein Risiko darstellen würde. Mit der Verteilungsfunktion des Risikos, lässt sich ein Risikomaß wie z. B. der Value at Risk bilden, welches im ER-Typ *Risikomaß* abgebildet wird.



Risiko (R-ID, Bezeichnung, Beschreibung)
Risikomaß (RM-ID, PE-ID, R-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Risiko-Prozessziel-Einfluss (R-ID, PSZG-ID)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Funktion (F-ID, Bezeichnung, Typ)
Funktionsparameter (FP-ID, F-ID, Bezeichnung, Ausprägung)
Risikoverteilung (R-ID, PE-ID, F-ID)

Abbildung 96: Datenmodell Risikoquantifizierung

Abbildung 97 stellt das SERM zur Abbildung von Risikokorrelationsbeziehungen dar. Eine Korrelation besteht immer für eine bestimmte Periode, da sich der Grad der Korrelation im Verlauf ändern kann. Im ER-Typ *Risikokorrelation* wird der Grad des Zusammenhangs zwischen zwei Risiken mittels des Korrelationskoeffizienten erfasst.

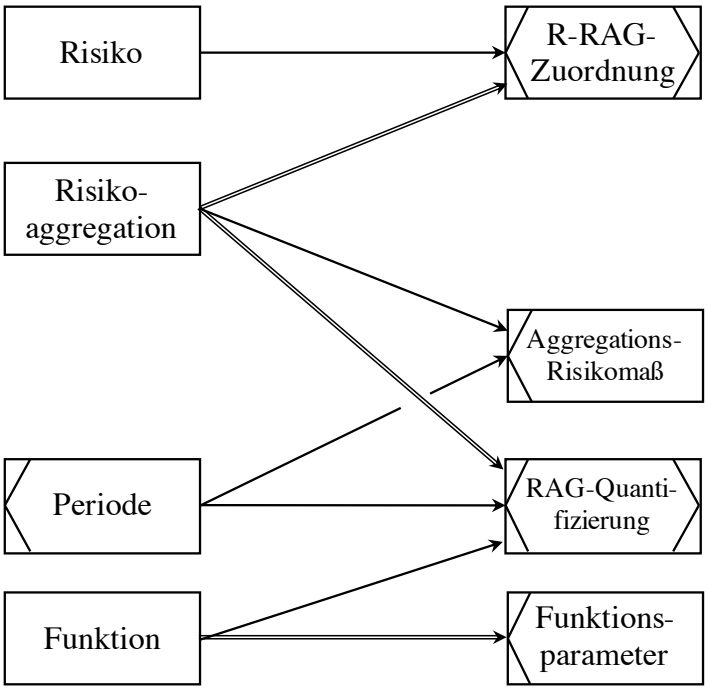


Risiko(R-ID, Bezeichnung, Beschreibung)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Risikokorrelation(RKO-ID, PE-ID, Risiko1-ID, Risiko2-ID,
Vorzeichen, Korrelationskoeffizient)

Abbildung 97: SERM Risikokorrelation

Zur Aggregation von Einzelrisiken ist die gemeinsame Verteilung der Risiken festzulegen bzw. zu bilden und im RMIS zu erfassen (siehe Abbildung 98).[477] Die Auswahl der Risiken, die zu aggregieren sind, erfolgt über die Anwendungslogik. Die Zuordnung eines Risikos zu einer Risikoaggregation wird über den R-Typ *R-RAG-Zuordnung* realisiert. Ein Risiko kann dabei Teil mehrerer Risikoaggregationen sein. Letztere besteht immer aus mehreren Risiken. Wenn die Gesamtverteilung bekannt und bereits als ein Tupel im E-Typ *Funktion* abgebildet ist, kann sie der Risikoaggregation über den R-Typ *RAG-Quantifizierung* zugewiesen werden. Eine Aggregation von Einzelrisiken bezieht sich stets auf eine bestimmte Periode und eine für diese Periode gültige Gesamtverteilungsfunktion der Risiken. Diese Beziehung wird mit Hilfe des ER-Typs *Periode* und des E-Typs *Funktion* im R-Typ *RAG-Quantifizierung* abgebildet. Wie bereits bei den Einzelrisiken lassen sich aus der Verteilung einer Risikoaggregation Risikomaße bilden. Diese werden im ER-Typ *Aggregations-Risikomaß* erfasst.

[477] Zur Erläuterung der Verfahren der Risikoaggregation siehe Kapitel 4.3.2.4.

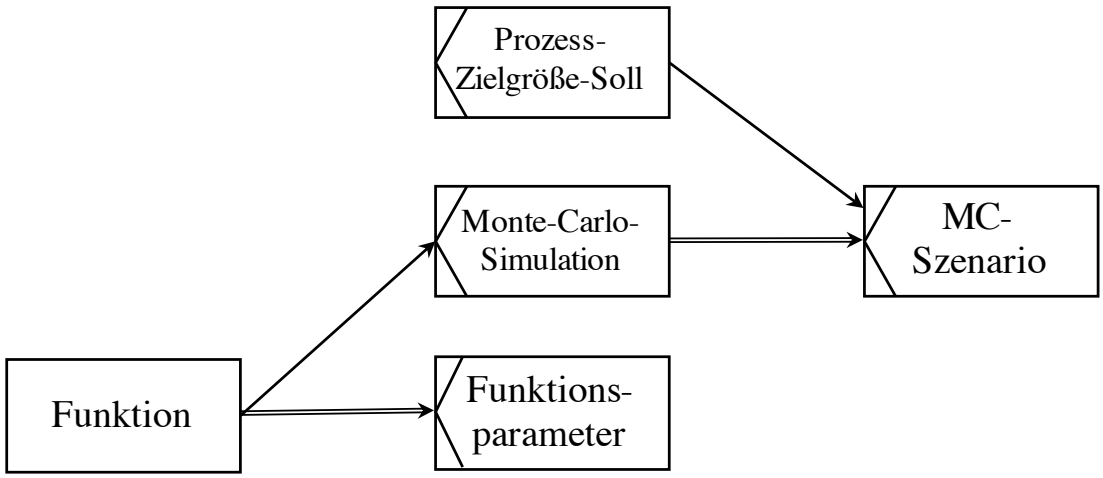


Risiko (R-ID, Bezeichnung, Beschreibung)
Risikoaggregation (RAG-ID, Bezeichnung, Aggregationsverfahren)
R-RAG-Zuordnung (RAG-ID, R-ID)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Funktion (F-ID, Bezeichnung, Typ)
Funktionsparameter (FP-ID, F-ID, Bezeichnung, Ausprägung)
RAG-Quantifizierung (RAG-ID, PE-ID, F-ID)
Aggregations-Risikomaß (ARM-ID, PE-ID, RAG-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)

Abbildung 98: SERM Risikoaggregation

Ist die Verteilung eines Einzelrisikos oder die Gesamtverteilung von zu aggregierenden Risiken nicht bekannt, ermöglicht das RMIS die Annäherung dieser mittels simulationsbasierter Verfahren (siehe Kapitel 4.3.2.4) und Expertenbefragungen. Im Ergebnis wird jeweils eine angenäherte Verteilung ermittelt, die dann als eine neue Verteilungsfunktion im E-Typen *Funktion* gespeichert und über den R-Typen *Risikoverteilung* dem Einzelrisiko bzw. *RAG-Quantifizierung* der ausgewählten Risikoaggregation zugewiesen werden kann. Zur Annäherung einer Gesamtverteilungsfunktion werden in der Praxis überwiegend die Monte Carlo Simulation und die Historische Simulation angewendet.

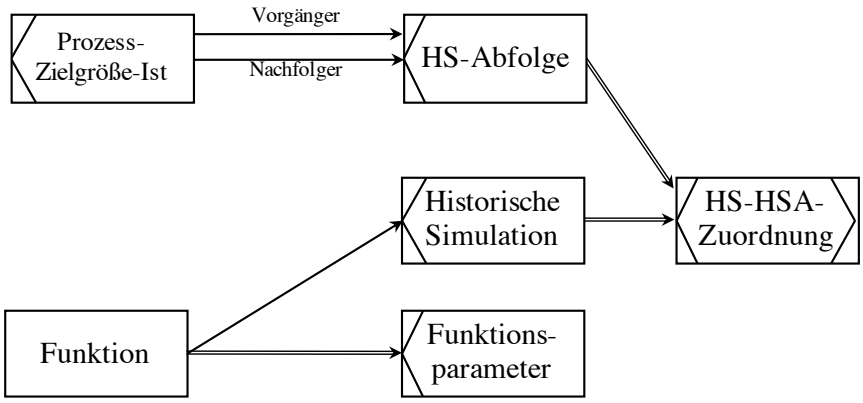
Eine Monte Carlo Simulation (siehe Abbildung 99) besteht aus mehreren Zufallsexperimenten (sog. Szenarien), die jeweils für eine Zielgröße (hier die monetäre Bewertung im ER-Typ *Prozess-Zielgröße-Soll*) einen Zufallswert generieren. Dieser wird im ER-Typ *MC*-Szenario festgehalten. Jeder generierte *Zielgrößenszenariowert* unterliegt dabei den Risiken die Teil der Risikoaggregation sind und Einfluss auf die Zielgröße haben (siehe Abbildung 96 und Abbildung 98). In Abhängigkeit der Verteilungen der Einzelrisiken und ihres Einflusses auf die Zielgröße, wird in vielen (tausenden) Simulationsläufen je ein Zufallswert für die Zielgröße erzeugt. Aus den so generierten Szenariowerten der Zielgröße wird eine empirische Häufigkeitsverteilung gebildet, die als Schätzer verwendet werden kann. Diese wird im E-Typ *Funktion* bzw. ihre Eigenschaften im ER-Typ *Funktionsparameter* festgehalten und kann dann dem E-Typen Risikoaggregation zugewiesen werden (über den R-Typ *RAG-Quantifizierung* in Abbildung 98). Jeder erzeugten Monte Carlo Simulation liegt so genau eine Verteilungsfunktion zugrunde.



Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Monte-Carlo-Simulation (MCS-ID, F-ID, Bezeichnung)
MC-Szenario (MCSZ-ID, PZGS-ID, MCS-ID, Zielgrößenszenariowert)
Funktion (F-ID, Bezeichnung, Typ)
Funktionsparameter (FP-ID, F-ID, Bezeichnung, Ausprägung)

Abbildung 99: SERM Verteilungsannäherung mittels Monte-Carlo Simulation

Die Historische Simulation benötigt Zeitreihendaten, die sich aus den importierten Aktivitäten und den daraus ermittelten historischen Prozess-Zielgrößen beziehen lassen (siehe Abbildung 92 und Abbildung 93). Nach Zeitpunkt geordnet kann die Abfolge der Belege im Objekttyp *HS-Abfolge* mit der jeweiligen relativen oder absoluten Änderung zwischen zwei Zeitpunkten erfasst werden (siehe Abbildung 100). Mit einer hinreichend großen Anzahl an Vergangenheitswerten lässt sich so für jede Historische Simulation eine Verteilungsfunktion bestimmen (siehe Kapitel 4.3.2.4). Diese wird ebenfalls im E-Typ *Funktion* erfasst und kann so der Risikoaggregation über den R-Typ *RAG-Quantifizierung* zugewiesen werden. Jeder erzeugten Historischen Simulation liegt ebenfalls genau eine Verteilungsfunktion zugrunde.

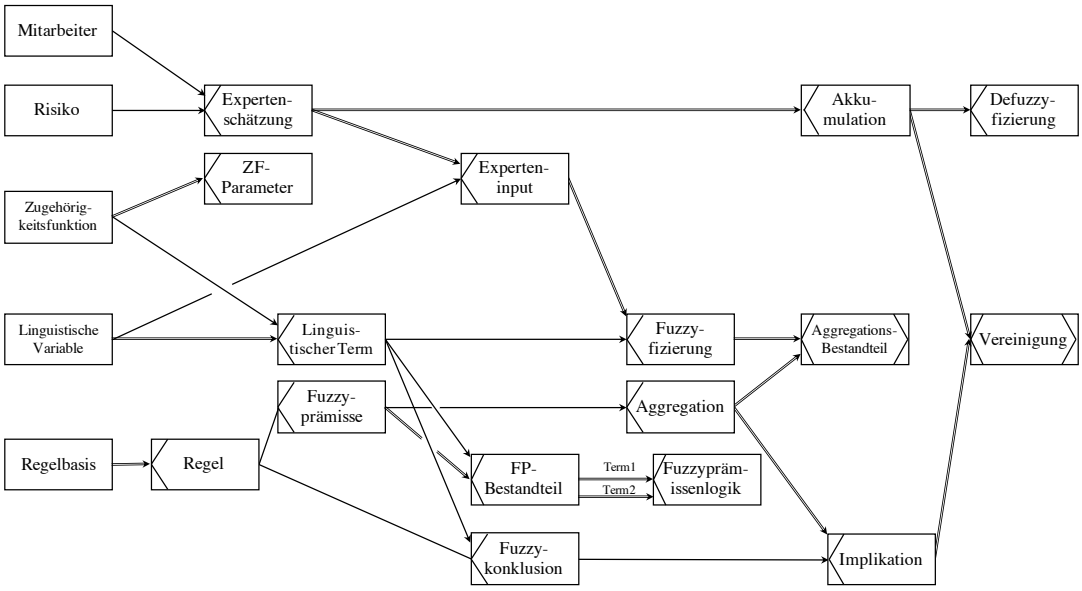


Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Historische-Simulation (HS-ID, F-ID, Bezeichnung, Referenzwert)
HS-Abfolge (HSA-ID, Vorgänger-PZGI-ID, Nachfolger- PZGI-ID, relative-Änderung, absolute Änderung)
HS-HSA-Zuordnung (HS-ID, HSA-ID)
Funktion (F-ID, Bezeichnung, Typ)
Funktionsparameter (FP-ID, F-ID, Bezeichnung, Ausprägung)

Abbildung 100: SERM Verteilungsannäherung mittels Historischer Simulation

Zur Annäherung der unbekannten Verteilung eines Einzelrisikos bieten sich Expertenbefragungen zur Einschätzung eines Risiko an. Da solche Einschätzungen für die Experten vielfach einfacher in qualitativen Größen abzugeben sind, bietet sich das bereits erwähnte Fuzzy-basierte Verfahren zur Ermittlung einer Verteilungsfunktion an. Dazu wird das SERM um entsprechende Objekttypen erweitert (siehe Abbildung 101). So können Eintrittswahrschein-

lichkeit, Schadensausmaß und Risiko als linguistische Variablen modelliert werden, die wiederum jeweils durch linguistische Terme wie z. B. gering, mittel, hoch charakterisiert werden.



Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Risiko (R-ID, Bezeichnung, Beschreibung)
Expertenschätzung (ES-ID, M-ID, R-ID)
Zugehörigkeitsfunktion (ZF-ID, Bezeichnung)
ZF-Parameter (ZFPA-ID, Bezeichnung, Ausprägung)
Linguistische-Variable (LV-ID, Bezeichnung, Min, Max, Einheit)
Linguistischer-Term (LT-ID, LV-ID, ZF-ID, Bezeichnung)
Experteninput (ESI-ID, ES-ID, LV-ID, Ausprägung)
Fuzzyfizierung (FUZ-ID, ES-ID, ESI-ID, LT-ID, Zugehörigkeitsgrad)
Aggregations-Bestandteil (FUZ-ID, AGG-ID, ES-ID)
Regelbasis (REB-ID, Bezeichnung)

Regel (RE-ID, REB-ID, Bezeichnung)
Fuzzyprämisse (FPR-ID, RE-ID)
FP-Bestandteil (FPR-ID, LT-ID)
Fuzzyprämissenlogik (FPR-ID, Term1-ID, Term2-ID, Junktor)
Fuzzykonklusion (FKO-ID, RE-ID, LT-ID)
Aggregation (AGG-ID, PR-ID, Erfüllungsgrad-Prämisse)
Implikation (IM-ID, AGG-ID, KO-ID, Inferenzmethode, Erfüllungsgrad-Konklusion)
[Methode: Max-Min- oder Max-Prod-Inferenz - je nach konkreter Anwendung]
Vereinigung (IM-ID, AKK-ID)
Akkumulation (AKK-ID, ES-ID)
Defuzzyfizierung (DEFUZZ-ID, AKK-ID, ES-ID, Defuzzifizierungsmethode, Wert)

Abbildung 101: Datenmodell Fuzzy-Regler

Jeder linguistische Term hat genau eine Zugehörigkeitsfunktion, welche definiert, zu welchem Grad ein Eingangswert (der Experteninput) zu der Menge, die der linguistische Term beschreibt, gehört. Des Weiteren ist mit den linguistischen Termen ein Regelsystem, bestehend aus Prämissen und Konklusionen zu definieren. Dieses wird im E-Typ *Regelbasis* erfasst und besteht aus mehreren Regeln, die jeweils im ER-Typ *Regel* abgebildet sind. Jede Regel besteht aus einer Prämisse und einer Konklusion. Die linguistischen Terme, welche Bestandteil einer *Fuzzyprämisse* sind, werden im ER-Typ *FP-Bestandteil* festgehalten. Die Bestandteile sind über logische Verknüpfungen miteinander verbunden. So lassen sich Regeln für alle Kombinationen von zwei Prämissenbestandteilen und eine daraus resultierende Konklusion, wie bspw. „Wenn die Eintrittswahrscheinlichkeit hoch ist und das Schadensausmaß

hoch ist, dann ist das Risiko hoch“, beschreiben. Die linguistischen Variablen und Terme sowie die Zugehörigkeitsfunktionen und das Regelsystem sind vor Nutzung des Fuzzy-Reglers von Domänenexperten festzulegen und im RMIS einzurichten. Ein Anwender kann so seine *Experteneinschätzung* für ein Risiko durch eine qualitative Einschätzung ausdrücken (z. B. Eintrittswahrscheinlichkeit sehr hoch und Schadensausmaß gering). Diese wird im ER-Typ *Experteninput* erfasst. Im Rahmen der Fuzzyfizierung wird der Zugehörigkeitsgrad jeder Experteneinschätzung zu der jeweiligen Fuzzy-Menge (im Beispiel gering, mittel und hoch) ermittelt. Im ER-Typ *Aggregation* werden die Erfüllungsgrade der Prämissen erfasst und im ER-Typ *Implikation* die Erfüllungsgrade der Konklusionen. Im ER-Typ *Akkumulation* werden die Ergebnisse aus allen Regeln zusammengefasst. Die Anwendungslogik bildet dazu aus allen zugehörigen Implikationen (über den R-Typ *Vereinigung*) die Gesamtfläche, die sich aus dem Experteninput und dem Regelset ergeben hat. Im Rahmen der Defuzzyfizierung wird mit entsprechenden Methoden (z. B. der Flächenschwerpunktmethode) ein spezifischer Ausgangswert gebildet. Als Ergebnis der Expertenschätzung unter Anwendung des Fuzzy-Reglers, kann der Anwender im E-Typ *Funktion* eine neue Verteilungsfunktion, z. B. eine Standardnormalverteilung, anlegen und als Funktionsparameter den im Rahmen der Defuzzyfizierung ermittelten Wert als Erwartungswert festlegen. Durch die Anwendung des Fuzzy-Reglers werden Informationslücken vermieden, die bspw. durch künstliche Mittelwertbildung oder bei einer klassenbasierten Einteilung (siehe Abbildung 10) entstehen, so dass die Einschätzungen der Experten etwas genauer erfasst werden können.

Steuerungssicht

Sind die Risiken identifiziert und im ROPM erfasst, können sie quantifiziert werden. In der Phase der Risikoquantifizierung muss im RMIS das zu quantifizierende Risiko zunächst ausgewählt werden (siehe Abbildung 102). Anschließend ist die Periode festzulegen, auf welche sich die Quantifizierung bezieht. Ist die Einzelverteilung eines Risikos noch nicht festgelegt, muss der Anwender diese entweder aus einer gegebenen Menge bekannter Verteilungen auswählen und etwaige Verteilungsparameter erfassen oder die Verteilung über die bekannten Verfahren (siehe Kapitel 4.3.2) annähern. Ist die Verteilung (dann) bestimmt, kann sowohl die Berechnung von Risikomaßen auf Basis der ermittelten Verteilung durchgeführt werden, als auch die Erfassung bekannter Korrelationen mit anderen Risiken festgehalten werden.

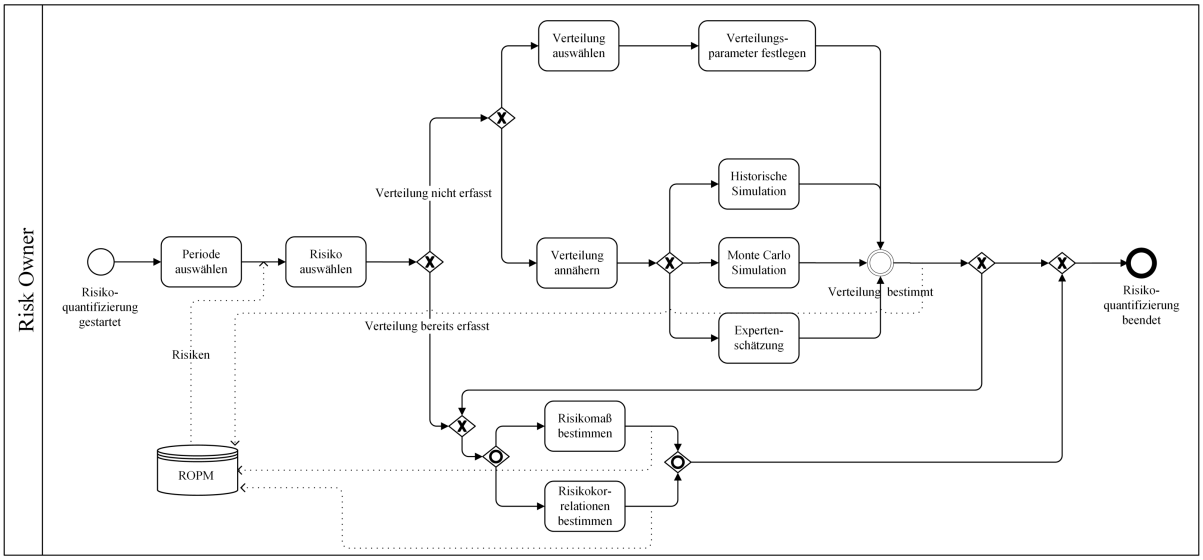


Abbildung 102: Prozessmodell Risikoquantifizierung

Für die Aggregation von Risiken, ist zunächst die Periode, für die das Gesamtrisiko bestimmt werden soll, zu selektieren (siehe Abbildung 103). Falls eines der zu aggregierenden Einzelrisiken für die gewählte Periode noch nicht quantifiziert wurde, wird es bei der Aggregation nicht berücksichtigt. Ein entsprechender Hinweis muss anwendungsseitig implementiert werden. Sind alle zu aggregierenden Einzelrisiken quantifiziert, kann die Gesamtverteilung durch Auswahl eines Aggregationsverfahren (z. B. Faltung der Einzelverteilungen, Historische Simulation, Monte Carlo Simulation) unter Angabe der notwendigen Parameter bestimmt werden. Optional kann nach Ermittlung der gemeinsamen Verteilung aller Einzelrisiken der Periode ein Risikomaß für die Gesamtverteilung , wie z. B. der Value at Risk, ermittelt werden.

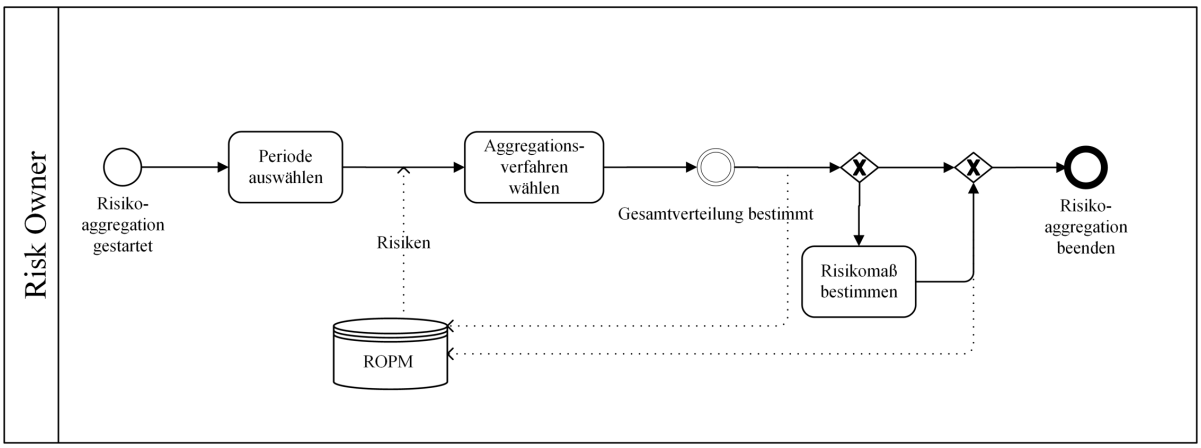


Abbildung 103: Prozessmodell Risikoaggregation

9.2.5. Detailsichten für die Risikobeurteilung

Funktionssicht

Zur Risikobeurteilung bietet das RMIS Funktionen zur Schwellenwertdefinition für jedes erfasste Risiko an und ermöglicht es jedem Risiko einen Priorisierungsgrad zuzuweisen. Im Rahmen der Definition eines Schwellenwertes ist zu festzulegen, ab welchem Differenzwert zwischen einer geplanten Soll- und einer Istgröße das Risiko als schlagend geworden angesehen wird. Damit eine Priorisierung der Risiken erfolgen kann, ermöglicht die Funktion *Klassenbildung* das Anlegen von Wesentlichkeitsklassen (z. B. A-Risiko, B-Risiko, C-Risiko) und über die Funktion *Risiko-Klassen-Zuordnung* kann ein Risiko einer zuvor erzeugten Klasse zugewiesen werden.[478]

[478] Ebenso wie im Rahmen der Risikoquantifizierung ist an dieser Stelle der Einsatz eines Fuzzy-Reglers denkbar, um eine genauere Zuordnung zu Risikoklassen zu realisieren bzw. um Risiken genauer zu gewichten. Zur Komplexitätsreduktion wird an dieser Stelle darauf verzichtet.

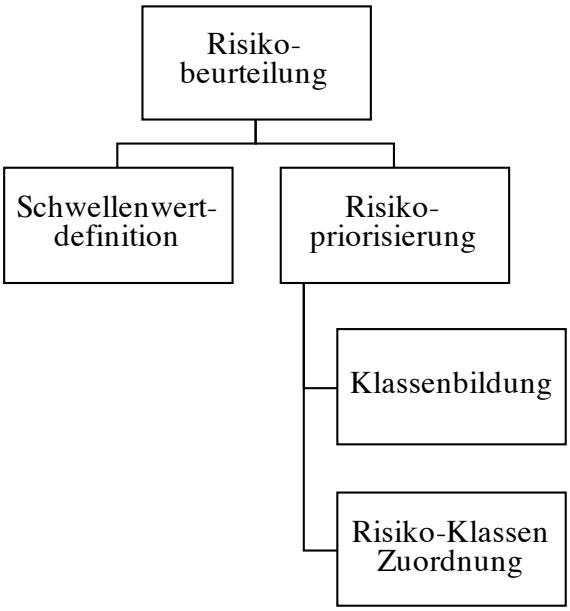
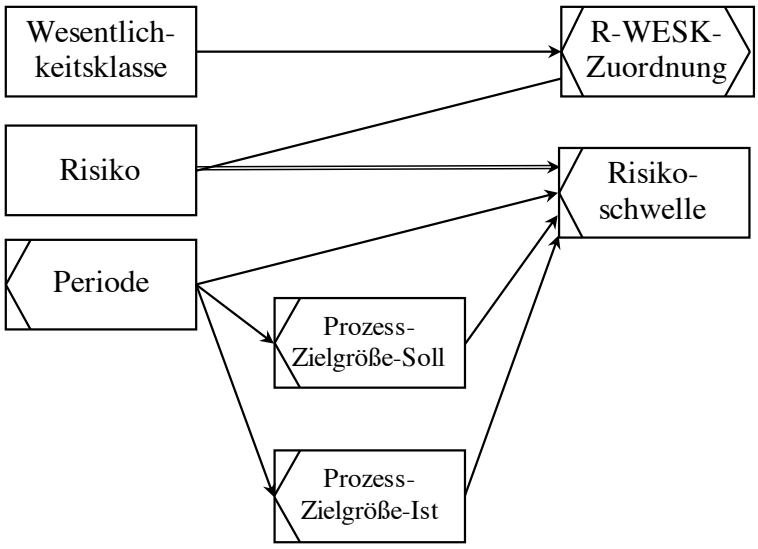


Abbildung 104: Funktionsbaum Risikobeurteilung

Datensicht

Zur Risikobeurteilung ist festzulegen, ab welchem Zustand das Risiko als eingetreten anzusehen ist. Dazu ist eine Schwelle im ER-Typ *Risikoschwelle* zu definieren (siehe Abbildung 105). In diesem ist die Differenz zwischen Soll- und Istgröße sowie Vergleichs- und Vorzeichen abgebildet. So wird definiert, ab welchem Wert bzw. welcher Wertüber- oder Wertunterschreitung das Risiko als eingetreten anzusehen ist. Das Datenschema berücksichtigt des Weiteren die Erfassung einer Wesentlichkeitsklasse zur Priorisierung eines Risikos. Ein Risiko kann keiner oder genau einer Klasse zugeordnet werden.



Wesentlichkeitsklasse (WESK-ID, Bezeichnung)
Risiko (R-ID, Bezeichnung, Beschreibung)
R-WESK-Zuordnung (WESK-ID, R-ID)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit)
Risikoschwelle (RS-ID, R-ID, PE-ID, PZGS-ID, PZGI-ID, Vergleichszeichen, Vorzeichen, Differenz-Schwellenwert)

Abbildung 105: Datenmodell Risikobeurteilung

Steuerungssicht

Zur Risikobeurteilung ist zunächst die Periode auszuwählen, um einerseits die Risikoauswahl gemäß dem spezifizierten Zeitraum einzuschränken und andererseits die Beurteilung des Risikos für diese konkrete Periode festzulegen. Im Anschluss wird das zu beurteilende Risiko ausgewählt und in Abhängigkeit von den Zielgrößen, die dem Risiko bereits in der Risikoidentifizierungsphase zugewiesenen wurden, entsprechende Schwellenwerte vom Anwender erfragt und erfasst. Im Anschluss besteht die Möglichkeit, dass der Anwender das Risiko einer Wesentlichkeitsklasse zuordnet, um Prioritäten für die spätere Risikosteuerung vorzugeben.

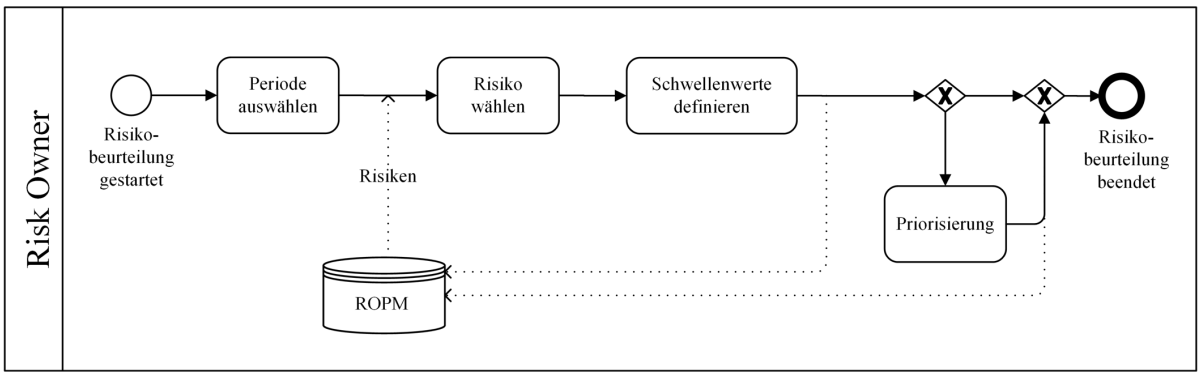


Abbildung 106: Prozessmodell Risikobeurteilung

9.2.6. Detailsichten für die Risikosteuerung

Funktionssicht

Das konzipierte RMIS fasst Funktionen zur Festlegung von Steuerungsmaßnahmen sowie zur Risikoüberwachung und -kontrolle als Risikosteuerungsfunktionen zusammen. Mithilfe der Funktion *Maßnahmenstammdaten erfassen* werden Eigenschaften erfasst, die eine Maßnahme charakterisieren (z. B. die Bezeichnung und den für die Steuerung verantwortlichen Risk Owner). Mittels der Funktion *Maßnahmenzuordnung* wird eine Maßnahme einem Risiko zugeordnet und so der Bezug zwischen steuernder Maßnahme und zu steuerndem Risiko geschaffen. Eine Steuerungsmaßnahme benötigt weiterhin einen fest definierten Start und ein fest definiertes Ende (*Start-Ende-Definition*). Im Rahmen der Risikoüberwachung ermöglicht das RMIS über die Funktion *Neuen Indikator definieren* die Festlegung von Indikatoren, welche als Hinweis auf einen bevorstehenden Risikoeintritt angesehen werden. Sie beziehen sich auf die aktuelle Ausprägung einer zu überwachenden Zielgröße. Über die Funktion *Monitoring anzeigen* kann die Risikolage überblickt werden, indem dem Anwender eine Übersicht aller Risiken, ihrer aktuellen Ist-Prozess-Zielgrößen und den dazugehörigen Indikatoren gegeben wird. Sobald die Ausprägung der Ist-Zielgröße eine im Indikator definierte Bedingung erfüllt, kann eine E-Mail Alarmierung des Risk Owners ausgelöst werden.

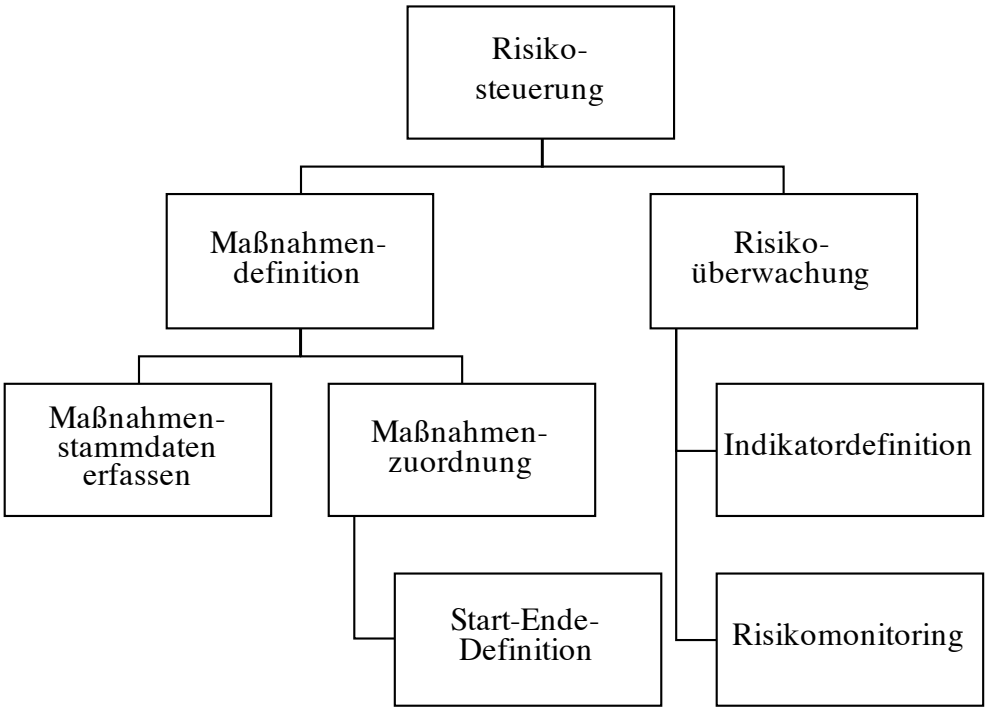
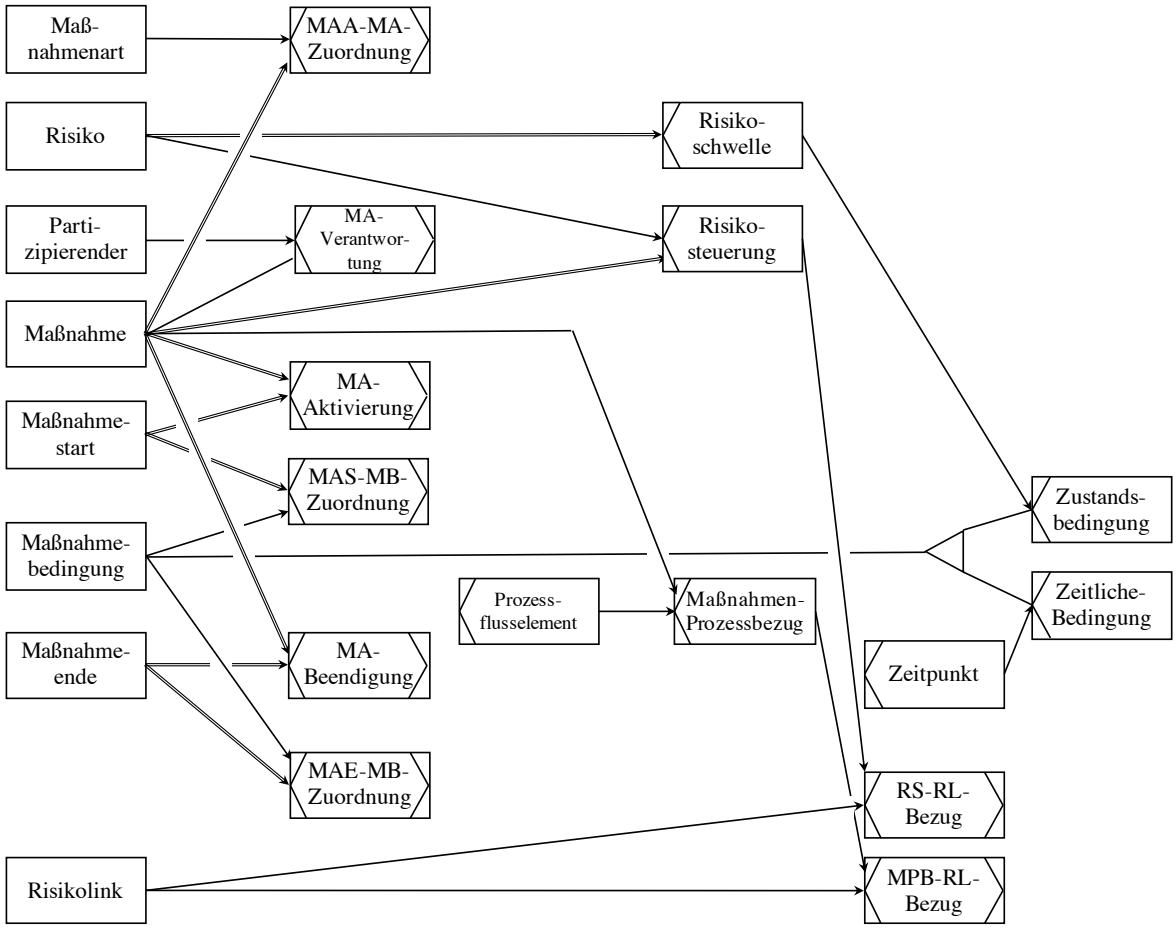


Abbildung 107: Funktionsbaum Risikosteuerung

Datensicht

Das SERM zur Abbildung von Risikosteuerungsmaßnahmen ist in Abbildung 108 dargestellt. Eine Maßnahme wird keinem (falls noch nicht definiert) oder genau einem für die Durchführung der Steuerungsmaßnahme verantwortlichen Prozesspartizipierenden sowie mindestens einer Maßnahmenart zugeordnet. Über den ER-Typ *Risikosteuerung* erfolgt die Zuweisung einer Risikosteuerungsmaßnahme zu einem oder mehreren von dieser Maßnahme zu steuernden Risiken. Über die Attribute dieses ER-Typs wird die erwartete Wirkung auf die Eintrittswahrscheinlichkeit bzw. das Schadensausmaß des jeweiligen Risikos erfasst. Des Weiteren sind mindestens ein Maßnahmenstart und ein Maßnahmenende zu definieren. Dies kann entweder eine zeitliche Bedingung (z. B. Start am 01.01.2018 um 10:00 Uhr) oder eine Zustandsbedingung (z. B. Start, wenn der Differenz-Schwellenwert der Risikoschwelle einen definierten Wert überschreitet) sein.



Risiko (R-ID, Bezeichnung, Beschreibung)
Risikoschwelle (RS-ID, R-ID, PE-ID, PZGS-ID, PZGI-ID, Vergleichszeichen, Vorzeichen, Differenz-Schwellenwert)
Partizipierender (PART-ID)
MA-Verantwortung (PART-ID, MA-ID)
Maßnahme (MA-ID, Bezeichnung, Kosten, Währung)
Maßnahmenart (MAA-ID, Bezeichnung, Beschreibung)
MAA-MA-Zuordnung (MAA-ID, MA-ID)
Risikosteuerung (RS-ID, MA-ID, R-ID, Vorzeichen, WSK-Wirkung, Ausmaßwirkung)
Maßnahmestart (MS-ID)
MA-Aktivierung (MA-ID, MS-ID)
Maßnahmeende (ME-ID)
MA-Beendigung (MA-ID, ME-ID)

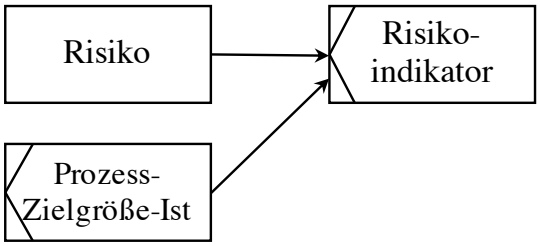
MAE-MB-Zuordnung (ME-ID, MB-ID)
MAS-MB-Zuordnung (MS-ID, MB-ID)
Maßnahmebedingung (MB-ID, Bezeichnung)
Zustandsbedingung (MB-ID, RM-ID, Vergleichszeichen, Vorzeichen, Bedingungswert)
Zeitliche-Bedingung (MB-ID, Z-ID, Vergleichszeichen)
Zeitpunkt (Z-ID, Zeitpunkt)
Prozessflusselement (PFE-ID, P-ID, SP-ID, SL-ID, Bezeichnung)
Maßnahmen-Prozessbezug (MPB-ID, MA-ID, PFE-ID)
Risikolink (RL-ID, Name)
RS-RL-Bezug (RS-ID, RL-ID)
MPB-RL-Bezug (MPB-ID, RL-ID)

Abbildung 108: Datenmodell Risikosteuerung

Auch eine Kombination von Zeit- und Zustandsbedingungen ist denkbar. Entsprechend können einem Maßnahmenstart und einem Maßnahmenende ein oder mehrere Start- und Endbedingungen zugewiesen werden. Dies erfolgt über die E-Typen *Maßnahmenbedingung*, *Maßnahmenstart* bzw. *-ende* und über die R-Typen *MA-Aktivierung*, *MAS-MB-Zuordnung*, *MA-*

Beendigung und *MAE-MB-Zuordnung*. Der ER-Typ *Risikosteuerung* entspricht im ROPM einem Risikofluss und wird entsprechend über den R-Typ *RS-RL-Bezug* mit dem E-Typ *Risikolink* verbunden, damit auch lane- und poolübergreifende Maßnahmen-Risiko-Bezüge modelliert werden können. Da Maßnahmen auch einen Bezug zu den Prozessflusselementen haben können (siehe Kapitel 7.5.2.4), wird dies im SERM entsprechend über den ER-Typ *Maßnahmen-Prozessbezug* modelliert.

Für die Realisierung der Risikoüberwachungsfunktionen wird im SERM der ER-Typ *Risikoindikator* eingeführt (siehe Abbildung 109). Ein Risikoindikator definiert eine konkrete Bedingung, die aus Vergleichszeichen, Vorzeichen und Indikatorwert besteht und sich auf eine Ist-Prozess-Zielgröße bezieht. So können die Ausprägungen einer Zielgröße über einen bestimmten Zeitraum überwacht werden und der dem Risiko zugewiesene Risk Owner bei Erfüllung der Bedingung alarmiert werden.



Risiko (R-ID, Bezeichnung, Beschreibung)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Risikoindikator (RIN-ID, PZGI-ID, R-ID, PE-ID, Bezeichnung, Vergleichszeichen, Vorzeichen, Indikatorwert)

Abbildung 109: Datenmodell Risikoüberwachung

Steuerungssicht

Über die Risikosteuerungsfunktionen des RMIS kann der Anwender für jegliche Risiken Steuerungsmaßnahmen definieren und periodenbezogen einem oder mehreren Risiken eine oder mehrere Maßnahmen zur Risikosteuerung zuweisen (siehe Abbildung 110). Die Maßnahmen werden durch den Anwender als eigenes Objekt im ROPM modelliert und über Risikoflüsse mit den entsprechenden Risiken verbunden. Nach Definition eines eindeutigen Start-

bzw. Endzustands oder eines Start- bzw. Endzeitpunkts für eine Maßnahme ist die Risikosteuerung eines Risikos abgeschlossen. Je nach Situation kann die Maßnahmen-Risiko-Zuordnung beliebig häufig geändert werden.

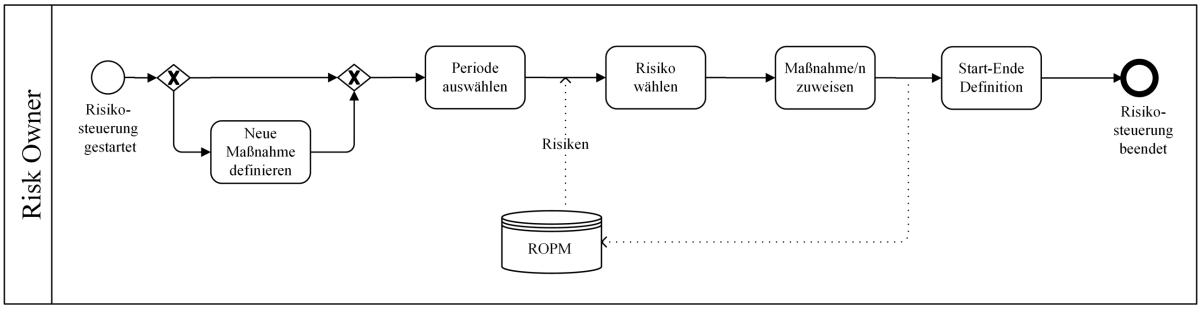


Abbildung 110: Prozessmodell Risikosteuerung

Für die Risikoüberwachung bietet das RMIS die Möglichkeit Indikatoren zu definieren, welche der Kontrolle spezifischer Zielgrößen eines Risikos dienen (siehe Abbildung 111). Zu jedem Indikator werden Bedingungen festgelegt, deren Erfüllung bzw. Nicht-Erfüllung durch das RMIS regelmäßig überwacht werden. Nach Auswahl einer Periode und eines in dieser Periode bestehenden Risikos, werden ein oder mehrere Indikatoren dem Risiko zugewiesen. Über die Funktion *Monitoringdaten anzeigen* kann der jeweilige Status der Zielgrößen und zugehöriger Indikatoren jederzeit beobachtet werden.

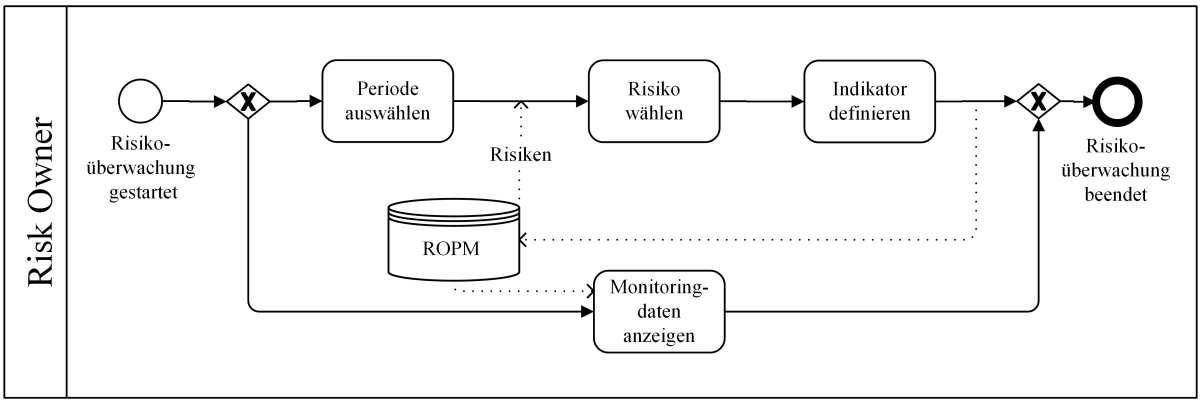


Abbildung 111: Prozessmodell Risikoüberwachung

9.2.7. Detailsichten für das Risikoreporting

Funktionssicht

Das RMIS bietet im Rahmen des Risikoreporting die Möglichkeit Risikoberichte zu erzeugen und den Stakeholdern zur Verfügung zu stellen. Des Weiteren können Risikoberichte zur Erfüllung gesetzlicher Vorgaben archiviert werden.

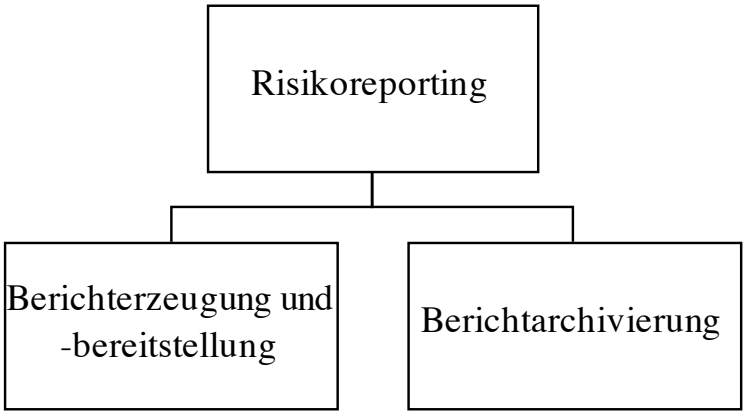
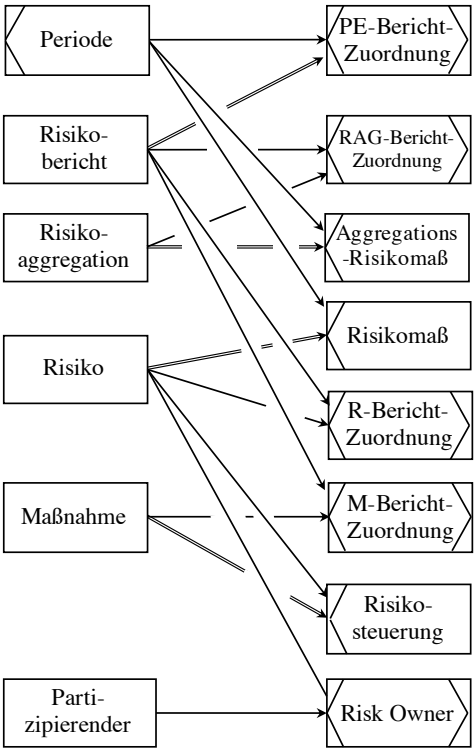


Abbildung 112: Funktionsbaum Risikoreporting

Datensicht

Das Datenschema in Abbildung 113 stellt die Beziehungen zwischen den Objekten dar, die im Rahmen des Reporting in einen Risikobericht zusammen dargestellt werden können. Ein Risikobericht kann sich jeweils auf eine oder mehrere Perioden beziehen. Je nach Informationsbedarf kann der Bericht Informationen zu aggregierten Risiken, Einzelrisiken und Risikosteuerungsmaßnahmen aus diesen Perioden sowie die jeweiligen Verantwortlichen enthalten. Die jeweilige Auswahl wird in der Anwendungslogik durch den Anwender getroffen.



Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID, Bezeichnung)
Risikobericht (RB-ID, Bezeichnung)
PE-Bericht-Zuordnung (PE-ID, BE-ID)
Risikoaggregation (RAG-ID, Bezeichnung, Aggregationsverfahren)
Aggregations-Risikomaß (ARM-ID, PE-ID, RAG-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)
RAG-Bericht-Zuordnung (RB-ID, RAG-ID)
Risiko (R-ID, Bezeichnung, Beschreibung)
Risikomaß (RM-ID, PE-ID, R-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)

R-Bericht-Zuordnung (R-ID, RB-ID)
Maßnahme (MA-ID, MAA-ID, Bezeichnung, Kosten, Einheit)
M-Bericht-Zuordnung (MA-ID, RB-ID)
Risikosteuerung (RS-ID, MA-ID, R-ID, Vorzeichen, WSK-Wirkung, Ausmaßwirkung)
Partizipierender (PART-ID)
Risk Owner (PART-ID, R-ID)

Abbildung 113: Datenmodell Risikoreporting

Steuerungssicht

Die Funktionen des Reportings ermöglichen die Erzeugung eines Risikoberichts für eine oder mehrere Perioden sowie das Öffnen eines bereits archivierten Berichts aus der Datenbank. Der Risikobericht soll einen Überblick über die Risikolage und eingeleitete Maßnahmen geben. Im Falle der Neuerzeugung des Berichts ist zunächst, nach Auswahl der Perioden, der Umfang festzulegen. Hierbei kann die Menge der in den Bericht einzuschließenden Risiken nach gewissen Kriterien, wie z. B. nach Risikoarten oder nach Unternehmensbereichen (Partizipierenden), eingegrenzt werden. Darauf aufbauend wird der Bericht erzeugt und dem Anwender zur Auswertung angezeigt. Es ist nun möglich den Bericht in Form eines Downloads lokal zu speichern, per E-Mail an andere Stakeholder zu versenden oder im System zu archi-

vieren. Wird ein bereits archivierter Bericht geöffnet, so wird dieser angezeigt und kann ebenfalls heruntergeladen oder versendet werden.

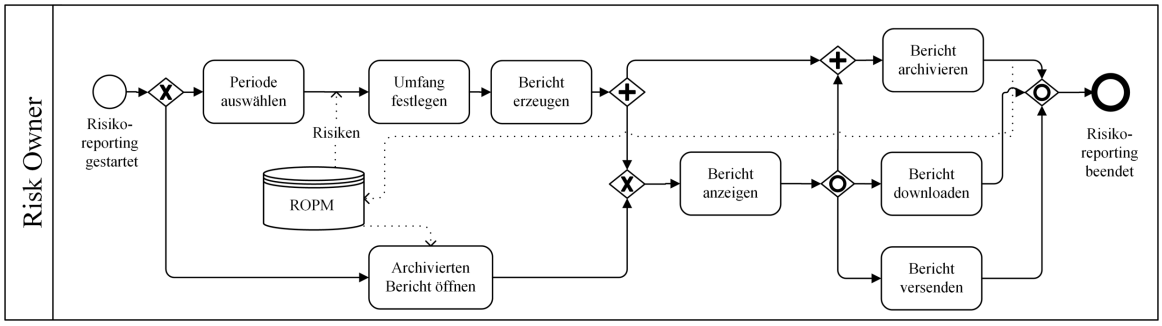


Abbildung 114: Prozessmodell Risikoreporting

10. Fazit

10.1. Zusammenfassung

In der vorliegenden Arbeit wurden eine Erweiterung des BPMN Standards zur Modellierung von Risikophänomenen in Geschäftsprozessmodellen und ein darauf aufbauendes Risikomanagement-Informationssystem konzipiert. Dabei wurden zunächst drei bestehende Mängel adressiert: (i) *die systematische Herleitung von Anforderungen an eine Notation zur Modellierung von Risiken in Geschäftsprozessmodellen, (ii) die vergleichende Analyse aktueller Ansätze und (iii) die Konzeption einer Notation zur Realisierung einer umfassenden Modellierung von Risikophänomenen in Geschäftsprozessmodellen.*

Der erste Mangel wurde durch eine systematische Herleitung der Anforderungen entlang der Phasen des Geschäftsprozess- und des Risikomanagements behoben. Unter Berücksichtigung der disziplinspezifischen Aufgaben in den jeweiligen Phasen wurden Vorteile identifiziert, die sich aus einer Verbindung beider Managementdisziplinen ergeben. Aus den ermittelten Vorteilen resultierten die Anforderungen an die Notation. Der Status der Erfüllung der Anforderungen durch aktuelle Ansätze wurde durch eine umfangreiche Literaturanalyse überprüft. Hierbei zeigte sich, dass keiner der bestehenden 40 Ansätze eine umfassende Modellierung von Risikophänomenen in Geschäftsprozessmodellen leistet. Diese Lücke wurde in dieser Arbeit durch die Konzeption der Risikoerweiterung des BPMN Standards geschlossen. Sie erweitert sowohl das Metamodell der BPMN Notation als auch die konkrete Syntax, so dass, nach bestem Wissen des Autors, erstmals eine umfassende Abbildung von Risikoaspekten in Geschäftsprozessmodellen realisiert werden kann. Die Erweiterung ermöglicht die vollständige Modellierung von Risikoaspekten und ihr Zusammenwirken mit den Elementen eines Geschäftsprozesses. Neben der Abbildung von Einzelrisiken können auch Risiko-Ursache-Wirkungsketten, Risikokorrelationen und Risikosteuerungsmaßnahmen in die Geschäftsprozessmodelle integriert werden. Die Erweiterung unterstützt alle Phasen des Risikomanagements. Sie kann im Rahmen der Dokumentation von Prozessrisiken, Risikoverantwortlichkeiten und Risikosteuerungsmaßnahmen genutzt werden. Des Weiteren ist sie maschinenlesbar und kann so für das tägliche Risikomanagement in Risikomanagement-Informationssysteme (RMIS) integriert werden. Im vorgestellten Metamodell der Erweiterung ist die informationstechnische Abbildung entsprechend berücksichtigt, indem die eingeführten Risikoobjekte um

spezifische Klassen ergänzt wurden, um jegliche Eigenschaften eines Risikoobjekts, die in den einzelnen Phasen des Risikomanagements benötigt werden, erfassen zu können.

Da im Rahmen des Risikomanagements grundsätzlich eine umfassende Informationsversorgung notwendig ist und eine Risikoanalyse auf Geschäftsprozessebene die Verarbeitung vieler prozessbezogener Daten erfordert, ergaben sich drei weitere zu betrachtende Mängel, denen in dieser Arbeit begegnet wird: (iv) *eine fehlende umfassende Definition eines Anforderungskatalogs an Risikomanagement-Informationssysteme,* (v) *eine fehlende aktuelle Untersuchung zum Leistungsstand von RMIS* und (vi) *ein fehlendes Konzept für die IT-Unterstützung der Risikomodellierung und Risikoanalyse auf Geschäftsprozessebene durch Risikomanagement-Informationssysteme*.

Da in der Literatur kein umfassender Anforderungskatalog an RMIS existiert, wurde ein solcher in dieser Arbeit auf Basis bestehender Anforderungskataloge, umfassender Literaturanalyse und sachlogischer Überlegungen aufgebaut.

Mithilfe dieses Katalogs wurde der Leistungsstand des aktuellen RMIS Marktangebots in einer Studie untersucht. Aufgrund der nicht zufriedenstellenden Unterstützung der Abbildbarkeit von Prozessrisiken wurde ein Informationssystem konzipiert, welches die Identifizierung, Erfassung, Quantifizierung, Steuerung, Überwachung und das Reporting von Risikophänomenen in Geschäftsprozessen unterstützt. Es erlaubt somit ein umfassendes Management der Prozessrisiken eines Unternehmens. Den Kern des Informationssystems bilden BPMN Modelle, die auf Basis der in dieser Arbeit konzipierten Notation mit Risikoinformationen angereichert werden können. Das Informationssystem ist in der Lage, die Analyse, die Steuerung und das Reporting von Risiken auf Geschäftsprozessebene nahezu in Echtzeit vorzunehmen, da es an belegorientierte betriebliche Informationssysteme, wie z. B. ein ERP System, über Schnittstellen angebunden werden kann. Eine solche detaillierte geschäftsprozessorientierte Unterstützung des Risikomanagements leistet aktuell keines der untersuchten RMIS.

10.2. Limitationen und Ausblick

Die konzipierte Notation zur Modellierung von Risiken in Geschäftsprozessmodellen basiert auf dem internationalen BPMN Standard. Somit stellt sie keinen generischen Ansatz dar und ist auf den Einsatz im BPMN Umfeld limitiert. Forschungsbedarf besteht in der Generalisierung des Ansatzes, damit auch andere Notationssprachen von den Konzepten der vorgestellten Risikosicht profitieren können. Die in dieser Arbeit erstellte formale Darstellung im UML Metamodell der BPMN kann hierfür als Vorlage dienen.

Des Weiteren ist der vorgestellte Ansatz bisher nicht empirisch getestet, so dass sich hierin weiterer Forschungsbedarf ergibt. Es bedarf einer fundierten Evaluierung, um die Anwendbarkeit, die propagierten Vorteile und die Akzeptanz in der Unternehmenspraxis zu überprüfen. Auf dieser Basis ergeben sich eventuell Ideen zur Weiterentwicklung des Ansatzes.

Die vorliegende Modellierungsmethode erfordert bei manueller Pflege einen enormen Personalaufwand, um die Risikophänomene zu identifizieren, zu analysieren und in den Prozessmodellen zu dokumentieren. Forschungsbedarf ergibt sich somit insbesondere in der automatisierten Aufbereitung der Risiken und ihrer Zusammenhänge innerhalb der Prozesse. Mit den Methoden des Process Mining existieren bereits fortgeschrittene Ansätze, um tatsächliche Prozessverläufe automatisiert aus betrieblichen Daten abzuleiten und in Form von Prozessmodellen darzustellen. Die dazu verwendeten Verfahren der Datenanalyse bieten einen möglichen Ansatz, um auch Risikophänomene, die Einfluss auf die Prozesse nehmen bzw. in den Prozessen entstehen, in den betrieblichen Daten automatisiert zu identifizieren.

Die grundlegende Architektur des vorgestellten Risikomanagement-Informationssystems ist vollständig beschrieben, so dass es perspektivisch in ein eigenständiges Softwareprodukt überführt werden könnte. Alternativ können Hersteller bestehender Risikomanagementsoftware das konzipierte RMIS als ein Modul in ihre RMIS Anwendung einbinden, sofern diese, ebenso wie das vorgestellte RMIS, auf einer relationalen Datenbank aufbaut. Auf diese Weise könnte dem in dieser Arbeit identifizierten Mangel einer unzureichenden Unterstützung des Managements von Prozessrisiken durch die auf dem Markt existierenden RMIS begegnet werden.

Literaturverzeichnis

Accenture (2011): Report on the Accenture 2011 Global Risk Management Study. https://www.rims.org/resources/ERM/Documents/Accenture_Global_Report%202011.pdf, abgerufen: Mai 2014.

AKEIÜ – Arbeitskreis Externe und Interne Überwachung der Unternehmung der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V. (2010): Aktuelle Herausforderungen im Risikomanagement – Innovationen und Leitlinien. In: Der Betrieb, 23, S. 1245-1252.

Ale, Bernadus; Aven, Terje; Jongejan, Ruben (2009): Review and discussion of basic concepts and principles in integrated risk management. In: Bris, Radim; Roades, Guedes; Martorell, Sebastián (Hrsg.): Reliability, Risk and Safety, Theory and Applications, London, S. 421-427.

Alviniussen, Alf; Jankensgård, Hakan (2009): Enterprise Risk Budgeting - Bringing Risk Management Into the Financial Planning Process. In: Journal of Applied Finance, Issues 1 & 2, S. 178–192.

Allweyer, Thomas (2011): BPM-Round-Trip: Wunsch oder Wirklichkeit? In: Komus, Ayelt (Hrsg.): BPM Best Practice, Berlin Heidelberg.

Angermüller, Niels Olaf; Gleißner, Werner (2011): Verbindung von Controlling und Risikomanagement: Eine empirische Studie der Gegebenheiten bei H-DAX Unternehmen. In: Controlling – Zeitschrift für erfolgsorientierte Unternehmenssteuerung, 23 (6), S. 308–316.

Anton, Tobias; Lackes, Richard; Siepermann, Markus (2018): Risk Management and ERP-Systems – An Empirical Study of Software Tools. Erscheint in: Lecture Notes in Business Information Processing (LNBIP), Switzerland 2018.

Anton, Tobias; Lackes, Richard; Siepermann, Markus (2016): Integration of Risk Aspects into Business Process Modeling. In: Innovations in Enterprise Information Systems Management and Engineering, LNBIP 245, S. 46-61.

Arena, Marika; Arnaboldi, Michela; Azzone, Giovanni (2011): Is enterprise risk management real? In: Journal of Risk Research, 14 (7), S. 779-797.

Asnar, Yudistira; Giorgini, Paolo (2008): Analyzing Business Continuity Through a Multi-layers Model. In: Proceedings of the Sixth International Conference on Business Process Management (BPM'08), Berlin Heidelberg, S. 212-227.

Austrian Standards Institute (2014): ONR 49000 – Risikomanagement für Organisationen und Systeme. https://www.austrian-standards.at/fileadmin/user/bilder/downloads-produkte-und-leistungen/fachinformation06_risikomanagement.pdf, abgerufen: Juli 2016.

Autorité des Marchés Financiers (AMF) (2010): Risk management and internal control system, http://www.amf-france.org/technique/multimedia?docId=workspace://SpacesStore/5fa2466b-27df-4297-85f4-5fd100340539_en_1.0_rendition, abgerufen: Juli 2016.

Aven, Terje (2012): Foundational Issues in Risk Assessment and Risk Management. In: Risk Analysis, 32 (10), S. 1647–1656.

Aven, Terje; Renn, Ortwin (2009): On risk defined as an event where the outcome is uncertain. In: Journal of Risk Research, 12 (1), S. 1–11.

Bandara, Wasana; Gable, Guy G.; Rosemann, Michael (2005): Factors and measures of business process modelling: model building through a multiple case study. In: European Journal of Information Systems, 14, S. 347-360.

Barateiro, Jose; Borbinha, José (2011): Integrated management of risk information. In: Proceedings of the Federated Conference on Computer Science and Information Systems, S. 791–798.

Barateiro, José; Borbinha, José (2012): Managing Risk Data: from Spreadsheets to Information Systems. In: Proceedings Electrotechnical Conference (MELECON) - 16th IEEE Mediterranean.

Basel Committee on Banking Supervision (2001): Operational Risk - Supporting Document to the New Basel Capital Accord. https://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/Banking_supervision/Basel_Committee/2001_01_consultative_document_operational_risk.pdf?__blob=publicationFile, abgerufen: Januar 2015.

Baumgrass, Anne; Herzberg, Nico; Meyer, Andreas; Weske, Mathias (2014): BPMN Extension for Business Process Monitoring. In: EMISA 2014 Proceedings: Evolution of Information Systems and their Design Methods, Luxembourg, September 25-26, S. 85-98.

Beasley, Mark S.; Clune, Richard; Hermanson, Dana R. (2005): Enterprise risk management: An empirical analysis of factors associated with the extend of implementation. In: Journal of Accounting and Public Policy, 24, S. 521-531.

Beasley, Mark S.; Branson, Bruce C.; Hancock, Bonnie V. (2009): Take your risk management system to the next level. In: Journal of Accountancy, September, S. 28–32.

Beasley, Mark S.; Branson, Bruce C.; Hancock, Bonnie V. (2010): COSO's 2010 Report On ERM. http://www.coso.org/documents/cososurveyreportfull-webr6finalforwebposting111710.pdf, abgerufen: Juni 2016.

Beck, Andreas; Lesko, Michael; Schlottmann, Frank; Wimmer, Konrad (2006): Copulas im Risikomanagement. In: Zeitschrift für das gesamte Kreditwesen, 14, S. 29-33.

Becker, Jörg; Köster, Christoph; Ribbert, Michael (2005): Geschäftsprozessorientiertes Risikomanagement. In: Controlling, 17 (12), S. 709-718.

Becker, Jörg; Mathas, Christoph; Winkelmann, Axel (2009): Geschäftsprozessmanagement, Berlin Heidelberg.

Becker, Jörg; Kahn, Dieter (2012): Der Prozess im Fokus. In: Becker, Jörg; Kugeler, Martin; Rosemann, Michael (Hrsg.): Prozessmanagement – Ein Leitfaden zur prozessorientierten Organisationsgestaltung, 7. Auflage, Berlin Heidelberg, S. 3-16.

Becker, Wolfgang; Ebner, Robert; Fischer-Petersohn, Daniela; Ruhnau, Markus (2015): Projektrisikomanagement im Mittelstand, Wiesbaden.

Berkau, Carsten (2007): Risiko-Controlling mit Geschäftsprozessen. In: Loos, Peter und Krcmar, Helmut (Hsrg.): Architekturen und Prozesse, Berlin Heidelberg, S. 151–165.

Bernasconi, Elena; Filippi, Franco; Lazzerini, Beatrice; Niccolini, Benedetta; Petronella, Gianluca (2013): An integrated approach based on business process modeling and fuzzy logic for risk identification and evaluation in production processes. In: Intelligent Decision Technologies, 7, S. 113–122.

Beroggi, Giampiero E. G. (1995): Neue Technologien zur Unterstützung des Risikomanagements. Eine Systems Engineering Betrachtungsweise zum Entwurf von Risikoinformationssystemen. Zürich.

Beretta, Sergio; Bozzolan, Saverio (2004): A framework for the analysis of firm risk communication. In: The International Journal of Accounting, 39 (3), S. 265-288.

Betz, Stefanie; Hickl, Susan; Oberweis, Andreas: Risk-Aware Business Process Modeling and Simulation Using XML Nets. In: Proceedings of the 2011 IEEE Conference on Commerce and Enterprise Computing. S. 349-356.

Bleuel, Hans-H. (2006): Monte-Carlo-Analysen im Risikomanagement mittels Software-Erweiterungen zu MS-Excel. In: Controlling, 7, S. 378.

Boatright, John R. (2011): Risk Management and the Responsible Corporation: How Sweeping the Invisible Hand? In: Business and Society Review, 116 (1), S. 145–170.

Bömelburg, Peter; Zähres, Raimund; Beyer, Georg; Schöffel, Christian P. (2012): Risikomanagement im Mittelstand – Eine aktuelle Bestandsaufnahme. In: Der Betrieb, 21, S. 1161–1166.

Bosetti, Luisa (2015): Risk Management Standards in Global Markets. In: QUAESTI-Virtual Multidisciplinary Conference 2015 Proceedings, S. 81-86.

Brabänder, Eric; Ochs, Heike(2002): Analyse und Gestaltung prozessorientierter Risikomanagementsysteme mit Ereignisgesteuerten Prozessketten. In: Nüttgens, Markus; Rump, Frank (Hrsg.): Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten – EPK 2002. Proceedings des GI Workshops und Arbeitskreistreffens, S. 17-35.

Braun, Herbert (1984): Risikomanagement. - Eine spezifische Controllingaufgabe. Darmstadt.

Braun, Richard; Schlieter, Hannes; Burwitz, Martin; Esswein, Werner (2015): Extending a Business Process Modeling Language for Domain-Specific Adaption in Healthcare. In: Wirtschaftsinformatik Proceedings, 32, S. 468-481.

Brebeck, Frank; Herrmann, Dagmar (1997): Zur Forderung des KonTraG-Entwurfs nach einem Frühwarnsystem und zu den Konsequenzen für die Jahres- und Konzernabschlußprüfung. In: Die Wirtschaftsprüfung, 50 (12), S. 381-391.

Brink, Gerri Jan van den (2007): Management von operationellen Risiken in Finanzinstituten: Qualitative Verfahren. In: Kaiser, Thomas (Hrsg.): Wettbewerbsvorteil Risikomanagement. Berlin, S.177-194.

Bromiley, Philip; McShane, Michael; Nair, Anil; Rustambekov, Elzotbek (2015): Enterprise Risk Management. Review, Critique, and Research Directions. In: Long Range Planning, 48 (4).

Brustbauer, Johannes (2016): Enterprise Risk Management in SMEs: Towards a structural model. In: International Small Business Journal, 34 (1), S. 70-85.

Brühwiler, Bruno (2016): Notwendigkeit und Nutzen von internationalen Standards im Logistik-Risikomanagement. In: Huth, Michael; Romeike, Frank (Hrsg.): Risikomanagement in der Logistik. Wiesbaden, S. 159-169.

Buchanan, Steven; McMenemy, David (2012): Digital service analysis and design: The role of process modelling. In: International Journal of Information Management, 32, S. 251-256.

Budäus, Dietrich; Hilgers, Dennis (2009): Öffentliches Risikomanagement – zukünftige Herausforderungen an Staat und Verwaltung. In: Scholz, Frank; Schuler, Andreas; Schwintowski, Hans-Peter (Hrsg.): Risikomanagement der Öffentlichen Hand. Heidelberg, S. 17-77.

Bundesrepublik Deutschland (1998): Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG, Nr. 24. In: Bundesgesetzblatt Teil I.

Bundesverband der Deutschen Industrie e.V. / PricewaterhouseCoopers AG (2011): Risikomanagement 2.0. http://www.bdi.eu/download_content/Marketing/15389_BDI_Risiko_7.pdf, abgerufen: Oktober 2014.

Bungartz, Oliver (2006): Risikokultur. In: ZRFG - Zeitschrift Risk, Fraud & Governance 4, S. 170-178.

Burger, Anton; Buchhart, Anton (2002): Risiko-Controlling. München Wien.

Burth, Andreas; Hilgers, Dennis (2012): Kommunale Risikoberichterstattung – Eine vergleichende Analyse doppischer Lageberichte. In: Verwaltung und Management, 18 (1), S. 7-16.

Bussmann, Karl F. (1955): Das betriebswirtschaftliche Risiko. In: Schriften zur wirtschaftswissenschaftlichen Forschung, 4, Meisenheim am Glan.

Caron, Filip; Vanthienen, Jan; Baesens, Bart (2013): A comprehensive investigation of the applicability of process mining techniques for enterprise risk management. In: Computers in Industry, 64 (4), S. 464-475.

Chinosi, Michele; Trombetta, Alberto (2012): BPMN: An introduction to the standard. In: Computer Standards & Interfaces, 34, S. 124–134.

Christians, Uwe (2006): Performance Management und Risiko. Strategieumsetzung mit risikointegrierter Balanced Scorecard, Wissensbilanzen und Werttreibernetzen; Methodik und Fallbeispiele aus dem Bankensektor. Berlin.

Colquitt, Lee L.; Hoyt, Robert E.; Lee, Ryan B. (1999): Integrated Risk Management and the Role of the Risk Manager. In: Risk Management and Insurance Review, 2 (3), S. 43-61.

Conforti, Raffaele; Fortino, Giancarlo; La Rosa, Marcello; ter Hofstede, Arthur H.M. (2011): History-Aware, Real-Time Risk Detection in Business Processes. In: Meersman, Robert et al. (Hrsg.): On the Move to Meaningful Internet Systems: OTM 2011. Lecture Notes in Computer Science, 7044, Berlin Heidelberg, S. 100-118.

Conforti, Raffaele; La Rosa, Marcello; Fortino, Giancarlo; ter Hofstede, Arthur H.M.; Recker, Jan; Adams, Michael (2013): Real-time risk monitoring in business processes: A sensor-based approach. In: Journal of Systems and Software, 86 (11), S. 2939-2965.

Cope, E.W.; Kuster, J.M.; Etzweiler, D.; Deleris, L.A.; Ray, B. (2010): Incorporating risk into business process models. In: IBM Journal of Research and Development. 54, S. 4:1-4:13.

COSO (2004): Enterprise Risk Management - Integrated Framework Executive Summary. https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf, abgerufen: Januar 2017.

COSO (2012): COSO – Risk Assessment in Practice. https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf, abgerufen: Januar 2017.

Cottin, Claudia; Döhler, Sebastian (2013): Risikoanalyse. 2. Auflage, Wiesbaden.

Cox, Louis Anthony (2008): What's wrong with Risk Matrices? In: Risk Analysis, 28 (2), S. 497-512.

Daldrup, Andre (2005): Kreditrisikomaße im Vergleich. In: Schumann, Matthias (Hrsg.): Arbeitsbericht Nr. 13/2005, Institut für Wirtschaftsinformatik, Georg-August-Universität Göttingen, http://webdoc.sub.gwdg.de/ebook/serien/lm/arbeitsberichte_wi2/2005_13.pdf, abgerufen: April 2017.

de Morais, Rinaldo Macedo; Kazan, Samir; Dallavalle de Pádua, Silvia Inês; Lucirton Costa, André (2014): An analysis of BPM lifecycles: from a literature review to a framework proposal. In: Business Process Management Journal, 20 (3), S. 412-432.

Deiters, Wolfgang (1997): Prozessmodelle als Grundlage für ein systematisches Management von Geschäftsprozessen. In: Informatik Forschung und Entwicklung, 12, S. 52–60.

Deloitte (2015): Global risk management survey, ninth edition, https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/ru-global-risk-management-survey-9th-edition.pdf, abgerufen: Mai 2017.

Deutscher Bundestag (1998): Drucksache 13/9712. http://dipbt.bundestag.de/doc/btd/13/097/1309712.pdf, angerufen: Januar 2016.

Deutsches Rechnungslegungs Standards Committee e. V. (2012): Deutscher Rechnungslegungs Standard Nr. 20 (DRS 20).

Derfuß, Klaus; Körner, Stephan; Lenz, Frank (2016): Kommunales Risikomanagement – Empirische Befunde aus deutschen Landkreisen. In: Zeitschrift Führung + Organisation (zfo), 04/2016, S. 249-256.

Diederichs, Marc (2004a): Risikomanagement und Risikocontrolling. 1. Auflage, München.

Diederichs, Marc; Form, Stephan; Reichmann, Thomas (2004b): Standard zum Risikomanagement. In: Controlling, 4 (5), S. 189-198.

Diederichs, Marc (2010): Risikomanagement und Risikocontrolling. 2. Auflage, München.

Diederichs, Marc (2012): Risikomanagement und Risikocontrolling. 3. Auflage, München.

Diederichs, Marc; Imhof, Markus (2011): Corporate Governance und Controlling: Die Gestaltung des rechnungslegungsbezogenen Internen Kontrollsystems der Beiersdorf AG. In: Controlling, 23 (3), S. 172-177.

Dobler, Michael (2005): Zur Verbindung von Risikomanagement und Risikopublizität. In: ZfCM – Zeitschrift für Controlling & Management, 49 (2), S. 144-152.

Dobler, Michael; Lajili, Kaouthar; Zéghal, Daniel (2011): Attributes of Corporate Risk Disclosure: An International Investigation in the Manufacturing Sector. In: Journal of International Accounting Research, 10 (2), S. 1—22.

Dörner, Dietrich; Bischof, Stefan (1999): Zweifelsfragen zur Berichterstattung über die Risiken der künftigen Entwicklung im Lagebericht. In: Die Wirtschaftsprüfung (12), S. 445–455.

Dörner, Dietrich; Horváth, Péter; Kagermann, Henning (2000): Praxis des Risikomanagements. Stuttgart.

Duijm, Nijs Jan (2015): Recommendations on the use and design of risk matrices. In: Safety Science, 76, S. 21-31.

Ebert, Christof (2013): Risikomanagement kompakt. 2.Auflage, Berlin Heidelberg.

Eickemeier, Susanne (2002): Fuzzy-Entscheidungsmodelle im Risikomanagement. In: Lecture Notes in Informatics, 32. GI Jahrestagung 2002, S. 660-669.

Einarsson, Stefan; Rausand, Marvin (1998): An Approach to Vulnerability Analysis of Complex Industrial Systems. In: Risk Analysis, 18 (5), S. 535–546.

Elzahar, Hany; Hussainey, Khaled (2012): Determinants of narrative risk disclosures in UK interim reports. In: The Journal of Risk Finance, 13 (2), S. 133-147.

Engels, Jörg; Cluse, Michael (2007): Kontext der gesetzlichen und regulatorischen Anforderungen. In: Kaiser, Thomas (Hrsg.): Wettbewerbsvorteil Risikomanagement, Berlin, S. 21-38.

Erben, Roland Franz (2000): Fuzzy-Logic-basiertes Risikomanagement. Dissertation, Bayerische Julius-Maximilians-Universität, Wirtschaftswissenschaftliche Fakultät, Würzburg.

Erben, Roland Franz; Romeike, Frank (2002): Risk Management-Informationssysteme – Potentiale einer umfassenden IT-Unterstützung des Risk Managements. In: P. M. Pastors (Hrsg.): Risiken des Unternehmens – vorbeugen und meistern. München und Mering, S. 551–588.

Erben, Roland Franz; Romeike, Frank (2003): Risikoreporting mit Unterstützung von Risk Management-Informationssystemen (RMIS). In: Romeike , Frank und Finke, Robert B. (Hrsg.): Erfolgsfaktor Risikomanagement. Wiesbaden, S. 275–297.

Erben, Franz (2007): Lessons Learned: Beispiele für den Eintritt von Strategierisiken, operationellen Risiken und Reputationsrisiken. In: Thomas Kaiser (Hrsg.): Wettbewerbsvorteil Risikomanagement. Berlin, S.45-49.

Ergün, Ismail; Kreipl, Markus Philipp; Müller, Stefan (2015): Stand der Ausgestaltung des Risikomanagements in mittelständischen Unternehmen. In: Controlling, 27 (6), S. 338-343.

Europäische Kommission (2003): Empfehlung der Kommission vom 6.Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG. In: Amtsblatt der Europäischen Kommission, L 124/36, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN, abgerufen: Februar 2017.

Farrell, Mark; Gallagher, Ronan (2015): The Valuation Implications of Enterprise Risk Management. In: The Journal of Risk and Insurance, 82 (3), S. 625-657.

Federation of European Risk Management Association (FERMA) (2002): A Risk Management Standard, http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf, abgerufen: Juli 2016.

Ferstl, Otto; Sinz, Elmar (2013): Grundlagen der Wirtschaftsinformatik. 7. Auflage, München.

Fiss, Peer C.; Zajac, Edward, J. (2004): The Diffusion of Ideas over Contested Terrain: The (Non) Adoption of a Shareholder Value Orientation among German Firms. In: Administrative Science Quarterly, 49 (4), S. 501-534.

Freund, Jakob; Rücker, Bernd (2012): Praxishandbuch BPMN 2.0. 3. Auflage, München Wien.

Frigo, Mark L.; Anderson, Richard J. (2014): Risk Management Frameworks: Adapt, Don't Adopt. In: Strategic Finance, 96 (1), S. 49-53.

Funk RMCE GmbH; Rödl & Partner GmbH; Weissmann & Cie. GmbH & Co. KG (2011): Risikomanagement im Mittelstand, https://www.risknet.de/fileadmin/eLibrary/Benchmarkstudie-RM_im_Mittelstand-2011-04.pdf, abgerufen: Mai 2017.

Gampenrieder; Peter; Greiner, Matthias (2002): Risikomanagement als gesetzliche Forderung an mittelständische Unternehmen. In: krp - Kostenrechnungspraxis, 46 (5), S. 283-289.

Gao, Simon S. (2011): Risk management capability building in SMEs: A social capital perspective. In: International Small Business Journal, 31 (6), S. 677-700.

Gates, Stephen (2006): Incorporating Strategic Risk into Enterprise Risk Management. In: Journal of Applied Corporate Finance, 18 (4), S.81-90.

Gericke, Anke; Bayer, Franz; Kühn, Harald; Rausch, Tobias; Strobl, Robert (2013): Der Lebenszyklus des Prozessmanagements. In: Bayer, Franz; Kühn, Harald (Hrsg.): Prozessmanagement für Experten. Berlin Heidelberg.

Gjerdrum, Dorothy; Peter, Mary (2011): The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework. In: Risk Management (Society of Actuaries), 21, S. 8-12.

Gleißner, Werner (2011): Quantitative Verfahren im Risikomanagement: Risikoaggregation, Risikomaße und Performancemaße. In: Gleich, Ronald; Klein, Andreas (Hrsg.): Der Controlling-Berater. Band 16, S. 179-204.

Gleißner, Werner; Meier, Günter (1999): Risikoaggregation mittels Monte-Carlo-Simulation. In: Versicherungswirtschaft, 13, S. 926-929.

Gleißner, Werner; Romeike, Frank (2005a): Anforderungen an die Softwareunterstützung für das Risikomanagement. In: ZfCM - Zeitschrift für Controlling & Management, 49 (2).

Gleißner, Werner; Romeike, Frank (2005b): Risikomanagement. Umsetzung – Werkzeuge - Risikobeurteilung. 1. Auflage, München.

Gonschorek Torsten; Petzold, Christian (2014): Risiken managen. In: Haubold, Anne-Katrin; Gonschorek, Torsten; Gestring, Ingo; Sonntag, Ralph; von der Werth, Rüdiger (Hrsg.): Managementkompetenzen im Mittelstand. Wiesbaden, S. 47-67.

Grace, Martin F.; Leverty, J. Tyler; Phillips, Richard D.; Shimpi, Prakash (2015): The Value of Investing in Enterprise Risk Management. In: Journal of Risk and Insurance, 82 (2), S. 289–316.

Gtnews (2013): 2013 Treasury Risk Survey, https://www.gtnews.com/wp-content/uploads/sites/21/2015/09/2013gtnews_TreasuryRisk-51.pdf, abgerufen: Mai 2017.

Günther, Thomas; Smirska, Katarzyna; Schiemann, Frank; Weber, Sebastian (2009): Optimierung des Risikomanagementsystems am Beispiel der R. STAHL Technologiegruppe. In: Controlling, 21, S. 48-56.

Güttner, Andrea; Manthe, Rainald (2013): Risikomanagement? Rücklagenmanagement und Finanzplanung an deutschen Hochschulen. CHE gemeinnütziges Centrum für Hochschulentwicklung Arbeitspapier Nr. 162, http://www.che.de/downloads/CHE_AP_162_Ruecklagenmanagement.pdf, abgerufen: Februar 2017.

Hampel, Volker; Lueger, Marcus; Roth, Ute (2004): Risikocontrolling aus der Sicht des Abschlussprüfers. In: ZFCM - Zeitschrift für Controlling & Management, Sonderheft 3, S. 108-119.

Häntsch, Marius; Huchzermeier, Arnd (2013): Identifying, analyzing, and assessing risk in the strategic planning of a production network: the practical view of a German car manufacturer. In: Journal of Management Control, 24, S. 125-158.

Härterich, Susanne (1987): Risk Management von industriellen Produktions- und Produktrisiken. In: Helten, E.; Lorenz, E. (Hrsg.): Veröffentlichungen des Instituts für Versicherungswissenschaften der Universität Mannheim. Band 37, Karlsruhe.

Haimes, Yacov Y. (2006): On the definition of vulnerabilities in measuring risks to infrastructures. In: Risk Analysis: an official publication of the Society for Risk Analysis, 26 (2), S. 293–296.

Haimes, Yacov Y. (2009): On the definition of resilience in systems. In: Risk Analysis: an official publication of the Society for Risk Analysis, 29 (4), S. 498–501.

Harrington, Scott E.; Niehaus, Greg; Risko, Kenneth J. (2002): Enterprise Risk Management: The Case of United Grain Growers. In: Journal of Corporate Finance, 14 (4), S. 71-81.

Hasenmüller, Philipp (2009): Unternehmensrisiko Klimawandel. Wiesbaden.

Head, George L. (1967): An Alternative to defining Risk as Uncertainty. In: The Journal of Risk and Insurance, 34 (2), S. 206–214.

Helten, Elmar (1994): Die Erfassung und Messung des Risikos. 1. Auflage, Wiesbaden.

Helten, Elmar; Bittl, Andreas; Liebwein, Peter (2000): Versicherung von Risiken. In: Dörner, Dietrich; Horváth, Péter und Kagermann, Henning (Hrsg.): Praxis des Risikomanagements. Stuttgart, S. 153–192.

Hempel, Mario; Offerhaus, Jan (2008): Risikoaggregation als wichtiger Aspekt des Risikomanagements. In: Gesellschaft für Risikomanagment e.V. (Hrsg.): Risikoaggregation in der Praxis. Berlin Heidelberg, S. 3–12.

Hengmith, Lars (2005): Geschäftsprozessmodellierung und -simulation als Hilfsmittel zum Management operationaler Risiken. In: Banking and information technology. 2, S. 17-29.

Henschel, Thomas (2010): Erfolgreiches Risikomanagement im Mittelstand. Berlin.

Hermann, Dirk Christian (1996): Strategisches Risikomanagement kleinerer und mittlerer Unternehmen. 1. Auflage, Berlin.

HGB (2015): Handelsgesetzbuch vom 10.05.1897 mit allen späteren Änderungen einschließlich der Änderung vom 22.12.2015. https://www.gesetze-im-internet.de/bundesrecht/hgb/gesamt.pdf, abgerufen: Februar 2016.

Hoitsch, Hans-Jörg; Winter, Peter (2004): Die Cash Flow at Risk-Methode als Instrument eines integriert holistischen Risikomanagements. In: ZfCM - Zeitschrift für Controlling & Management, 48 (4), S. 235-246.

Hoitsch, Hans-Jörg; Winter, Peter; Bächle, Raphael (2005): Risikokultur und risikopolitische Grundsätze: Strukturierungsvorschläge und empirische Ergebnisse. In: Controlling & Management Review: Zeitschrift für Controlling & Management, 49 (2), S. 125-133.

Hölscher, Reinhold; Giebel, Stefan; Karrenbauer, Ulrike (2006): Stand und Entwicklungstendenzen des industriellen Risikomanagements. Teil 1. In: Zeitschrift für Risk, Fraud and Governance, 1 (4), S. 149–154.

Hommelhoff, Peter; Mattheus, Daniela (2000): Grundlagen des Risikomanagements - Gesetzliche Grundlagen: Deutschland und international. In: Dörner, Dietrich; Horváth, Péter; Kagermann, Henning (Hrsg.): Praxis des Risikomanagements. Stuttgart, S. 5-40.

Hopkin, Paul (2015): Fundamentals of Risk Management. 3. Auflage, London Philadelphia.

Hornung, Karlheinz; Reichmann, Thomas; Baumöl, Ulrike (1997): Informationsversorgungsstrategien für einen multinationalen Konzern. In: Controlling, 9 (1), S. 38-45.

Hornung, Karlheinz; Reichmann, Thomas; Diederichs, Marc (1999): Risikomanagement – Teil 1: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen. In: Controlling, 11 (7), S. 317-325.

Hoyt, Robert E.; Liebenberg, Andre P. (2011): The Value of Enterprise Risk Management. In: Journal of Risk and Insurance, 78 (4), S. 795–822.

Hung, Richard Yu-Yuan (2006): Business Process Management as Competitive Advantage: a Review and Empirical Study. In: Total Quality Management, 17 (1), S. 21-40.

Hunziker, Stefan; Balmer, Patrick; Schellenberg, Christina (2016): Enterprise Risk Management 2016 – Studie zum Risikomanagement in Schweizer Unternehmen, Hochschule Luzern, Institut für Finanzdienstleistungen, http://swisserm.ch/wp-content/uploads/2016/12/Enterprise-Risk-Management-2016.pdf, abgerufen: Februar 2017.

Hwang, Bon-Gang; Zhao, Xianbo; Toh, Li Ping (2014): Risk management in small construction projects in Singapore: Status, barriers and impact. In: International Journal of Project Management, 32, S. 116-124.

IET – The Institution of Engineering and Technology (2015): Quantified Risk Assessment Techniques – Part 2: Event Tree Analysis – ETA, Health and Safety Briefing No. 26b, http://www.theiet.org/factfiles/health/hsb26b-page.cfm?type=pdf, abgerufen: Mai 2016.

Imboden, Carlo (1983): Ein entscheidbezogenes Verfahren. Bern Stuttgart.

Institut der Wirtschaftsprüfer (IDW) (2000): IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340). Düsseldorf.

Institut der Wirtschaftsprüfer (IDW) (2017): IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981). Düsseldorf.

Institute of Directors in Southern Africa (IoDSA) (2009): King Code of Governance Principles and the King Report on Governance (King III).

Institute of Management Accountants (2011): Enterprise Risk Management: Frameworks, Elements and Integration. http://www.imanet.org/docs/default-source/research/sma/erm_frameworks-elements-and-integration.pdf?sfvrsn=2, abgerufen: Juni 2016.

International Organization for Standardization (ISO) (2009): ISO 31000:2009 Risk Management – Principles and Guidelines.

Iwona, Gorzen-Mitka (2016): Leading Risk Management Determinants of Small and Medium-Sized Enterprises (SMEs): An Exploratory Study in Poland. In: Bilgin, M.H.; Danis, H. (Hrsg.): Entrepreneurship, Business and Economics – Vol. 1. Eurasien Studies in Business and Economics, 3/1, S. 289-298.

Jahnke, Bernd; Thomas, Tobias (2004): Zum Einsatz IT-gestützter Risikomanagementsysteme im Rahmen der Corporate Governance-Debatte. In: Jahnke, Bernd (Hrsg.): Arbeitsberichte der Wirtschaftsinformatik, Band 28, Universität Tübingen.

Jakoubi, Stefan; Tjoa, Simon; Quirchmayr, Gerald (2007): ROPE: A Methodology for Enabling the Risk-aware Modelling and Simulation of Business Processes. In: Proceedings of the Fifteenth European Conference on Information Systems (ECIS'07), S. 1596-1607.

Jallow, A. K.; Majeed, Basim; Vergidis, K.; Tiwari, Ashutosh; Roy, Rajkumar (2007): Operational risk analysis in business processes. In: BT Technology Journal, 25, S. 168-177.

Jonen, Andreas (2006): Semantische Analyse des Risikobegriffs. Strukturierung der betriebswirtschaftlichen Risikodefinition und literaturempirische Auswertung. In: Beiträge zur Controlling-Forschung, 11, Lehrstuhl für Unternehmensrechnung und Controlling, Technische Universität Kaiserslautern.

Joos-Sachse, Thomas (2006): Controlling, Kostenrechnung und Kostenmanagement. 4. Auflage, Wiesbaden.

Kajüter, Peter (2012): Risikomanagement im Konzern. München.

Kalwait, Rainer; Meyer, Ralf; Romeike, Frank (2008): Risikomanagement in der Unternehmensführung. 1. Auflage, Weinheim.

Kaplan, Robert S.; Mikes, Anette (2012): Managing Risks: A new Framework. In: Harvard Business Review, 6 (90), S. 48–60.

Karagiannis, Dimitris; Mylopoulos, John; Schwab, Margit (2007): Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act. 15th IEEE International Requirements Engineering Conference (RE 2007), Delhi, S. 315-321.

Karagiannis, Dimitris (2008): A Business Process-Based Modelling Extension for Regulatory Compliance. Multikonferenz Wirtschaftsinformatik.

Kazap, Deniz; Kaymak, Murat (2007): Risk Identification Step of the Project Risk Management. In: Proceedings of PICMET 07, Aug. 2007, S. 2116-2120.

Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner (2013): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. 4. Auflage, Wiesbaden.

Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner (2016): IT-Sicherheitsmanagement nach der neuen ISO 27001. Wiesbaden.

Khan, Majid J.; Hussain, Dildar; Mehmood, Waqar (2016): Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. In: Management Decision, 54 (8), S. 1886-1907.

Khidzir, Nik Zulkarnaen; Mohamed, Azlinah; Arshad, Noor Habibah (2010): Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. In: 2010 International Conference on Information Retrieval & Knowledge Management (CAMP), Shah Alam, Selangor, S. 194–199.

Kirchmer, Mathias (2017): High Performance Through Business Process Management - Strategy Execution in a Digital World. 3. Auflage, Cham.

Kleffner, Anne E.; Lee, Ryan B.; McGannon, Bill (2003): The Effect Of Corporate Governance On The Use Of Enterprise Risk Management: Evidence From Canada. In: Risk Management and Insurance Review, 6 (1), S. 53-73.

Kocbek, Mateja; Jost, Gregor; Hericko, Marjan; Polancic, Gregor (2015): Business process model and notation: The current state of affairs. In: Computer Science Information Systems, 12, S. 509-539.

Korte, Thomas; Romeike, Frank (2011): MaRisk VA erfolgreich umsetzen. Berlin.

Kosow, Hannah; Gaßner, Robert (2008): Methoden der Zukunfts- und Szenarioanalyse – Überblick, Bewertung und Auswahlkriterien. Werkstatt Bericht Nr. 103, Institut für Zukunftsstudien und Technologiebewertung, Berlin.

Kromschröder, Bernhard; Lück, Wolfgang (1998): Grundsätze risikoorientierter Unternehmensüberwachung. In: Zeitschrift für Interne Revision (ZIR), 33 (5), S. 237-248.

Lackes, Richard; Siepermann, Markus; Springwald, Stefan (2010): Risikomanagementsoftware für die Supply Chain – Anforderungen und Umsetzungsstand. In: Betriebswirtschaftliche Forschung und Praxis (BFuP), 62 (1), S. 56–70.

Lechner, Philipp; Gatzert, Nadine (2016): Determinants And Value Of Enterprise Risk Management: Empirical Evidence From Germany, Working Paper, Department of Insurance Economics and Risk Management, Friedrich-Alexander University Erlangen-Nürnberg, Version vom 17.3.2016, https://www.vwrm.rw.fau.de/files/2016/05/ERM_Dtld_2016-02-19_WP.pdf, abgerufen: Februar 2017.

Liebenberg, André P.; Hoyt, Robert E. (2003): The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. In: Risk Management and Insurance Review, 6, S. 37–52.

Liu, Ying; Zhang, Hui; Li, Chunping; Jiao, Roger J. (2012): Workflow simulation for operational decision support using event graph through process mining. In: Decision Support Systems, 52, S. 685-697.

Löhr, Benjamin (2010): Integriertes Risikocontrolling für Industrieunternehmen. Eine normative Konzeption im Kontext der empirischen Controllingforschung von 1990 bis 2009. In: Controlling & Business Accounting 4, Frankfurt am Main.

Lübbecke, Patrick; Anton, Tobias; Lackes, Richard (2013): Cross-Border Risk Factors of Cloud Services: Risk Assessment of IS Outsourcing to Foreign Cloud Service Providers. In: Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, S. 565-572.

Lück, Wolfgang (2000): Managementrisiken. In: Dörner, Dietrich; Horváth, Péter und Kagermann, Henning (Hrsg.): Praxis des Risikomanagements. Stuttgart, S. 311-343.

Lundqvist, Sara A. (2014): An Exploratory Study of Enterprise Risk Management: Pillars of ERM. In: Journal of Accounting, Auditing & Finance, 29 (3), S. 393–429.

Mafrolla, Elisabetta; Matozza, Felice; D'Amico, Eugenio (2016): Enterprise Risk Management In Private Firms: Does Ownership Structure Matter? In: The Journal of Applied Business Research, 32 (2), S. 671-685.

Manab, Norlida A.; Kassim, Isahak; Hussin, Mohd R. (2010): Enterprise-Wide Risk Management (EWRM) Practices: Between Corporate Governance Compliance and Value Creation. In: International Review of Business Research Papers, 6, S. 239-252.

McShane, Michael K.; Nair, Anil; Rustambekov, Elzotbek (2011): Does Enterprise Risk Management Increase Firm Value? In: Journal of Accounting, Auditing & Finance, 26 (4), S. 641–658.

Meletiadou, Anastasia; Müller, Simone; Grimm, Rüdiger (2009): Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS). Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik, 3, http://kola.opus.hbz-nrw.de/volltexte/2009/362/pdf/2009_03_Arbeitsberichte.pdf, abgerufen: August 2016.

Merkelsen, Henrik (2011): The constitutive element of probabilistic agency in risk: a semantic analysis of risk, danger, chance, and hazard. In: Journal of Risk Research, 14 (7), S. 881–897.

Montag, Pia (2015): Risikoberichterstattung mittelständischer Unternehmen. In: Zeitschrift für Corporate Governance (ZCG), 5, S. 223-228.

Motel, Jens; Richter, Martin (2016): Risikomanagement in einer Bundesbehörde. In: Verwaltung und Management, 22 (2), S. 73-82.

Müller, Tobias (2015): Systematische Analyse des Marktes für Risikoinformationssysteme. Bachelor Thesis, Fakultät Wirtschaftswissenschaften, Technische Universität Dortmund.

Mugler, Josef (1979): Risk Management in der Unternehmung. Wien.

Muralidhar, K. (2010): Enterprise risk management in the Middle East oil industry: An empirical investigation across GCC countries. In: International Journal of Energy Sector Management, 4 (1), S. 59-86.

National Audit Office (2011): Managing risks in government, https://www.nao.org.uk/wp-content/uploads/2011/06/managing_risks_in_government.pdf, abgerufen: Februar 2017.

Neumann, Stefan; Probst, Christian; Wernsmann, Clemens (2012): Kontinuierliches Prozessmanagement. In: Becker, Jörg; Kugeler, Martin; Rosemann, Michael (Hrsg.): Prozessmanagement – Ein Leitfaden zur prozessorientierten Organisationsgestaltung. 7. Auflage, Berlin Heidelberg, S. 303-325.

Nguyen, Tristan; Molinari, Robert Danilo (2009) : Quantifizierung von Abhängigkeitsstrukturen zwischen Risiken in Versicherungsunternehmen. In: German Risk and Insurance Review (GRIR), 5 (2), S. 28-52.

Oberparleiter, Karl (1955): Funktionen und Risiken des Warenhandels. 2. Auflage, Wien.

Object Management Group (2011): Business Process Model and Notation (BPMN) Version 2.0, http://www.omg.org/spec/BPMN/2.0, abgerufen: August 2017.

Offerhaus, Jan (2009): Risikomanagement der öffentlichen Hand – Erfahrungen aus angelsächsischen Ländern. In: Scholz, Frank; Schuler, Andreas; Schwintowski, Hans-Peter (Hrsg.): Risikomanagement der Öffentlichen Hand. Heidelberg, S. 79-116.

Paape, Leen; Spekle, Roland F. (2012): The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. In: European Accounting Review, 21 (3). S. 533-564.

Paetzmann, Karsten (2012): Corporate Governance. 2. Auflage, Berlin Heidelberg.

Pagach, Donald; Warr, Richard (2011): The Characteristics of Firms That Hier Chief Risk Officers. In: The Journal of Risk and Insurance, 78 (1), S. 185-211.

Palermo, Tommaso (2014): Accountability and Expertise in Public Sector Risk Management: A Case Study. In: Financial Accountability & Management, 30 (3), S. 322-341.

Pauli, Marcus (2008): Risikomanagement-Informationssysteme (RMIS) – Basis eines modernen Risikomanagements. In: Kalwait, Rainer; Meyer, Ralf und Romeike, Frank (Hrsg.): Risikomanagement in der Unternehmensführung, 1. Auflage, Weinheim, S. 273–299.

Perera, Jeevan; Holsomback, Jerry (2005): An Integrated Risk Management Tool and Process. In: IEEE Aerospace Conference Proceedings, S. 129-136.

Pérez-Gonzáles. F.; Yun, H. (2013): Risk Management and Firm Value: Evidence from Weather Derivatives. In: Journal of Finance, 68 (5), S. 2143-2176.

Philipp, Fritz (1967): Risiko und Risikopolitik. Stuttgart.

Piaz, Jean-Marc (2002): Operational Risk Management bei Banken. Zürich.

PricewaterhouseCoopers AG (2012): Risk Management Benchmarking 2011/2012. http://www.pwc.de/de_DE/de/risiko-management/assets/PwC_Risk_Management_Benchmarking_2011_2012.pdf, abgerufen: Januar 2013.

PricewaterhouseCoopers AG (2015): Risk Management Benchmarking 2015. https://www.pwc-wissen.de/pwc/de/shop/publikationen/Risk-Management-Benchmarking+2015/?card=16118, abgerufen: Februar 2017.

Purdy, Grant (2010): ISO 31000:2009 – Setting a New Standard for Risk Management. In: Risk Analysis, 30 (6), S. 881-886.

Rau-Bredow, Hans (2002): Value at Risk, Normalverteilungshypothese und Extremwertverhalten. In: Finanz Betrieb, Zeitschrift für Unternehmensfinanzierung und Finanzmanagement, 3, S. 603-607.

Recker, Jan C.; Rosemann, Michael; Indulska, Marta; Green, Peter (2009): Business process modeling: a comparative analysis. In: Journal of the Association for Information Systems, 10 (4), S. 333-363.

Recker, Jan (2010): Opportunities and constraints: the current struggle with BPMN. In: Business Process Management Journal, 16 (1), S. 181-201.

Reichling, Peter (2003): Basel II: Rating und Kreditkonditionen. In: Reichling, Peter (Hrsg.): Risikomanagement und Rating. 1. Auflage, Wiesbaden, S. 3-21.

Reichmann, Thomas; Kißler, Martin (2013): Sinnvolles Risikomanagement für den Mittelstand. In: Controlling, 25, Heft 4-5, S. 200-202.

Reichmann, Thomas; Kißler, Martin (2012): Betriebswirtschaftlich sinnvolles Risikomanagement für den Mittelstand. In: Controlling, 24, S. 241-246.

Renn, Ortwin (1998): Three decades of risk research: accomplishments and new challenges. In: Journal of Risk Research, 1 (1), S. 49–71.

Rikhardsson, Pall; Best, Peter J.; Green, Peter; Rosemann, Michael (2006): Business Process Risk Management and Internal Control: A proposed Research Agenda in the context of Compliance and ERP systems. Research in Progress, Presented at Second Asia/Pacific Research Symposium on Accounting Information Systems, Melbourne, https://eprints.qut.edu.au/5192/, abgerufen: Mai 2018.

Riehle, Dennis M.; Jannaber, Sven; Karhof, Arne; Thomas, Oliver; Delfmann, Patrick; Becker, Jörg (2016): On the de-facto Standard of Event-driven Process Chains: How EPC is defined in Literature. In: Modellierung 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, S. 61-76.

Rieke, Tobias (2009): Prozessorientiertes Risikomanagement: ein informationsmodellorientierter Ansatz. Berlin.

Rieke, Tobias; Winkelmann, Axel (2008): Modellierung und Management von Risiken. Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen. In: Wirtschaftsinformatik, 5, S. 346-356.

Risk and Insurance Management Society (2009): Enterprise Risk Management Technology Solutions, RIMS Inc., New York, https://www.rims.org/resources/ERM/Documents/ERM%20Technology%20Solutions.pdf, abgerufen: Mai 2017.

Risk Management Society (RIMS) (2013): 2013 RIMS Enterprise Risk Management (ERM) Survey. http://www.advisenltd.com/wp-content/uploads/rims-erm-survey-2013-09.pdf, abgerufen: Juni 2016.

Rochette, Michel (2009): From risk management to ERM. In: Journal of Risk Management in Financial Institutions, 2 (4), S. 394-408.

Rogler, Silvia (2002): Risikomanagement im Industriebetrieb. 1. Auflage, Wiesbaden.

Romeike, Frank; Finke Robert B. (2003): Erfolgsfaktor Risikomanagement. Wiesbaden.

Romeike, Frank; Gleißner, Werner (2012): Betriebswirtschaftlich sinnvolles Risikomanagement für den Mittelstand. In: Risk, Compliance & Audit, 5, S. 14-20.

Romeike, Frank; Eicher, Andreas; Köcher, Anette; Meissner, Jens (2013): Chancen-/ Risiko-Radar 2013 - Status quo einer risiko- und chancenorientierten Unternehmenssteuerung, https://www.risknet.de/fileadmin/eLibrary/Chancen-Risiko-Radar-2013_20130223.pdf, abgerufen: Juni 2016.

Rommelfanger, Heinrich (2008): Stand der Wissenschaft bei der Aggregation von Risiken. In: Deutsche Gesellschaft für Risikomanagement e.V. (Hrsg.): Risikoaggregation in der Praxis. Berlin Heidelberg, S. 15-50.

Rosenkranz, Friedrich; Missler-Behr, Magdalena (2005): Unternehmensrisiken erkennen und managen - Einführung in die quantitative Planung. Berlin Heidelberg.

Rostami, Ali; Sommerville, James; Wong, Ing Liang; Lee, Cynthia (2015): Risk management implementation in small and medium enterprises in the UK construction industry. In: Engineering, Construction and Architectural Management, 22 (1), S. 91-107.

Rossiter, Carmen (2001): Risk culture - up close and personal. In: CAmagazine, 134 (3), S. 45-50.

Rücker, Uwe-Christian (1999): Finanzierung von Umweltrisiken im Rahmen eines systematischen Risikomanagements. Sternenfels.

Rump, Frank L. (1999): Geschäftsprozeßmanagement auf der Basis ereignisgesteuerter Prozeßketten. Stuttgart Leipzig.

Ruud, Flemming T.; Sommer, Katerina (2006): Enterprise Risk Management - Das COSO-ERM-Framework. In: Der Schweizer Treuhänder, 3, S. 126-131.

Sadiq, Shazia, Governatori, Guido; Namiri, Kioumars (2007): Modeling Control Objectives for Business Process Compliance. In: Alonso G., Dadam P., Rosemann M. (Hrsg.): Business Process Management, BPM 2007, Lecture Notes in Computer Science, 4714, Berlin Heidelberg.

Sauerwein, Elmar; Thurner Matthias (1998): Der Risiko-Management-Prozeß im Überblick. In: Hinterhuber, Hans; Sauerwein, Elmar; Fohler-Norek, Christine (Hrsg.): Betriebliches Risikomanagement. Wien.

Scheer, August-Wilhelm (1992): Architektur integrierter Informationssysteme. 2. Auflage, Berlin Heidelberg.

Scheer, August-Wilhelm (1994): Wirtschaftsinformatik – Referenzmodelle für industrielle Geschäftsprozesse. 4. Auflage, Berlin Heidelberg.

Scheer, August-Wilhelm; Klueckmann, Joerg (2009): BPM 3.0. In: Dayal U.; Eder J.; Koehler J.; Reijers H.A. (Hrsg.): Business Process Management, BPM 2009, Lecture Notes in Computer Science, 5701, Berlin Heidelberg, S. 15-27.

Schenk, Alexander (1998): Techniken der Risikoidentifikation. In: Hinterhuber, Hans; Sauerwein, Elmar; Fohler-Norek, Christine (Hrsg.): Betriebliches Risikomanagement. Wien, S. 43-62.

Schierenbeck, Henner; Lister, Michael (2002): Value Controlling. 2. Auflage, München.

Schiller, Frank; Prpich, George (2014): Learning to organise risk management on organisations: what future for enterprise risk management? In: Journal of Risk Research, 17 (8), S. 999–1017.

Scholz, Roland W.; Blumer, Yann B.; Brand, Fridolin S. (2012): Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective. In: Journal of Risk Research, 15 (3), S. 313-330.

Schorcht, Heike; Brösel, Gerrit (2005): Risiko, Risikomanagement und Risikocontrolling im Lichte des Ertragsmanagements. In: Keuper, Frank; Roesing, Dirk und Schomann, Marc (Hrsg.): Integriertes Risiko und Ertragsmanagement. Wiesbaden.

Schuy, Axel (1989): Risiko-Management. Frankfurt am Main.

Schwintowski, Hans-Peter (2009): Gesetzlicher Rahmen für das Risikomanagement im öffentlichen Recht. In: Scholz, Frank; Schuler, Andreas; Schwintowski, Hans-Peter (Hrsg.): Risikomanagement der Öffentlichen Hand. Heidelberg, S. 184-203.

Searle, Samantha (2011): BPM Survey Insights: Organizations Using BPM to Reduce Costs and Improve Process Quality. https://www.gartner.com/id=1729244, abgerufen: April 2018.

Siepermann, Markus (2008): Risikokostenrechnung - Erfolgreiche Informationsversorgung und Risikoprävention. Berlin.

Sienou, Amadou; Lamine, Elyes; Karduck, Achim; Pingaud, Hervé (2007): Conceptual Model of Risk: Towards a Risk Modelling Language. In: Weske, Mathias; Hacid, Mohan-Said; Godart, Claude (Hrsg.): WISE 2007 Workshops, LNCS 4832, S. 118–129.

Sienou, Amadou; Lamine, Elyes; Karduck, Achim; Pingaud, Hervé (2009): Aspects of the BPRIM Language for Risk Driven Process Engineering. In: Meersman, Robert: Herrero, Pilar; Dillon, Tharam (Hrsg.): OTM 2009 Workshops, LNCS 5872, S. 172–183.

Smart, Philip. A.; Maddern, Harry; Maull, Roger S. (2008): Understanding Business Process Management: Implications for Theory and Practice. In: British Journal of Management, 20, S. 491–507.

Soltanizadeh, Sara; Rasid, Siti Z. A.; Golshan, Nargess; Quoquab, Farzana; Basiruddin, Rohaida (2014): Enterprise risk management practices among Malaysian firms. In: Procedia – Social and Behavioral Science, 164, S. 332-337.

Standards Australia and Standards New Zealand Technical Committee OB-007 (2009): AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines.

Steinhoff, Carsten (2008): Quantifizierung operationeller Risiken in Kreditinstituten. Göttingen.

Stohr, Edward A.; zur Muehlen, Michael (2008): Business Process Management: Impact on Organizational Flexibility. In: Global Journal of Flexible Systems Management, 9 (4), S. iii-v.

Strecker, Stefan; Heise, David; Frank, Ulrich (2011): RiskM: A multi-perspective modeling method for IT risk assessment. In: Information Systems Frontiers, 13 (4), S. 595–611.

Streitferdt, L. (1973): Grundlagen und Probleme der betriebswirtschaftlichen Risikotheorie. Wiesbaden.

Stroppi, Luis Jesús Ramón; Chiotti, Omar; Villarreal, Pablo David (2011): Extending BPMN 2.0: Method and Tool Support. In: Lecture Notes in Business Information Processing, 95, S. 59-73.

Suriadi, Suriadi; Weiß, Burkhard; Winkelmann, Axel; ter Hofstede, Arthur H.M.; Adams, Michael (2014): Current Research in Risk-Aware Business Process Management – Overview, Comparison and Gap Analysis. In: Communications of the Association for Information Systems (CAIS), 34, S. 933-984.

Szabo, Alina (2012): An Integrated Approach To Risk Management And Assessment. In: Annals of Faculty of Economics, University of Oradea, Faculty of Economics, 2 (1), S. 776–781.

Taylor, Paul ; Jimenez Godino, Jesús; Majeed, Basim (2008): Use of Fuzzy Reasoning in the Simulation of Risk Events in Business Processes. In: Proceedings of the 22nd European Conference on Modelling and Simulation, S. 25-30.

Tchankova, Lubka (2002): Risk identification - basic stage in risk management. In: Environmental Management and Health, 13 (3), S. 290-297.

Theuermann, Christian; Ebner, Gerhart (2014): Risikomanagement im österreichischen Mittelstand. https://www.campus02.at/news/risikomanagement-im-osterreichischen-mittelstand/, abgerufen: Mai 2017.

Thun Jörn-Henrik; Hoenig Daniel (2011): An empirical analysis of supply chain risk management in the German automotive industry. In: International Journal of Production Economics, 131 (1), S. 242-249.

Thun, Jörn-Henrik; Drüke, Martin; Hoenig, Daniel (2011): Managing uncertainty – an empirical analysis of supply chain riskmanagement in small and medium-sized enterprises. In: International Journal of Production Research, 49(18), S. 5511-5525.

United Kingdom Financial Reporting Council (FRC) (2014): Guidance on Risk Management, Internal Control and Related Financial and Business Reporting. https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pdf, abgerufen: Juli 2016.

United States of America: Sarbanes-Oxley Act of 2002. http://www.gpo.gov/fdsys/pkg/BILLS-107hr3763enr/pdf/BILLS-107hr3763enr.pdf, abgerufen: Januar 2015.

United States Securities and Exchange Commission - U.S. SEC (2003): Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

van der Aalst, Will M. P.; ter Hofstede, Arthur H.M.; Weske, Mathias (2003): Business Process Management: A Survey. In: van der Aalst, W.M.P; Weske M. (Hrsg.): Business Process Management, BPM 2003, Lecture Notes in Computer Science, Vol. 2678, Berlin Heidelberg.

van der Aalst, Will M. P.; Reijers, H. A.; Weijters, A. J. M.; van Dongen, B. F.; Alves de Medeiros, A. K.; Song, M.; Verbeek, H.M.W. (2007): Business process mining: An industrial application. In: Information Systems, 32, S. 713–732.

van der Aalst, Will M. P.; La Rosa, Marcello; Santoro, Flávia M. (2016): Business Process Management – Don’t Forget to Improve the Process! In: Business & Information Systems Engineering, 58 (1), S. 1-6.

van der Aalst, Will M. P. (2011): Process Mining – Discovery, Conformance and Enhancement of Business Processes. Heidelberg Dordrecht London New York.

Van der Gaag, L.C.; Renoooj, S.; Witteman, C.L.M.; Aleman, B.M.P.; Taal, B.G. (2002): Probabilities for a probabilistic network: a case study in oesophageal cancer. In: Artificial Intelligence in Medicine, 25 (2), S. 123-148.

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

Vanini, Ute (2014): Instrumente für eine systematische Identifikation von Risiken. In: Controller Magazin, 39 (4), S. 65-70.

Verbano, Chiara; Venturini, Karen (2011): Development paths of risk management: approaches, methods and fields of application. In: Journal of Risk Research, 14 (5), S. 519–550.

Victorian Auditor General (2013): Victorian Auditor General's Report: Implementation of the Government Risk Management Framework. http://www.audit.vic.gov.au/publications/20131030-Risk-Framework/20131030-Risk-Framework.pdf, abgerufen: Februar 2017.

Victorian Department of Treasury and Finance (2015): Victorian Government Risk Management Framework, http://www.dtf.vic.gov.au/files/ed6d7cd1-2fb4-44e2-bf38-a6ff010ee61e/Victorian-Government-Risk-Management-Framework.pdf, abgerufen: Februar 2017.

Viscelli, Therese R.; Hermanson, Dana R.; Beasley, Mark S. (2014): ERM: The Implementation Process and Strategic Effectiveness. http://coles.kennesaw.edu/research/docs/fall-2014/FALL14-05.pdf, abgerufen: Mai 2017.

Vollmer, Ken; Leganza, Gene; Pilecki, Mary; Smillie, Katie (2008): The EA View: BPM Has Become Mainstream.

Vose, David (2008): Risk Analysis - a quantitative quide. 3. Auflage, West Sussex.

Wagner, Karl; Klückmann, Jörg (2006): Prozessdesign als Grundlage von Compliance Management, Enterprise Architecture und Business Rules. In: Scheer, August Wilhelm; Kruppke, Helmut; Jost, Wolfram; Kindermann, Herbert (Hrsg.): Agilität durch ARIS Geschäftsprozessmanagement. Berlin Heidelberg.

Walther, Alfred (1953): Einführung in die Wirtschaftslehre der Unternehmung. Die Unternehmung, 2, Zürich.

Weiß, Burkhard; Winkelmann, Axel (2011): Developing a Process-Oriented Notation for Modeling Operational Risks – A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry. In: Proceedings of the 44th Hawaii International Conference on System Sciences, S. 1-10.

Wengert, Holger; Schittenhelm, Frank Andreas (2013): Corporate Risk Management. Berlin Heidelberg.

Werth, Dirk (2008): Modellierung unternehmensübergreifender Geschäftsprozesse: Modelle, Notationen und Vorgehen für prozessorientierte Unternehmensverbünde. In: Buchenau, Gerrit; Rietz, Steffen (Hrsg.): bdvb-Award Geschäftsprozess- und Projektmanagement 2006/07, Band 1, Bremen Hamburg.

Weske, Mathias (2012): Business Process Management. 2. Auflage, Heidelberg.

Weuster, Sandra (2014): Werkzeugunterstützung für Governance, Risk und Compliance Management.
https://www.softwareforen.de/portal/media/softwareforenleipzig/wissen/eigene_publikationen/Werkzeugunterstuetzung_fuer_Governance_Risk_und_Compliance_Management_-_Anwendungen_und_Marktuebersicht.pdf, abgerufen: April 2016.

Wolf, Klaus (2003): Risikoaggregation anhand der Monte-Carlo-Simulation. In: Controlling, 21 (10), S. 565-572.

Wolf, Klaus; Runzheimer, Bodo (2009): Risikomanagement und KonTraG. 5. Auflage, Wiesbaden.

Wolf, Rainer-Johannes (2010): Risikoorientiertes Netzwerkcontrolling: Bestimmung der Risikoposition von Unternehmensnetzwerken und Anpassung kooperationsspezifischer Controllinginstrumente an die Anforderungen des Risikomanagements. 1. Auflage, Bayreuth.

Wong, Wai Peng (2013): Business-process management: a proposed framework for future research. In: Total Quality Management, 24 (6), S. 719-732.

Worms, Martin- Josef (2014): Hessens Weg von der Kameralistik zur Doppik. In: Controlling & Management Review, Sonderheft 3, S. 58-63.

Wu, Desheng Dash; Chen, Shu-Heng; Olson, David L. (2014): Business intelligence in risk management: Some recent progresses. In: Information Sciences, 256 (20), S. 1-7.

Yaraghi, Niam; Langhe, Roland G. (2011): Critical success factors for risk management systems. In: Journal of Risk Research, 14 (5), S. 551–581.

Yousfi, Alaaeddine; Bauer, Christine; Saidi, Rajaa; Dey, Anind K. (2016): uBPMN: A BPMN extension for modeling ubiquitous business processes. In: Information and Software Technology, 74, S. 55–68.

Zhang, Yao; Fan, Zhi-ping (2014): An optimization method for selecting project risk response strategies. In: International Journal of Project Management, 32, S. 412-422.

Zhao, Xianbo; Hwang, Bon-Gang; Low, Sui Pheng Low (2014): Enterprise risk management implementation in construction firms. In: Management Decision, 52 (5), S. 814 – 833.

Zhao, Xianbo; Hwang, Bon-Gang; Low, Sui Pheng Low (2014): Enterprise risk management in construction firms: A proposed Implementation Framework. In: Proceedings of the 19th International Symposium on Advancement of Construction Management and Real Estate, S. 914-924.

zur Muehlen, Michael; Baumgart, A.; Junkers, C. (2006): A procedure model for the identification of risk in business processes. Technical report, Center of Excellence in Business Process Innovation, Stevens Institute of Technology, Hoboken, NJ.

zur Muehlen, Michael; Ho, Danny Ting-Yi (2006): Risk Management in the BPM Lifecycle. In: Bussler, Christoph; Haller, Armin (Hrsg.): BPM 2005 Workshops, LNCS, 3812, S. 454-466.

zur Muehlen, Michael; Rosemann, Michael (2005): Integrating Risks in Business Process Models. In: Proceedings of the 2005 Australasian Conference on Information Systems (ACIS 2005), Manly Sydney.

Anhang

Anbieter	Produkt	RM Phasenunterstützung					Systemart					Kommunikation		Flexibilität			ERP Anbindung						Datenbanken									Benutzerverwaltungen						
		Risiko identifizierung	Risikoquantifizierung & -beurteilung	Risikosteuerung	Risikokontrolle	Risikoreporting	Webbasiert Client/Server	Desktop Client/Server	Stand-Alone	Add-On	Nicht genannt	Im-/Export Funktionen	API	Entwickler Tools	Keine	Nicht genannt	SAP	MS Dynamics	Oracle	Andere	Keine	Nicht genannt	Oracle	MS SQL	MySQL	PostgreSQL	IBM DB2	Other SQL	Object Oriented	Keine	Nicht genannt	Active Directory	Novell edirectory	LDAP	IBM Domino	Andere	Keine	Nicht genannt
Informationssysteme mit Risikomanagement-Teilfunktionen (Q1)																																						
iGrafx GmbH (http://www.igrafx.com)	iGrafx	•	•		•	•	•	•				•	•	•			•						•	•							•		•				
Process Partner AG (http://www.processpartner.ch)	ProRisk	•	•	•	•	•	•					•	•	•			•						•	•			•				•		•				
Spezialapplikationen (Q2)																																						
CP Corporate Planning AG (http://www.corporate-planning.com)	CP Risk	•	•	•	•	•		•				•			•						•			•												•	
Ebix Inc (http://www.ebix.com)	RiskEnvision		•		•	•	•					•			•		•						•	•									•				
PVA Digital systems Ltd. (http://www.simprisk.com)	SimpRisk	•	•	•	•	•	•									•					•									•							•
Tinubu Square (http://www.tinubu.com)	Risk Management Center, etc.			•		•	•									•				•										•							•
UBS AG (https://www.ubs.com)	UBS Delta		•			•	•									•					•									•							•
WEHRSPOHN GmbH & Co. KG (http://www.wehrspohn.info)	RISK KIT SUITE	•	•			•	•	•	•	•		•	•	•							•			•												•	
Risikomanagement Software (Q3)																																						
Arengi (http://www.arengibox.com)	ArengiBox	•	•	•	•	•	•					•	•								•				•	•										•	
Avedos GmbH (http://www.avedos.com)	risk2value	•	•	•	•	•	•					•	•	•							•			•							•						
Decisio Unternehmensberatung GmbH (http://www.decisio.de)	RiskCity	•	•	•	•	•	•					•			•						•		•	•	•	•					•	•	•	•			
ibi systems GmbH (www.ibi-systems.de)	ibi systems iris	•	•	•	•	•	•					•	•							•			•	•	•			•					•		•		
Intaver Institute Inc. (http://www.intaver.com)	RiskyProject		•	•	•	•			•	•		•				•					•								•						•	
IRIS Intelligence Limited (http://www.irisintelligence.com)	IRIS (lite/prof/exp)	•	•	•	•	•	•		•			•	•								•			•							•		•				
LogicManager Inc. (http://www.logicmanager.com)	ERM Software	•	•	•	•	•	•									•						•									•						•
Observar AG (http://observar.ch)	Observar	•	•	•	•	•	•									•						•									•						•
Quantate Limited. (https://www.quantate.com)	Quantate Risk	•	•	•	•	•	•									•						•									•						•
RiskVision formerly Agiliance Inc. (https://www.riskvisioninc.com)	RiskVision	•	•	•	•	•	•					•				•						•	•		•												•
Secricon GmbH (http://www.secricon.ch)	Enterprise/Excel Risk Management	•	•	•	•	•	•	•	•			•		•							•			•	•							•		•				
ThomsonReuters (http://www.accelus.thomsonreuters.com)	Enterprise Risk Manager	•	•	•	•	•	•					•		•							•		•		•		•					•		•				
Risikomanagement-Informationssysteme (Q4)																																						
antares Informations-Systeme GmbH (http://www.antares-is.de)	RiMIS	•	•	•	•	•	•					•	•	•			•	•						•							•	•		•			
AxiomSL (http://www.axiomsl.com)	Risk Monitor	•	•	•	•	•	•	•				•		•			•	•	•	•			•	•	•	•	•				•	•	•	•			•
BOC Products & Services AG (http://www.boc-group.com)	ADONIS	•	•	•	•	•	•					•	•	•			•						•	•									•				
calpana business consulting gmbh (https://www.crisam.net)	CRISAM RMIS	•	•	•	•	•	•	•				•				•						•		•													•
CURA Software Solutions (http://www.curasoftware.com)	Cura GRC Suite	•	•	•	•	•	•		•			•	•				•	•	•	•				•								•						
Delta RM (http://www.deltarm.com)	Delta RM SUITE	•	•	•	•	•	•					•	•				•	•	•							•						•					
DHC Business Solutions GmbH & Co. KG (http://www.dhc-vision.com)	DHC VISION Risk Manager	•	•	•	•	•	•					•	•	•			•						•	•							•	•	•	•			
enrisma GmbH (http://www.enrisma.com)	Enrisma	•	•	•	•	•	•					•	•	•			•			•			•	•	•							•		•				
Fast Track Aust. Pty Ltd. (http://www.fasttrack365.com)	Fast Track	•	•	•	•	•	•					•	•				•	•	•				•	•									•				
Incom Pty Ltd. (http://www.incom.com.au)	Enterprise Risk Manager (ERM)	•	•		•	•						•	•				•	•	•	•					•							•		•	•			
interexa AG (http://interexa.de)	ORC Operational Risk Center	•	•	•	•	•					•					•					•									•							•
KdZen Inc. (http://riskgap.com)	RiskGap	•	•	•	•	•	•						•							•										•	•		•				
Marsh ClearSight LLC (http://www.marshclearsight.com)	Marsh ClearSight Platform	•	•	•	•	•	•					•			•			•	•				•										•				
MEGA International GmbH (http://www.mega.com)	HOPEX	•	•	•	•	•	•	•	•			•	•	•			•						•	•								•					
Opture AG (http://www.opture.com)	Opture	•	•	•	•	•	•					•	•				•	•	•				•	•	•	•	•	•				•	•	•			
PLATO AG (http://www.plato.de)	PLATO-SCIO Risikomanagement	•	•	•	•	•	•	•	•			•	•				•						•	•					•			•	•	•	•		•

Abbildung 115: Übersicht der Studienteilnehmer und des Leistungsangebots

	Anbieter	Produkt/e	RM-Prozessunterstützung						Systemart					Im-/Export					Anbindung				ERP-Anbindung						Datenbanken										Benutzerverwaltungen								Demoversion		Dauer Testzeitraum
			Identifikation	Bewertung	Steuerung	Überwachung	Reporting	Nicht aufgeführt	Webbasiert Client/Server	Desktop Client/Server	Stand-Alone	Add-On	nicht aufgeführt	Import	Export	beide	keine	nicht aufgeführt	API	E-Tools	keine	nicht aufgeführt	SAP	MS Dynamics	Oracle	Sonstige	keine	nicht aufgeführt	Oracle	MS SQL	MySQL	Postgre	IBM DB2	sonstige SQL	objektorientiert	keine	nicht aufgeführt	Active Directory	Novell edirectory	LDAP	IBM Domino	Sonstige	keine	nicht aufgeführt	Vermutliche Kategorie	freier Download	nach Registrierung	
1	360factors Inc. (http://www.360factors.com)	Predict360	●	●			●		●									●				●						●									●							●	Q3		x	30 Tage
2	3i Infotech Ltd. (http://3i-infotech.com3i-infotech)	KastleTM Risk Management	●	●		●	●		●							●						●						●	●								●							●	Q3			
3	4C Strategies (https://www.4cstrategies.com)	Exonaut RIM	●	●	●	●	●			●								●				●						●									●							●	Q3			
4	ACL Services Ltd. (http://www.acl.com)	ACL GRC	●	●	●	●	●		●							●						●	●														●							●	Q3			
5	Active Risk Group Ltd. (http://www.sword-activerisk.com)	Active risk Manager	●	●	●	●	●		●							●			●				●		●								●											●	Q4		x	
6	Acuity Risk Management LLP (http://www.acuityrm.com)	STREAM	●	●	●	●	●			●								●				●						●									●							●	Q3		x	
7	Agena (http://www.agenarisk.com)	AgenaRisk Desktop, AgenaRisk Enterprise		●		●					●					●			●									●									●							●	Q2	x		
8	AlignAlytics (http://align-alytics.com)	Align GRC	●	●	●	●	●		●									●				●						●									●							●	Q3			
9	Allegro Development Corporation (http://www.allegrodev.com)	Diverse		●									●					●				●						●									●							●	Q2			
10	Allgress (https://www.allgress.com)	Insight Risk Management Suite		●	●	●	●						●					●				●						●									●							●	Q3		x	
11	Alliantist Ltd. (http://www.isms.online)	ISMS.online		●	●	●	●		●									●				●						●									●							●	Q3	x		
12	Améthyste (http://www.amethyste.fr)	orKsoft						●		●								●				●						●									●							●	Q2			
13	antares Informations-Systeme GmbH (http://www.antares-is.de)	RiMIS	●	●	●	●	●		●							●			●	●			●	●						●							●	●		●					Q4			
14	APP Technologies, LLC (http://www.apptechnologies.biz)	Incident Management System	●			●	●		●							●			●									●		●							●								Q3			
15	AQ2 Technologies (http://aq2tech.com)	RiskXP				●							●					●				●						●									●							●	Q2			
16	Arengi (http://www.arengibox.com)	ArengiBox	●	●	●	●	●		●							●			●								●				●	●										●		Q3		x	
17	Avedos GmbH (http://www.avedos.com)	risk2value	●	●	●	●	●		●							●			●	●							●			●							●								Q3			
18	AxiomSL (http://www.axiomsl.com)	Risk Monitor	●	●	●	●	●		●	●						●				●			●	●	●	●			●	●	●	●	●					●	●	●	●	●			●	Q4		x	
19	Ba-PRO Company (https://www.ba-pro.com)	Risk Management Ba-PRO						●	●									●				●						●									●							●	Q2		x	30 Tage
20	BASIX4 (https://www.basix4.com)	BASIX4 Risk Reporting		●		●	●		●							●						●						●									●							●	Q3		x	
21	Bayesia S.A.S. (http://www.bayesia.com)	Bayesian Networks		●							●							●				●						●									●							●	Q2		x	
22	BishopPhillips Consulting Canada (http://www.bishopphillips.com)	RiskManager	●	●	●	●	●			●								●				●						●	●	●			●				●							●	Q3			
23	BOC Products & Services AG (http://www.boc-group.com)	ADONIS	●	●	●	●	●		●							●			●	●			●						●	●										●						Q4	x	x	10 Minuten Try-Out; 30 Tage Testversion
24	Brinqa (http://brinqa.com)	Brinqa	●	●	●	●	●		●							●						●						●						●			●							●	Q3		x	30 Tage
25	British Standards Institution (http://www.bsi-entropy.com)	Entropy						●					●					●				●						●									●							●	Q2		x	
26	BROWZ LLC (https://www.browz.com)	SURE Qualify						●	●									●				●						●									●							●	Q2		x	
27	Bureau van Dijk (http://www.bvdinfo.com)	Compliance Catalyst		●		●			●							●			●									●									●							●	Q2		x	
28	Bwise GmbH (http://www.bwise-grc.de)	BWise Risikomanagement	●	●	●	●	●		●									●				●						●									●							●	Q3			
29	CA Technology Pty Ltd. (http://www.cammsgroup.com)	CAMMS Integrated Risk Manager	●	●	●	●	●						●					●				●						●									●							●	Q3			
30	calpana business consulting gmbh (https://www.crisam.net)	CRISAM RMIS	●	●	●	●	●		●	●						●						●						●		●							●							●	Q4			
31	Castleforce (http://www.castleforce.co.uk)	Clarity GRC						●					●					●				●						●									●							●	Q2			
32	CEBOS Ltd. (http://www.cebos.com)	MQ1		●									●					●				●						●									●							●	Q2			
33	CGE Risk Management Solutions B.V. (http://www.cgerisk.com)	BowTieXP, BowTieServer, AuditXP	●	●						●								●				●						●									●							●	Q2		x	
34	Chase Cooper Limited (http://www.chasecooper.com)	aCCelerate	●	●	●	●	●						●					●				●						●									●							●	Q3			
35	Citicus Ltd. (http://www.citicus.com)	Citicus ONE	●	●	●	●	●		●							●						●						●									●	●		●					Q3		x	
36	CMO Software (http://www.cmo-software.com)	CMO COMPLIANCE	●	●	●	●	●		●									●	●				●					●									●							●	Q3		x	
37	ComplianceBridge Corporation (http://www.compliancebridge.com)	TotalCompliance	●						●									●				●						●									●							●	Q2		x	
38	Conning & Company (http://www.conning.com)	ADVISE		●									●					●				●						●									●							●	Q2			
39	CONNOS GmbH (https://www.aifm-control.de)	AIFMC.RM	●	●	●	●	●		●		●			●				●				●						●	●	●	●	●	●	●											Q3			
40	CorProfit Systems Pty Ltd. (http://www.corprofit.com)	KnowRisk	●	●	●	●	●			●	●							●				●						●	●	●				●											●	Q3		x	
41	Covalent Software Ltd. (http://www.covalentsoftware.com)	Covalent ERM	●	●	●	●	●		●					●								●						●									●							●	Q3		x	
42	CP Corporate Planning AG (http://www.corporate-planning.com)	CP Risk	●	●	●	●	●			●						●					●						●			●														●		Q2			
43	Crawford & Company (http://www.rkssciencesgroup.com)	DMITRI		●			●		●							●						●						●									●							●	Q2			
44	CURA Software Solutions (http://www.curasoftware.com)	Cura GRC Suite	●	●	●	●	●		●		●					●			●				●	●	●	●			●												●					Q4		x	
45	CWA GmbH (http://www.cwa.de)	CWA Flow	●	●	●	●	●		●						●							●						●									●							●	Q3		x	
46	Decisio Unternehmensberatung GmbH (http://www.decisio.de)	RiskCity	●	●	●	●	●		●							●					●						●	●	●	●	●							●	●	●	●	●				Q3		x	
47	Delta RM (http://www.deltarm.com)	Delta RM SUITE	●	●	●	●	●		●							●			●				●	●	●							●								●					Q4			
48	Devoteam (http://www.rvrparad.com)	RVR PARAD	●	●	●	●	●		●									●				●						●									●							●	Q3			
49	DHC Business Solutions GmbH & Co. KG (http://www.dhc-vision.com)	DHC VISION Risk Manager	●	●	●	●	●		●							●			●	●			●						●	●									●	●	●	●	●				Q4			
50	digital-media-lab pte Ltd. (http://www.digital-media-lab.com)	Business Risk Management	●	●	●	●	●						●					●				●						●									●							●	Q3			

	Anbieter	Produkt/e	RM-Prozessunterstützung						Systemart					Im-/Export				Anbindung				ERP-Anbindung					Datenbanken									Benutzerverwaltungen							Demoversion		Dauer Testzeitraum
			Identifikation	Bewertung	Steuerung	Überwachung	Reporting	Nicht aufgeführt	Webbasiert Client/Server	Desktop Client/Server	Stand-Alone	Add-On	nicht aufgeführt	Import	Export	beide	keine	nicht aufgeführt	API	E-Tools	keine	nicht aufgeführt	SAP	MS Dynamics	Oracle	Sonstige	keine	nicht aufgeführt	Oracle	MS SQL	MySQL	Postgre	IBM DB2	sonstige SQL	objektorientiert	keine	nicht aufgeführt	Active Directory	Novell edirectory	LDAP	IBM Domino	Sonstige	keine	nicht aufgeführt	Vermutliche Kategorie	freier Download	nach Registrierung	
51	docs&rules GmbH (http://www.grc-cockpit.de)	GRC Cockpit	●	●	●	●	●		●									●				●															●						●	Q3			
52	Effisoft SAS (http://www.effisoft.com)	Webrisk	●	●	●	●	●		●									●				●															●						●	Q3		x	
53	eFront (http://ermcrm.efront.com)	FrontERM, FrontGRC	●	●	●	●	●		●									●				●															●						●	Q3			
54	Ebix Inc			●		●	●		●							●					●		●																				Q2			
55	EMC Corporation (https://www.rsa.com)	RSA Archer	●	●	●	●	●		●							●						●														●						●	Q3		x	
56	Emex (http://emex.com)	EMEX EHS Solution	●	●			●		●									●				●														●						●	Q3			
57	ENABLON NORTH AMERICA CORP. (http://www.enablon.fr)	Enablon RM	●	●	●	●	●		●									●				●														●						●	Q3		x	
58	enrisma GmbH (http://www.enrisma.com)	Enrisma	●	●	●	●	●		●							●			●	●			●			●			●	●	●						●		●				Q4			
59	Essential Systems LLC (http://essentialsystemsllc.com)	OptiModel	●	●	●	●	●		●								●					●														●						●	Q3		x	
60	EuroRisk Systems Ltd. (http://www.eurorisksystems.com)	Risk Engine, Risk Framework, Risk Evaluator, PMS Modules		●									●					●				●														●						●	Q2		x	
61	Fair Isaac Germany GmbH (http://www.tonbeller.com)	FICO TONBELLER	●	●	●	●	●		●									●				●														●						●	Q3			
62	Fast Track Aust. Pty Ltd. (http://www.fasttrack365.com)	Fast Track	●	●	●	●	●		●							●			●				●	●	●				●	●									●				Q4		x	
63	FinAnalytica Inc. (http://www.finanalytica.com)	Cognity		●			●		●									●				●														●						●	Q2			
64	FIS (http://www.fisglobal.com)	Early Risk Manager	●	●	●	●	●						●					●				●														●						●	Q3		x	
65	Frontline Systems Inc. (http://www.solver.com)	Solver SDK Platform		●					●							●			●																	●						●	Q2		x	15 Tage
66	Funk Gruppe GmbH (http://www.funk-gruppe.de)	RIMIKS, EVIDENCE	●	●	●	●	●		●									●				●														●						●	Q3			
67	Fusion Risk Management Inc. (http://www.fusionrm.comproducts-services)	Fusion	●	●	●	●	●		●							●			●																	●						●	Q3		x	
68	Gesundheitsforen Leipzig GmbH (http://www.gesundheitsforen.net)	riskKV Suite, riskKH	●	●								●	●					●				●														●						●	Q2			
69	Great Budget Software (http://greatbudget.com)	CRIMS		●								●						●				●				●								●							●		Q2			
70	GUY CARPENTER & COMPANY, LLC (http://www.guycarp.com)	MetaRisk		●									●	●								●														●						●	Q2			
71	Hiperos LLC. (https://www.hiperos.com)	Hiperos 3PM	●	●	●	●	●						●					●				●														●						●	Q3		x	
72	Hulocon (http://www.hulocon.de)	rimanis	●	●	●	●	●				●				●							●														●						●	Q3		x	
73	ibi systems GmbH (www.ibi-systems.de)	ibi systems iris	●	●	●	●	●		●							●			●							●			●	●	●			●			●		●		●		Q3		x	3 Monate
74	IBM Deutschland GmbH (http://www-03.ibm.com)	OpenPages	●	●	●	●	●		●									●				●														●						●	Q3		x	
75	Ideagen, Plc. (http://www.ideagenplc.com)	Gael Enlighten, Gael Risk	●	●	●	●	●		●									●				●														●						●	Q3		x	
76	IDI Technology (Pty) Ltd. (http://www.barnowl.co.za)	BarnOwl	●	●	●	●	●						●		●							●														●						●	Q3		x	
77	IDV Solutions LLC. (http://idvsolutions.com)	Visual Command Center		●	●	●			●									●	●							●										●						●	Q3			
78	iGrafx GmbH (http://www.igrafx.com)	iGrafx	●	●		●	●		●	●						●			●	●			●						●	●							●		●				Q1		x	10 Tage
79	IHS Inc. (https://www.ihs.com)	IHS IMPACT ERM, IHS Risk Assessment		●	●	●							●					●				●														●						●	Q3			
80	IMS AG (http://www.ims-ag.com)	IMS Premium			●	●			●						●							●							●							●							Q2		x	
81	Incom Pty Ltd. (http://www.incom.com.au)	Enterprise Risk Manager (ERM)	●	●		●	●									●			●				●	●	●	●				●							●		●	●			Q4		x	
82	INFORM Applications Inc. (http://www.informapplications.com)	INFORM RMIS Portal		●	●		●		●									●				●														●						●	Q3			
83	Information Risk Management Ltd. (https://irmsecurity.com)	SYNERGi				●	●						●					●				●														●						●	Q2			
84	Inkling Incorporated (http://www.inklingmarkets.com)	Inkling Markets		●			●		●						●							●														●						●	Q2		x	14 Tage
85	Intaver Institute Inc. (http://www.intaver.com)	RiskyProject		●	●	●	●				●	●				●						●					●								●						●		Q3		x	30 Tage
86	interexa AG (http://interexa.de)	ORC Operational Risk Center	●	●	●	●	●						●					●				●														●						●	Q4			
87	Invantive BV (http://www.invantive.com)	Invantive Control for Excel		●		●						●				●				●								●								●					●		Q2	x		
88	Investor Analytics (http://www.investoranalytics.com)	Investor Analytics		●			●		●						●							●														●						●	Q2		x	
89	IRIS Intelligence Limited (http://www.irisintelligence.com)	IRIS (lite/prof/exp)	●	●	●	●	●		●		●					●			●								●			●							●		●				Q3		x	
90	ISARR (http://www.isarr.com)	ISARR		●		●	●						●		●			●				●														●						●	Q3			
91	JC Applications Development Limited (http://www.jcad.co.uk)	JCAD CORE/JCAD LACHS	●	●	●	●	●		●						●							●														●						●	Q3		x	
92	Kamakura Corporation (http://www.kamakuraco.com)	Kamakura Risk Manager		●	●	●							●					●				●														●						●	Q3			
93	KdZen Inc. (http://riskgap.com)	RiskGap	●	●	●	●	●		●									●	●							●										●		●				Q4		x	
94	Keyword SARL (http://www.keyword.fr)	ISMAN GRC	●	●	●	●	●		●							●						●														●						●	Q3			
95	LockPath Inc., prevalent (https://www.lockpath.complatform)	Keylight Platform, Risk Manager	●	●	●	●	●						●					●	●																	●						●	Q3		x	
96	LogicManager Inc. (http://www.logicmanager.com)	Enterprise Risk Management (ERM) Software	●	●	●	●	●		●									●				●														●						●	Q3		x	
97	Lumina Decision Systems (http://www.lumina.comwhy-analytica)	Analytica		●							●							●				●														●						●	Q2	x		
98	Maclear SA (http://maclear-grc.com)	Maclear eGRC Suite	●	●	●	●	●						●					●				●														●						●	Q3		x	
99	Magique Galileo Software Ltd. (http://www.magiquegalileo.com)	Magique	●	●	●	●	●		●						●							●														●						●	Q3			
100	Markit Group Limited (http://www.markit.com)	Markit Analytics		●									●					●				●														●						●	Q2			

	Anbieter	Produkt/e	RM-Prozessunterstützung						Systemart				Im-/Export				Anbindung				ERP-Anbindung					Datenbanken										Benutzerverwaltungen							Demoversion		Dauer Testzeitraum
			Identifikation	Bewertung	Steuerung	Überwachung	Reporting	Nicht aufgeführt	Webbasiert Client/Server	Desktop Client/Server	Stand-Alone	Add-On	nicht aufgeführt	Import	Export	beide	keine	nicht aufgeführt	API	E-Tools	keine	nicht aufgeführt	SAP	MS Dynamics	Oracle	Sonstige	keine	nicht aufgeführt	Oracle	MS SQL	MySQL	Postgre	IBM DB2	sonstige SQL	objektorientiert	keine	nicht aufgeführt	Active Directory	Novell edirectory	LDAP	IBM Domino	Sonstige	keine	nicht aufgeführt	Vermutliche Kategorie	freier Download	nach Registrierung	
101	Marsh ClearSight LLC (http://www.marshclearsight.com)	Marsh ClearSight Platform	●	●	●	●	●		●							●					●																						Q4		x	
102	MasterControl Inc. (http://de.mastercontrol.com)	MasterControl Risk Analysis	●	●	●	●	●		●									●				●						●								●							●	Q3			
103	MEGA International GmbH (http://www.mega.com)	HOPEX	●	●	●	●	●		●	●	●					●			●	●			●						●	●							●							Q4		x	
104	MetricStream Inc. (http://www.metricstream.com)	MetricStream GRC Platform	●	●	●	●	●		●									●		●								●								●							●	Q3			
105	Metrix Software Solutions (Pty) Ltd. (http://www.isometrix.com)	IsoMetrix	●	●	●	●	●						●					●				●						●								●							●	Q3		x	
106	Misys (http://www.misys.com)	FusionRisk		●									●					●				●						●								●							●	Q2			
107	Modulo Security LLC. (http://modulo.com)	Enterprise Risk Management	●	●	●	●	●						●					●				●						●								●							●	Q3			
108	Morgan Kai Limited (http://www.mkinsight.com)	MKinsight ERM	●	●	●	●	●		●									●				●						●								●							●	Q3			
109	msg life AG (https://www.msg-life.com)	msg.Alamos		●									●					●				●						●								●							●	Q2			
110	MUREX S.A.S (https://www.murex.com)	MX.3		●									●					●				●						●								●							●	Q2			
111	Nasdaq Inc. (http://www.bwise.com)	Bwise	●	●	●	●	●						●					●				●						●								●							●	Q3			
112	Novasecur S.A.S (http://www.novasecur.com)	MyNovasecur	●	●	●	●	●						●					●				●						●								●							●	Q3			
113	NTT DATA Figtree Systems Pty Ltd. (http://www.figtreesystems.com)	Claims and Risk Management Software Suite: Figtree<risk>	●	●	●	●	●		●						●							●						●								●							●	Q3			
114	Numerix LLC (http://www.numerix.com)	Numerix Oneview		●									●					●				●						●								●							●	Q2		x	
115	Objective Controls (Highwrite Group) (http://www.objectivecontrols.com)	Objective Controls Pro, Objective Controls Essentials	●	●	●	●	●		●									●				●						●								●							●	Q3			
116	Observar AG (http://observar.ch)	Observar	●	●	●	●	●		●									●				●						●								●							●	Q3			
117	Omega AS (https://www.omega.no)	Pims Risk Management	●	●	●		●			●								●				●						●								●							●	Q3		x	
118	OneSoft Connect (https://www.onesft.com)	OneSoft Connect		●	●	●			●									●				●						●								●							●	Q3		x	
119	OpenGamma Limited (http://www.opengamma.com)	OpenGamma Market Risk		●									●					●	●									●								●							●	Q2			
120	Optial UK Ltd. (http://www.optial.com)	SmartStart, OPRisk	●	●	●	●	●		●						●							●						●								●							●	Q3		x	
121	Opture AG (http://www.opture.com)	Opture	●	●	●	●	●		●							●			●				●	●	●				●	●	●	●	●	●			●	●	●	●				Q4			
122	Oracle BV. & Co. KG (http://www.oracle.com)	Crystall Ball		●								●				●						●						●								●							●	Q2			
123	Origami Risk LLC (http://www.origamirisk.com)	Origami Risk		●	●	●	●		●							●						●						●								●							●	Q3			
124	OVERMIND (http://www.overmind-dynamic.com)	Global Risk Assessment		●							●							●				●						●								●							●	Q2			
125	OXAND S.A.S (http://www.oxand.com)	Simeo		●								●						●				●						●								●							●	Q2			
126	Oxial AG (http://www.oxial.com)	OXIAL GRC Suite, OXIAL GRC Express	●	●	●	●	●		●									●				●						●								●							●	Q3		x	
127	Palisade Europe (http://www.palisade.com)	@RISK		●								●				●				●							●							●								●	Q2		x	
128	PAN Software Pty. Ltd. (http://www.riskcloud.net)	riskcloud.net, RiskWare	●	●	●	●	●		●									●				●						●								●							●	Q3		x	
129	parcIT GmbH (http://www.parcit.de)	Okular PROKORISK	●	●	●	●	●		●	●					●							●						●								●							●	Q3			
130	Pilgrim Quality Solutions Inc. (http://pilgrimquality.com)	SmartSolve	●	●	●	●	●						●					●				●				●										●							●	Q3			
131	PLATO AG (http://www.plato.de)	PLATO-SCIO Risikomanagement	●	●	●	●	●		●	●	●					●			●				●											●			●	●	●	●			●	Q4		x	90 Tage
132	Proactima Solution AS. (https://uxrisk.com)	UXRISK	●	●	●	●	●		●						●							●						●								●							●	Q3			
133	Process Partner AG (http://www.processpartner.ch)	ProRisk	●	●	●	●	●		●							●			●	●			●						●	●			●				●		●						Q1			
134	ProcessGene Ltd. (http://www.processgene.com)	ProcessGene Suite	●	●	●	●	●		●									●				●	●		●											●							●	Q3		x	30 Tage
135	ProcessUnity Inc. (http://www.processunity.com)	GRC Platform	●	●	●	●	●						●					●				●						●								●							●	Q3			
136	PRO-CONCEPTS LLC. (http://www.proconceptsllc.com)	Risk Radar	●	●	●	●	●		●						●							●						●								●							●	Q3		x	
137	Protecht (http://www.protecht.eu)	Protecht.ERM	●	●	●	●	●		●							●						●						●								●							●	Q3		x	
138	Protiviti GmbH (http://www.protiviti.de)	Governance Portal	●	●	●	●	●		●									●				●						●								●							●	Q3			
139	PVA Digital systems Ltd. (http://www.simprisk.com)	SimpRisk	●	●	●	●	●		●									●				●						●								●							●	Q2		x	
140	Quantar Solutions (www.quantarsolutions.com)	Risk Compliance & Resilience Suite (RCR Suite)		●							●							●				●						●								●							●	Q2			
141	Quantate Limited. (https://www.quantate.com)	Quantate Risk	●	●	●	●	●		●									●				●						●								●							●	Q3		x	
142	QUANTIFI Inc. (https://www.quantifisolutions.com)	Quantifi		●									●			●			●														●										●	Q2		x	
143	Quantivate LLC. (http://quantivate.com)	Quantitative GRC Suite	●	●	●	●	●						●					●				●						●								●							●	Q3			
144	QuantRisk Corporation. (http://www.quantrisk.com)	QR Risk		●					●									●				●						●								●							●	Q2			
145	Quartet FS. (https://quartetfs.com)	Activepivot		●									●					●				●						●								●							●	Q2			
146	Recovery Planner (https://www.recoveryplanner.com)	RPX Enterprise Risk Management	●	●	●	●	●		●							●			●									●								●							●	Q3			
147	Relational Security Corporation (http://www.rsam.com)	Rsam Platform		●	●	●	●						●			●						●				●		●					●						●						Q3			
148	Resolver Inc. (http://www.resolvergrc.com)	GRC Cloud / RM:A / RM:R	●	●	●	●	●		●									●				●						●								●							●	Q3		x	
149	Reval (http://www.reval.com)	CHOICE, CORE	●	●									●					●				●						●								●							●	Q2		x	
150	Risk Decisions Ltd. (http://www.riskdecisions.com)	Predict!	●	●	●	●	●		●	●		●				●						●						●								●							●	Q3			

	Anbieter	Produkt/e	RM-Prozessunterstützung						Systemart					Im-/Export					Anbindung				ERP-Anbindung						Datenbanken										Benutzerverwaltungen								Demoversion		Dauer Testzeitraum
			Identifikation	Bewertung	Steuerung	Überwachung	Reporting	Nicht aufgeführt	Webbasiert Client/Server	Desktop Client/Server	Stand-Alone	Add-On	nicht aufgeführt	Import	Export	beide	keine	nicht aufgeführt	API	E-Tools	keine	nicht aufgeführt	SAP	MS Dynamics	Oracle	Sonstige	keine	nicht aufgeführt	Oracle	MS SQL	MySQL	Postgre	IBM DB2	sonstige SQL	objektorientiert	keine	nicht aufgeführt	Active Directory	Novell edirectory	LDAP	IBM Domino	Sonstige	keine	nicht aufgeführt	Vermutliche Kategorie	freier Download	nach Registrierung	
151	Risk Reasoning Ltd. (http://www.riskreasoning.co.uk)	RiskAid		●	●	●							●	●								●						●									●							●	Q3			
152	Riskdata S. A. (https://www.riskdata.com)	Riskdata		●									●			●			●			●						●									●							●	Q2			
153	riskHive Software Solutions Ltd. (http://www.riskhive.com)	Enterprise Risk Manager		●					●							●						●						●									●							●	Q2			
154	riskmethods GmbH (http://www.riskmethods.net)	riskmethods: Risk Radar, Impact Analyser, Action Planner	●	●		●			●									●				●						●									●							●	Q3		x	30 Tage
155	Riskonnect Inc. (http://www.riskonnect.com)	Riskonnect GRC, Riskonnect GRC/RMIS/EHS/HC		●	●	●	●		●									●				●						●									●							●	Q3		x	
156	RiskTrak International (http://www.risktrak.com)	RiskTrak, RiskTrak.NET	●	●	●	●	●		●	●								●				●						●									●							●	Q3		x	
157	RiskVision formerly Agiliance Inc. (https://www.riskvisioninc.com)	RiskVision	●	●	●	●	●		●							●						●						●	●		●						●							●	Q3			
158	RiskWatch (http://www.riskwatch.com)	ComplianceWatch		●	●								●					●				●						●									●							●	Q2		x	
159	Rivo Software Ltd. (http://www.rivosoftware.com)	Rivo	●	●	●								●					●				●						●									●							●	Q3			
160	ROKOCO GmbH (http://www.rokoco.com)	RisCo2	●	●	●	●	●			●				●								●						●									●							●	Q3			
161	RSM UK Group LLP (http://www.insight4grc.com)	4risk	●	●	●	●	●		●									●				●						●									●							●	Q3			
162	Safety software Ltd. (http://www.airsweb.com)	airsweb		●	●	●			●									●				●						●									●							●	Q3			
163	SAI Global Limited (http://www.compliance360.com)	Compliance 360	●	●	●	●	●						●					●				●						●									●							●	Q3			
164	SAP Deutschland SE & Co. KG (http://go.sap.com)	SAP Risk Management	●	●	●	●	●		●							●			●	●			●							●			●					●	●	●					Q4			
165	SAS Institute GmbH (http://www.sas.com)	SAS Enterprise GRC	●	●	●	●	●		●									●				●						●	●	●		●	●				●							●	Q3			
166	Schleupen AG (https://www.schleupen.de)	R2C - risk to chance	●	●	●	●	●		●									●				●						●									●							●	Q3			
167	SecondFloor (https://www.secondfloor.com)	GRC Solutions		●	●	●							●					●				●						●									●							●	Q3		x	
168	Secricon GmbH (http://www.secricon.ch)	Enterprise/Excel Risk Management	●	●	●	●	●		●	●	●					●					●						●			●	●						●		●					Q3			
169	SimCorp A/S (http://www.simcorp.com)	SimCorp Dimension - Risk Analysis Manager		●			●						●					●				●						●									●							●	Q2			
170	Software AG (http://www.softwareag.com)	ARIS GRC Platform	●	●	●	●	●						●					●				●						●									●							●	Q3			
171	StatPro Group plc (http://www.statpro.com)	StatPro Revolution		●					●						●				●									●									●							●	Q2			
172	Stewart Business Software (http://www.stewart-software.co.uk)	MIMS RM	●	●	●	●	●						●		●							●						●									●							●	Q3			
173	Stiki (http://www.riskmanagementstudio.com)	RM Studio	●	●	●	●	●		●						●							●						●									●							●	Q3		x	15 Tage
174	Structured Data LLC (http://www.riskamp.com/)	RiskAMP		●								●				●					●						●								●						●			Q2	x		
175	SureCloud Limited (https://www.surecloud.com)	SureCloud Risk Management	●	●	●	●	●		●									●				●						●									●							●	Q3			
176	Sword Group Ltd. (http://www.sword-achiever.com)	Achiever	●	●	●	●	●		●									●				●						●									●							●	Q3		x	
177	Symbiant (www.symbiant.co.uk)	Symbiant Tracker, Symbiant Risk Suite	●	●	●	●	●		●									●				●						●									●							●	Q3		x	
178	Syncopation Software Inc. (https://www.syncopation.com)	DPL 8		●							●							●				●						●									●							●	Q2		x	
179	ThomsonReuters (http://www.accelus.thomsonreuters.com)	Enterprise Risk Manager	●	●	●	●	●		●							●				●						●			●		●						●		●					Q3			
180	Tinubu Square (http://www.tinubu.com)	Risk Management Center, etc.			●		●		●									●							●										●							●	Q2		x	
181	UB Dr. Matthias Vieth (http://www.vmc-sys.com)	SAMS interactive	●						●									●				●						●									●							●	Q2			
182	UBS AG (https://www.ubs.com)	UBS Delta		●			●		●									●				●						●									●							●	Q2			
183	Ultima Risk Management Ltd. (http://www.ultimariskmanagement.com)	Abriska	●	●	●	●	●						●					●				●						●									●							●	Q3			
184	Ultimate Risk Solutions (http://www.ultirisk.com)	Risk Explorer		●							●					●						●						●									●							●	Q2			
185	Unuby Software SRL (https://riscomatic.com)	Riscomatic		●		●			●									●				●						●									●							●	Q2		x	14 Tage
186	VelocityEHS (https://www.ehs.com)	VelocityEHS Product Suite		●	●	●	●		●									●				●						●									●							●	Q3		x	
187	Ventiv Technology Inc. (http://www.ventivtech.com)	RiskConsole	●	●	●	●	●		●							●						●						●									●							●	Q3		x	
188	WEHRSPOHN GmbH & Co. KG (http://www.wehrspohn.info)	RISK KIT SUITE	●	●			●		●	●	●	●				●			●	●							●			●												●		Q2		x	1 Monat
189	Wilshire Associates Europe B.V. (http://wilshire.com)	Wilshire Omnia		●	●	●	●			●						●			●									●									●							●	Q3			
190	Wynyard Group (https://www.wynyardgroup.com)	Wynyard Risk Management	●	●	●	●	●		●							●			●									●					●						●						Q3			
191	Xactium Limited (http://www.xactium.com)	Risk Management Software	●	●	●	●	●		●						●							●						●									●							●	Q3		x	
192	Xyea (http://www.xyea.com)	Xyea		●	●	●			●					●								●						●		●							●							●	Q3		x	15 Tage

Abbildung 116: Übersicht RMIS Gesamtmarkt

Fragebogen der Marktstudie

1. Wo befinden sich Ihre weltweiten Standorte?
   China
   Deutschland
   Frankreich
   Großbritannien
   Indien
   Italien
   Japan
   Kanada
   Niederlande
   Norwegen
   Polen
   Portugal
   Russland
   Schweden
   Spanien
   Südkorea
   USA
   Sonstiges
2. Bitte nennen Sie Ihre wichtigsten Referenzkunden.
3. Aus welchen Branchen stammen Ihre Kunden hauptsächlich?
   Automobilwirtschaft
   Bauwirtschaft
   Chemie
   Dienstleistungen
   Elektrotechnik- und Elektronikindustrie
   Energie
   Finanzdienstleistungen
   Gesundheit
   Informationstechnologie & -Dienste
   Lebensmittel
   Logistik
   Luft- und Raumfahrt
   Maschinen- und Anlagenbau
   Öffentliche Verwaltung
   Tourismus
   Sonstiges
4. Welche Zielgruppe sprechen Sie mit Ihrer Software an?
   Öffentlicher Sektor
   Kleine und mittelständische Unternehmen (KMUs)
   Großunternehmen
   Sonstiges
5. Bitte geben Sie den Umsatz Ihres Unternehmens im Jahre 2014 an.
   bis 500.000 €

zwischen 500.000€ und 2.000.000 €
über 2.000.000 €

6. Bitte geben Sie an, wie viel Prozent des Umsatzes in Forschung und Entwicklung investiert wird.
   unter 5%
   5% - 10%
   11% - 20%
   21% - 30 %
   über 30%
7. Bitte nennen Sie den Namen Ihrer Software.
8. Wie viele Releases Ihrer Software veröffentlicht Ihr Unternehmen jährlich?
9. Bitte geben Sie die Sprachen an, in denen Ihre Software angeboten wird.
   Chinesisch
   Deutsch
   Englisch
   Französisch
   Hindi
   Italienisch
   Japanisch
   Koreanisch
   Niederländisch
   Norwegisch
   Polnisch
   Portugiesisch
   Russisch
   Schwedisch
   Spanisch
   Sonstiges
10. Welche Währungen werden unterstützt?
    beliebige
    Chinesischer Yen
    Euro
    Britische Pfund
    Indische Rupie
    Japanischer Yen
    Kanadischer Dollar
    Norwegische Krone
    Polnischer Zloty
    Russischer Rubel
    Schwedische Krone
    Südkoreanischer Won
    US-Dollar
    Sonstiges
11. In welcher Programmiersprache ist Ihr Programm entwickelt?
    C
    C++
    Java

PHP
Sonstiges

12. Wie lange dauert die Einführung Ihrer Software bei einem Kunden üblicherweise?
    Sonstiges
    1 Woche
    3- 4 Wochen
    1 - 3 Monate
    4 - 6 Monate
    7 - 12 Monate
    über 1 Jahr
13. Welche Art der Software bieten Sie an?
    webbasiertes Client-Server System
    nicht webbasiertes Client-Server System
    Stand-Alone Software
    Add-On
14. Für welche Software gibt es Ihr Add-On?
15. Ist Ihre Software mandantenfähig?
16. Ist Ihre Software ein Ein- oder ein Mehrbenutzersystem?
    Einbenutzersystem
    Mehrbenutzersystem
17. Besteht die Möglichkeit einer Anbindung an eine externe Benutzerverwaltung?
18. Welche Benutzerverwaltungen können mit Ihrer Software verbunden werden?
    Microsoft Exchange
    Novell eDirectory
    OpenLDAP
    IBM Notes (Lotus Notes)
    Sonstiges
19. Welche der folgenden Datenbankmanagementsysteme unterstützt Ihre Software?
    Oracle
    Microsoft SQL Server
    MySQL
    PostgreSQL
    IBM - DB2
    jegliche
    Sonstiges
20. Für welche der folgenden Drittanbietersoftware bietet Ihre Lösung Schnittstellen für den Datenimport?
    SAP
    Microsoft Dynamics
    Oracle Enterprise Manager
    Sonstiges
21. In welcher Form kann zugegriffen werden?
    nur lesend
    lesend und schreibend
22. In welchen Formaten können Daten importiert bzw. exportiert werden?
    csv
    sql

xls
xml
Sonstiges

23. Bietet Ihre Software ein Application Programming Interface (API) ?
24. Unterstützt Ihre Software Entwicklertools, um die Standardfunktionen zu erweitern?
25. Welche Programmiersprachen werden durch die Entwicklertools unterstützt?
26. Nennen Sie alle Desktop-Browser, die von Ihrer Software unterstützt werden.
    Google Chrome
    Microsoft Edge
    Microsoft Internet Explorer
    Mozilla Firefox
    Opera
    Safari
    Sonstiges
27. Wie kann man Ihre Software auf mobilen Endgeräten nutzen?
    Mittels eigener App
    Per mobilem Webbrowser
    Software ist nicht auf mobilen Geräten einsetzbar
28. Nennen Sie alle mobilen Browser, die von Ihrer Software unterstützt werden.
    Dolphin
    Google Chrome
    Microsoft Edge
    Microsoft Internet Explorer Mobile
    Mozilla Firefox
    Opera Mini
    Safari
    Sonstiges
29. Nennen Sie alle mobilen Betriebssysteme, für die es eine App gibt.
    Android
    Apple iOS
    Windows Phone
    Blackberry OS
    Sonstiges
30. Welche Mindestsystemvoraussetzungen benötigt Ihre Software client-seitig?
31. Welche Mindestsystemvoraussetzungen benötigt Ihre Software server-seitig?
32. Unterstützt Ihre Software eine Backup-Funktion?
33. Wie funktioniert das Backup?
    automatisch
    manuell
34. Sind Backup-Zeiten konfigurierbar?
35. Werden inkrementelle Backups unterstützt?
36. Nutzt Ihre Software durchgängig verschlüsselte Kommunikation?
37. Unterstützt Ihre Software eine Historie von Aktionen der Benutzer?
38. Unterstützt Ihre Software ein Benutzerrollenkonzept?
39. Ist das Rollenkonzept frei konfigurierbar?
40. Gibt es die Möglichkeit, eigene Benutzerrollen zu erstellen?

41. Können Dateien in das System geladen werden (z.B. zum Wissensmanagement oder als Zusatz-/Hintergrundinformation)?
42. Welche Dateiformate werden unterstützt?
    csv
    docx
    pdf
    xlsx
    Sonstiges
43. Können Daten aus externen Web-Services in das System geladen werden?
44. Welche Web-Services können genutzt werden?
45. Unterstützt Ihre Software eine systemweite Suche? (z. B. nach Elementen wie Risiken, Maßnahmen, Abteilungen oder Personen)
46. Bietet Ihre Software konfigurierbare E-Mail-Benachrichtigungen bei bestimmten Ereignissen?
47. Unterstützt Ihre Software eine Papierkorbfunktion, um versehentliches Löschen von wichtigen Daten zu verhindern und diese bei Bedarf wiederherstellen zu können?
48. Unterstützt Ihre Software eine Art "Rückgängig-Funktion", über die es möglich ist einzelne Benutzeraktionen unmittelbar rückgängig zu machen?
49. Bietet Ihre Software eine interne Hilfsdatenbank zur Programmfunktionalität an?
    Ja
    Ja, mit eigener Suchfunktion
    Nein
50. Werden in der Benutzeroberfläche Ihrer Software Tooltipps angezeigt?
51. Unterstützt Ihre Software die Vergabe von Schlüsselwörtern (Tags) für Risiken, Maßnahmen, Abteilungen oder Personen?
52. Haben Sie Anmerkungen und Ergänzungen zu besonderen Funktionen Ihres Systems?
53. Bei welchen der folgenden Standards und Normen unterstützt Ihre Software den Nutzer bei deren Einhaltung?
    A Risk Management Standard – IRM/Alarm/AIRMIC 2002
    AS/NZS 4360:2004
    COSO 2004 - Enterprise Risk Management - Integrated Framework
    DIIR Revisionsstandard Nr. 2
    DRS 20 - Deutscher Rechnungslegung Standard Nr. 20
    IDW PS 340
    IDW PS 525
    ISO 19600 - Compliance Management Systems
    ISO 31000:2009 – Risk Management Principles and Guidelines
    ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
    OCEG “Red Book” 2.0: 2009 - a Governance, Risk and Compliance Capability Model
    ONR 49000 ff. 2014
    Sonstiges
54. Können Unternehmensgrößen aus Jahresabschlüssen in Ihrer Software abgebildet werden?
55. Können in Ihrer Software Organisationsformen abgebildet werden?
56. Welche Organisationsformen können abgebildet werden?
    Funktionale Organisation
    Matrix Organisation

Sparten Organisation
Stablinien Organisation
Sonstiges

57. Welchen Elementen der Organisation können Risiken zugeordnet werden?
    Konzernstrukturen
    Abteilungen
    Stellen
    Arbeitsplätzen
    Personen
    Projekten
    Geschäftsprozessen
    Sonstiges
58. In welcher Notationssprache können Geschäftsprozesse in der Software abgebildet werden?
    EPK
    BPMN
    es ist nicht möglich Geschäftsprozesse abzubilden
    Sonstiges
59. Welche Kollektionsmethoden im Rahmen der Risikoidentifikation werden von Ihrer Software unterstützt?
    Checklisten
    SWOT-Analyse
    Risiko-Self-Assessment
    Risikoidentifikationsmatrix
    Dokumentation von qualitativen Erhebungen (z.B. Interviews, Brainstorming etc.)
60. Welche weiteren Kollektionsmethoden unterstützt Ihre Software?
61. Welche analytischen Suchmethoden werden im Rahmen der Risikoidentifikation von Ihrer Software unterstützt?
    Fehlermöglichkeits- und Einflussanalyse (FMEA)
    Morphologische Verfahren (Morphologischer Kasten)
    Fehlerbaumanalyse
    Fragenkataloge
62. Welche weiteren Suchmethoden unterstützt Ihre Software?
63. Welche Charakteristika können für ein neu angelegtes Risiko festgehalten werden?
    verbale Beschreibung
    Risikokategorie
    Risk Owner
    Verursacher
    Relevanz
    Frühwarnindikatoren
    Schwellwerte
    Auftrittsort (Konzern, Produkt, Prozess etc.)
    Wahrscheinlichkeit des Auftretens
    Zugrundeliegende Wahrscheinlichkeitsverteilung
    Ausmaß bei Risikoeintritt
    betroffene betriebswirtschaftliche Kennzahlen
    betroffene Variablen der Unternehmensplanung

Häufigkeit mit der das Risiko zu überwachen ist (z.B. in Tagen, Wochen oder Monaten)
Eskalationsstufen
Sonstiges

64. Bietet Ihre Software ein Risikoinventar?
65. Bietet Ihre Software vordefinierte Risikokategorien an?
66. Sind diese Risikokategorien individualisierbar?
67. Können Korrelationen zwischen einzelnen Risiken berücksichtigt werden?
68. Können die Auswirkungen von Risiken auf Unternehmensgrößen abgebildet werden?
69. Kann Ihre Software die aggregierte Auswirkung aller Risiken auf Unternehmensgrößen (wie z. B. den Gewinn) durch Simulation ermitteln?
70. Können Risiko-Ursache-Wirkungs-Ketten erfasst werden?
71. Welche Bewertungsmethoden werden von Ihrer Software unterstützt?
    Fehlermöglichkeits- und Einfluss-Analyse (FMEA)
    Fehlerbaumanalyse
    Nutzwertanalyse
    Drei-Werte-Verfahren (Sensitivitätsanalyse)
    Fuzzy-basierte Verfahren
    ABC Analyse
    Portfolioanalyse
    Risikomatrix
    Sonstiges
72. Welche weiteren Bewertungsmethoden unterstützt Ihre Software?
73. Welche Risikomaße werden zur Beschreibung von Risiken verwendet?
    Ausfallwahrscheinlichkeit (Probability of Default)
    Cash Flow at Risk
    Conditional Value at Risk (CVaR)
    Semivarianz
    Risikobedingter Eigenkapitalbedarf (RAC)
    Return on Risk Adjusted Capital (RORAC)
    Varianz bzw. Standardabweichung
    Value at Risk (VaR)
    Sonstiges
74. Welche Methoden und Verfahren stehen zur Berechnung der Risikomaße zur Verfügung?
    Delta-Normal-Methode (oder andere analytische Methoden)
    Monte Carlo Simulation
    historische Simulation (Berechnung mit Vergangenheitswerten)
    Auswertung historischer Daten
    Sonstiges
75. Können Eintrittswahrscheinlichkeit und Schadensausmaß auf Basis von Vergangenheitswerten ermittelt werden?
76. Können die Korrelationen der Risiken quantifiziert werden?
77. Wie können Eintrittswahrscheinlichkeit und Schadensausmaß eines Risikos eingetragen werden?
    qualitativ
    quantitativ

Sonstiges

78. Bietet Ihre Software die Möglichkeit Risiken zu priorisieren?
79. Welche Methoden & Verfahren zur Bestimmung des Gesamtrisikoumfangs werden von Ihrer Software angeboten?
    Monte Carlo Simulation
    Sonstiges
80. Welche Charakteristika von Steuerungsmaßnahmen können in Ihrer Software festgehalten werden?
    Betreffende Risiken
    Einfluss auf Risiken
    Einfluss auf betriebswirtschaftliche Kennzahlen
    Einfluss auf Unternehmensplanung
    Umsetzungsfrist
    Status
    Sonstiges
81. Welche Funktionen bietet Ihre Software zur Steuerung von Risiken?
    Anzeige Erfüllungsgrad / Fortschritt für Maßnahmen
    Aufgabenzuteilung
    Dokumentation getroffener Maßnahmen
    Dokumentation von Versicherungen oder anderer Risikoträger
    Verwaltung von Policen
    Vordefinierte Ursachen-/Maßnahmendatenbank mit Beispielen
    Zuordnung getroffener Maßnahmen
82. Bietet Ihre Software die Möglichkeit, Auswirkungen von Maßnahmen simulieren?
83. Nennen Sie Besonderheiten Ihrer Software in Bezug auf die Risikosteuerungsmöglichkeiten.
84. Bietet Ihre Software eine Erinnerungsfunktion an, welche z.B. vor ablaufenden Fristen warnt?
85. In welcher Form können Erinnerungen generiert werden?
    E-Mail Benachrichtigung
    Hinweis in der Benutzeroberfläche
86. Bietet Ihre Software eine Ampelfunktion an?
87. Für was bietet Ihre Software eine Ampelfunktion an?
    Risiken
    Unternehmensgrößen
    Sonstiges
88. Kann man eigene Schwellwerte für die Ampelfunktion konfigurieren?
89. Gibt es einstellbare Benachrichtigungen bei Über- oder Unterschreiten bestimmter Werte?
90. Kann ein Überwachungszyklus festgelegt werden, in dem Maßnahmen und Risiken neu geprüft werden sollen?
91. Bietet Ihre Software eine Übersicht über alle Risiken mit den dazu getroffenen Maßnahmen?
92. Bietet Ihre Software Abweichungsanalysen, um den Erfolg umgesetzter Maßnahmen zu überprüfen?
93. Ist es möglich, bei einer Überschreitung eines Termins oder Ähnlichem, direkt über die Software Kontakt zum Risk Owner oder Verantwortlichen herzustellen?

94. Werden Eskalationsstufen im Rahmen der Risikoüberwachung berücksichtigt?
95. Bietet Ihre Software ein individualisierbares Dashboard an?
96. Bietet Ihre Software die Möglichkeit, auf verschiedenen Hierarchiestufen unterschiedlich verdichtete Daten darzustellen?
97. Bietet Ihre Software die Möglichkeit einer Drilldown Darstellung von Risiken, Maßnahmen, Abteilungen etc?
98. Ist es möglich, Reports zu archivieren?
99. Besteht die Möglichkeit, archivierte Reports zu durchsuchen?
100. Unterstützt Ihre Software Ad-hoc Reports?
101. Unterstützt Ihre Software Heat Map Reports?
102. Bietet Ihre Software individuelle Reports für verschiedene Adressaten wie Vorstand, Geschäftsführung, Banken etc. an?
103. Bietet Ihre Software eine Risikomatrix-Darstellung für die Risikosituation?
104. Lässt sich diese Matrixdarstellung auch auf Abteilungs- und Prozessebene anwenden?
105. Bietet Ihre Software eine Zeitstrahldarstellung für Risiken und Maßnahmen an?
106. Nennen Sie bitte sonstige besondere Funktionen Ihrer Software, welche den Risikomanagementprozess unterstützen.
107. Hier werden Informationen zu Distribution, Preisen und Support erfragt.
108. Wie wird Ihre Software angeboten?
    Verkauf zeitlich unbegrenzter Nutzungsrechte bzw. Lizenzen
    Verkauf zeitlich begrenzter Nutzungsrechte bzw. Lizenzen
    Vermietung des Nutzungsrechts
    Open Source
    Sonstiges
109. Welches Lizenzmodell bieten Sie an?
    Concurrent-User Lizenzmodell
    Named-User Lizenzmodell
    Sonstiges
110. Wie viele Named User benutzen Ihre Software?
111. Wie viele Concurrent User benutzen Ihre Software?
112. Wer ist für die Bereitstellung, Wartung, und den Betrieb der IT Infrastruktur zuständig?
    Wir (der Anbieter) stellen die nötigen Server zur Verfügung
    Der Kunde benötigt einen eigenen Server
    Beides ist möglich. Der Kunde kann einen Server bei uns nutzen oder seinen eigenen.
    Eine dritte Firma ist dafür zuständig
113. Bitte nennen Sie die jährlichen Kosten, die durch Wartung oder Ähnlichem (zusätzlich zu der normalen Mietgebühr) anfallen können.
114. Bitte nennen Sie die Preisstaffelung Ihrer Vollversion (inklusive aller zusätzlichen Module und Leistungen)
115. Bitte nennen Sie die jährliche Miet-Preisstaffelung Ihrer Vollversion (inklusive aller zusätzlichen Module und Leistungen)
116. Bitte nennen Sie die Preisstaffelung Ihrer Vollversion bei zeitlich begrenzten Lizenzen. (inklusive aller zusätzlichen Module und Leistungen)

117. Welche Kosten entstehen dem Kunden für die Installation Ihrer Software (zusätzlich zum Erwerb der Lizenz oder Miete)?
118. Bieten Sie einen Installationsservice an?
119. Nennen Sie die Kosten für Ihren Installationsservice.
120. Wodurch können dem Kunden Kosten entstehen?
Installationsservice
Customizing
Upgrades
Updates
Betrieb
Schulung
Support
Sonstiges
121. Beschreiben Sie bitte kurz die Preisstruktur für das Customizing Ihrer Software.
122. Bitte geben Sie die Anzahl Ihrer Kunden im deutschsprachigen Raum an, die Ihr Risikomanagementinformationssystem einsetzen.
123. Bitte geben Sie die Anzahl Ihrer Kunden weltweit an, die Ihr Risikomanagementinformationssystem einsetzen (inkl. deutschsprachiger Raum).
124. Bieten Sie Schulungen an?
125. Welche Arten von Schulungen bieten Sie an?
technische Schulungen zum Umgang mit der Software
funktionale und inhaltliche Schulungen im Bereich des Risikomanagements
Einführungsschulungen
modulbezogene Weiterbildung
Sonstiges
126. Nennen Sie die Kosten für Schulungen gemäß Ihrer Preisstaffelung.
technische Schulung
funktionale Schulung
127. Müssen Updates zusätzlich gekauft werden oder sind diese im Preis inbegriffen?
Updates sind im Preis inbegriffen
Updates werden zusätzlich zum Kauf angeboten
128. In welchem Rhythmus werden Updates zu Ihrer Software veröffentlicht?
wöchentlich
monatlich
pro Quartal
halbjährlich
jährlich
Sonstiges
129. Werden zu älteren Versionen auch regelmäßig Updates veröffentlicht?
Nein
Ja, kostenfrei
Ja, kostenpflichtig
Sonstiges
130. Müssen Upgrades zusätzlich gekauft werden oder sind diese im Preis inbegriffen?

Upgrades sind im Preis inbegriffen
Upgrades werden zusätzlich zum Kauf angeboten

131. In welchem Rhythmus werden Upgrades zu Ihrer Software veröffentlicht?
wöchentlich
monatlich
pro Quartal
halbjährlich
jährlich
Sonstiges

132. Werden Upgrades auch für ältere Versionen angeboten?
Nein
Ja, kostenfrei
Ja, kostenpflichtig
Sonstiges

133. Bitte kreuzen Sie an, welche der folgenden Support-Möglichkeiten von Ihnen angeboten werden.
Online Hilfe
Online Chat
Druckbares Benutzerhandbuch
Video Tutorials
Telefon-Hotline
Sonstiges

134. Bitte nennen Sie die Zeiten, in denen ein telefonischer Support angeboten wird.

135. Wie viele Mitarbeiter sind im technischen Support tätig?

136. Wie viele Mitarbeiter sind in der funktionalen/inhaltlichen Beratung tätig?

137. Gilt der Support auch noch für ältere Softwareversionen?

138. Bitte nennen Sie Besonderheiten und weitere Aspekte Ihres Supports.

139. Welche Aspekte unterscheiden Ihre Software von anderen Systemen und Ihr Unternehmen von anderen Anbietern?

140. Bietet Ihre Firma weitere Produkte oder Dienstleistungen im Bereich Risikomanagement an?

141. Beschreiben Sie kurz, welche Dienstleistungen Ihr Unternehmen im Bereich des Risikomanagements anbietet.

142. Beschreiben Sie kurz, was für Produkte Ihr Unternehmen im Bereich des Risikomanagement zusätzlich zur Software anbietet.

143. Gerne möchten wir für die Veröffentlichungen der Studie (Print und Web) Ihr Logo in der Anbieterübersicht verwenden. Falls Sie uns die Nutzung Ihres Firmenlogos für diesen Zweck gestatten, laden Sie es bitte hier in einer hohen Qualität hoch.

144. Abschließend haben Sie hier die Möglichkeit Ihr Firmenprofil einzufügen.

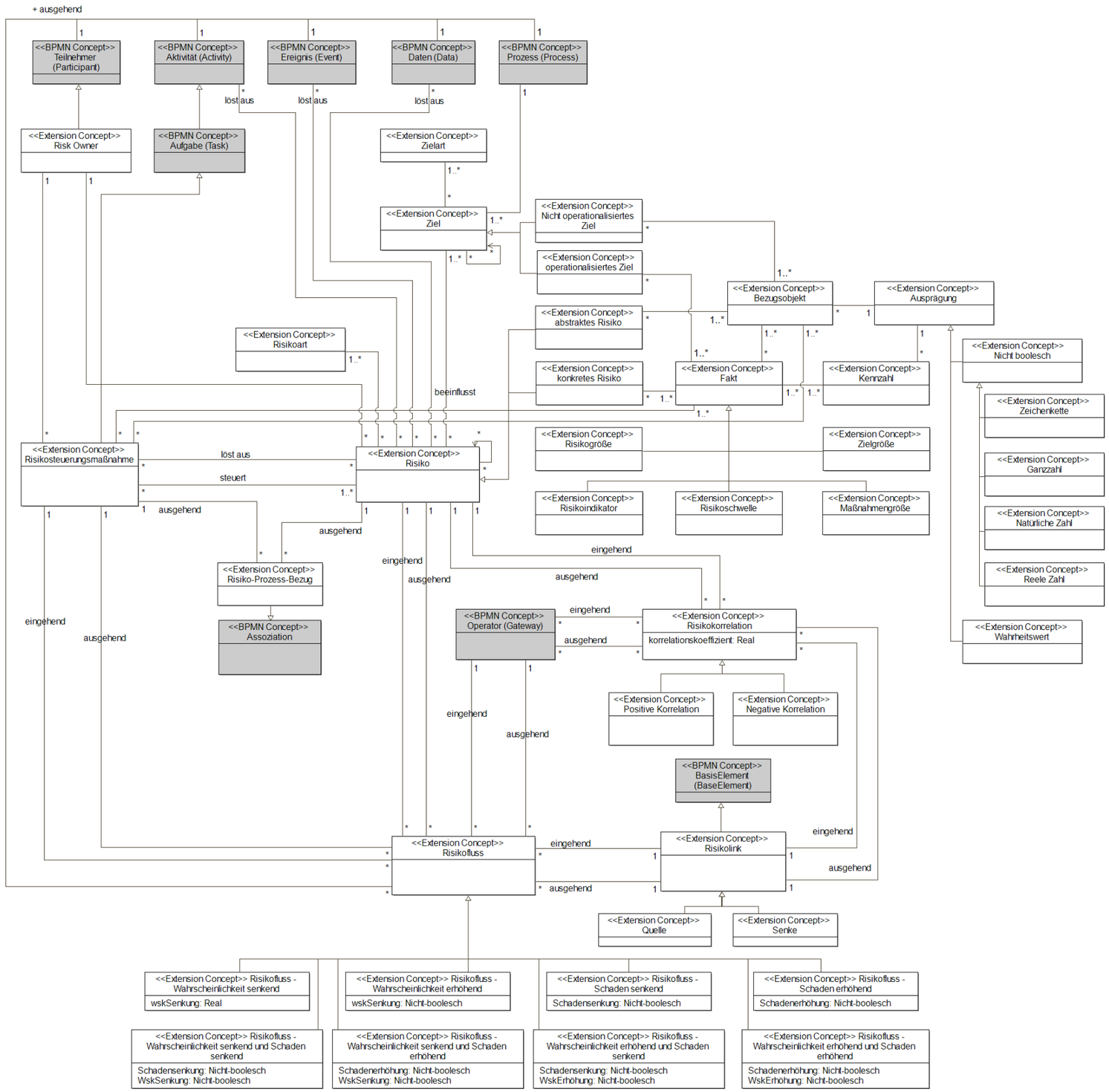


Abbildung 117: CDME Modell der BPMN Erweiterung

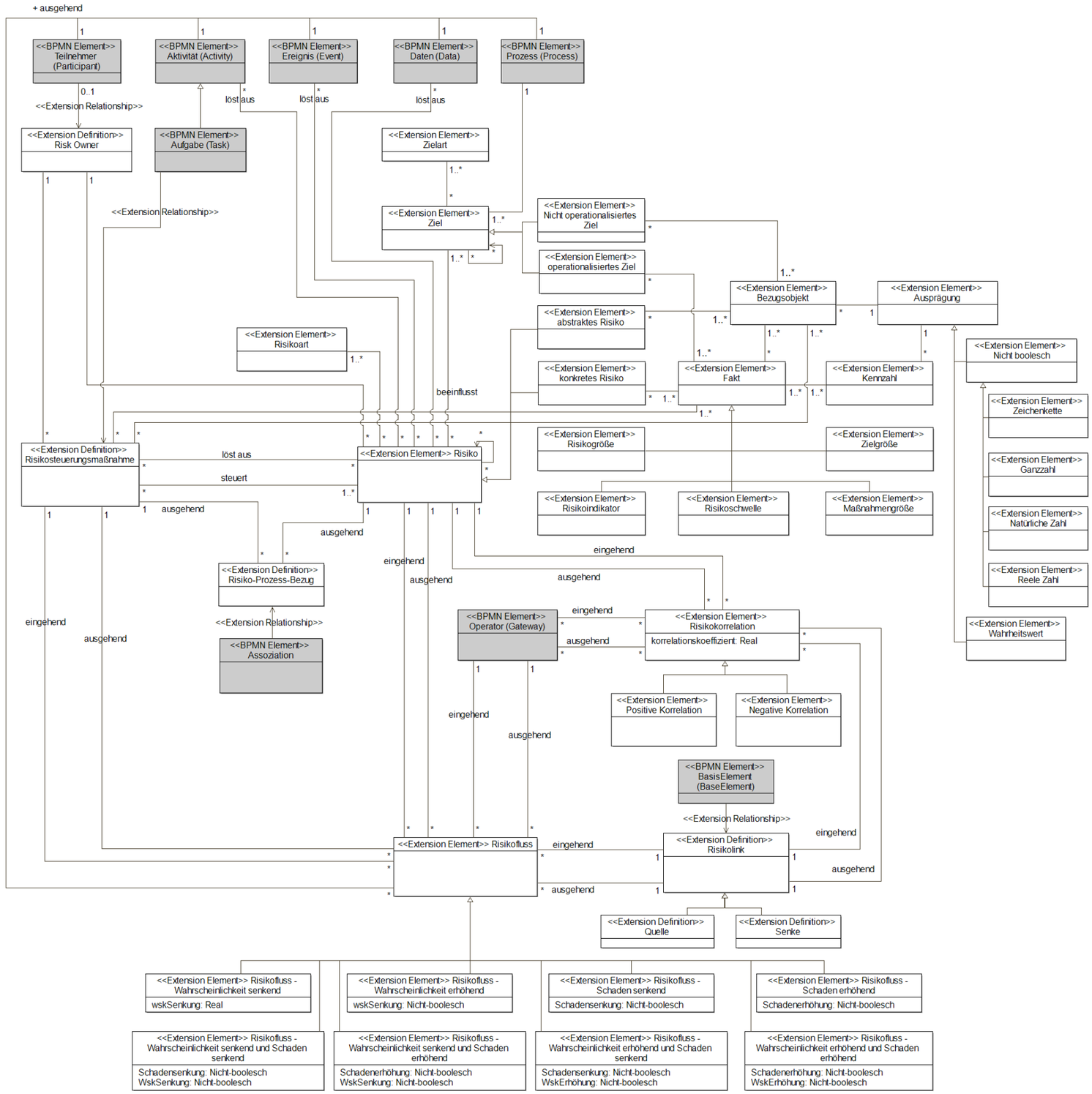
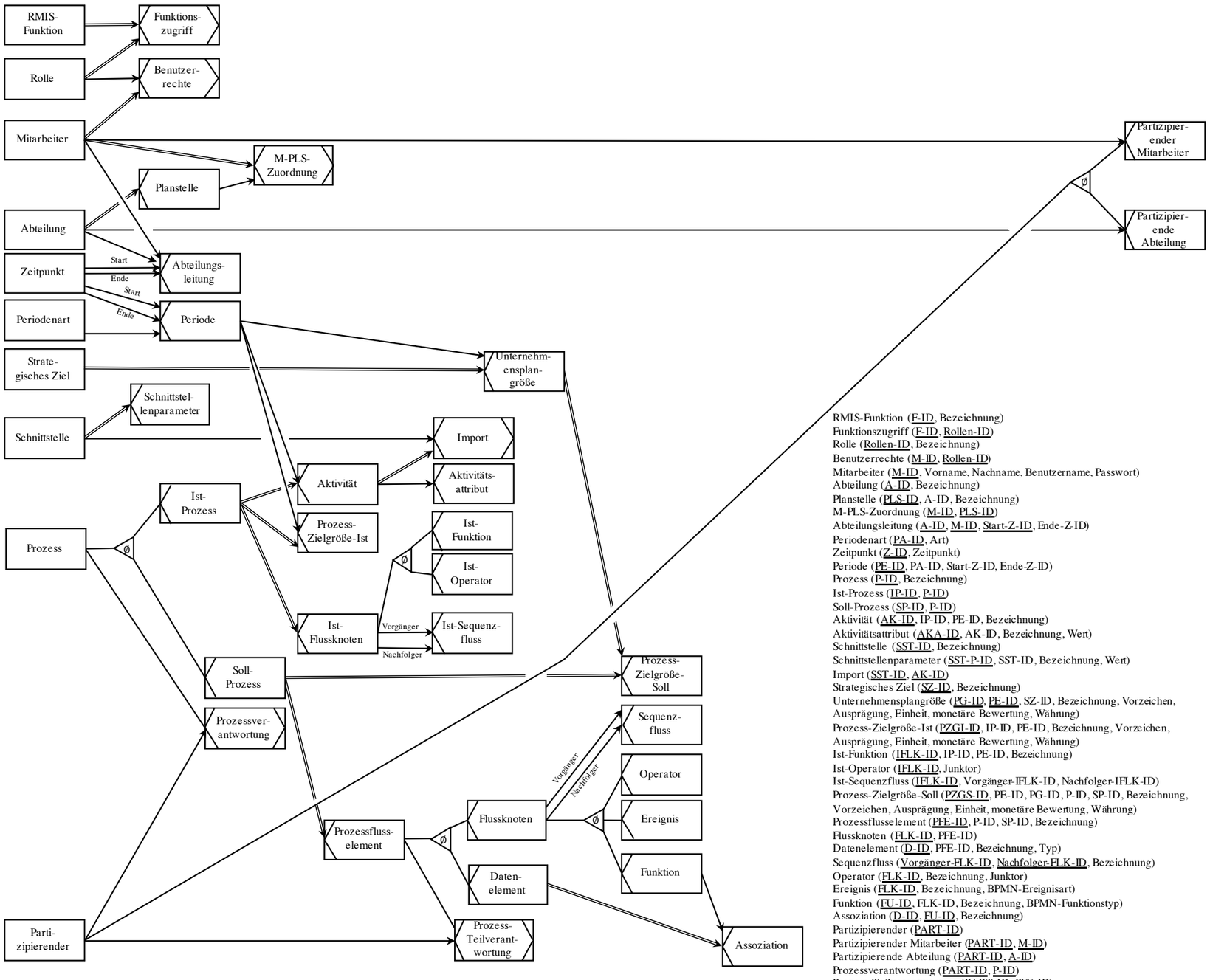
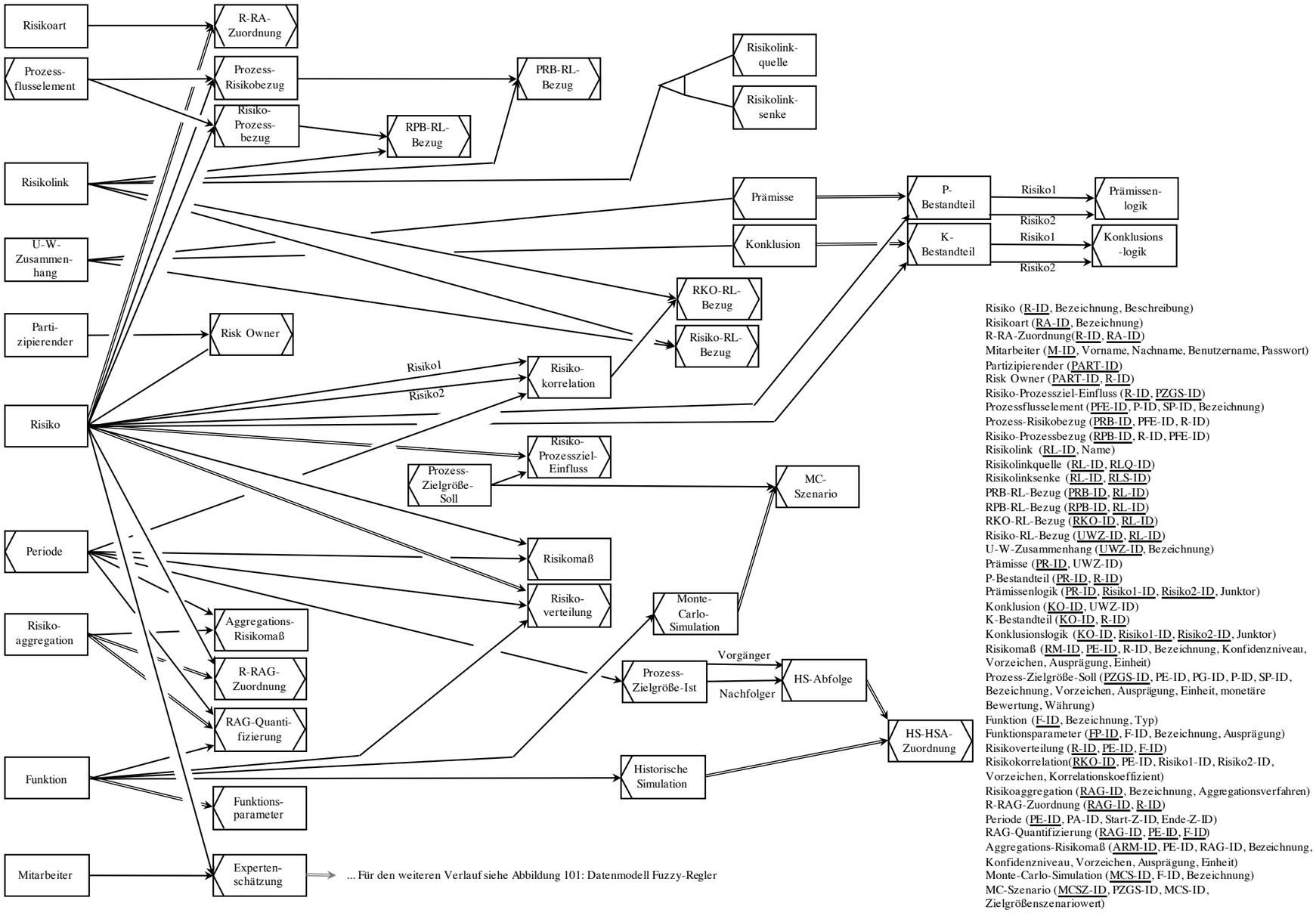


Abbildung 118: BPMN+X Modell der BPMN Erweiterung



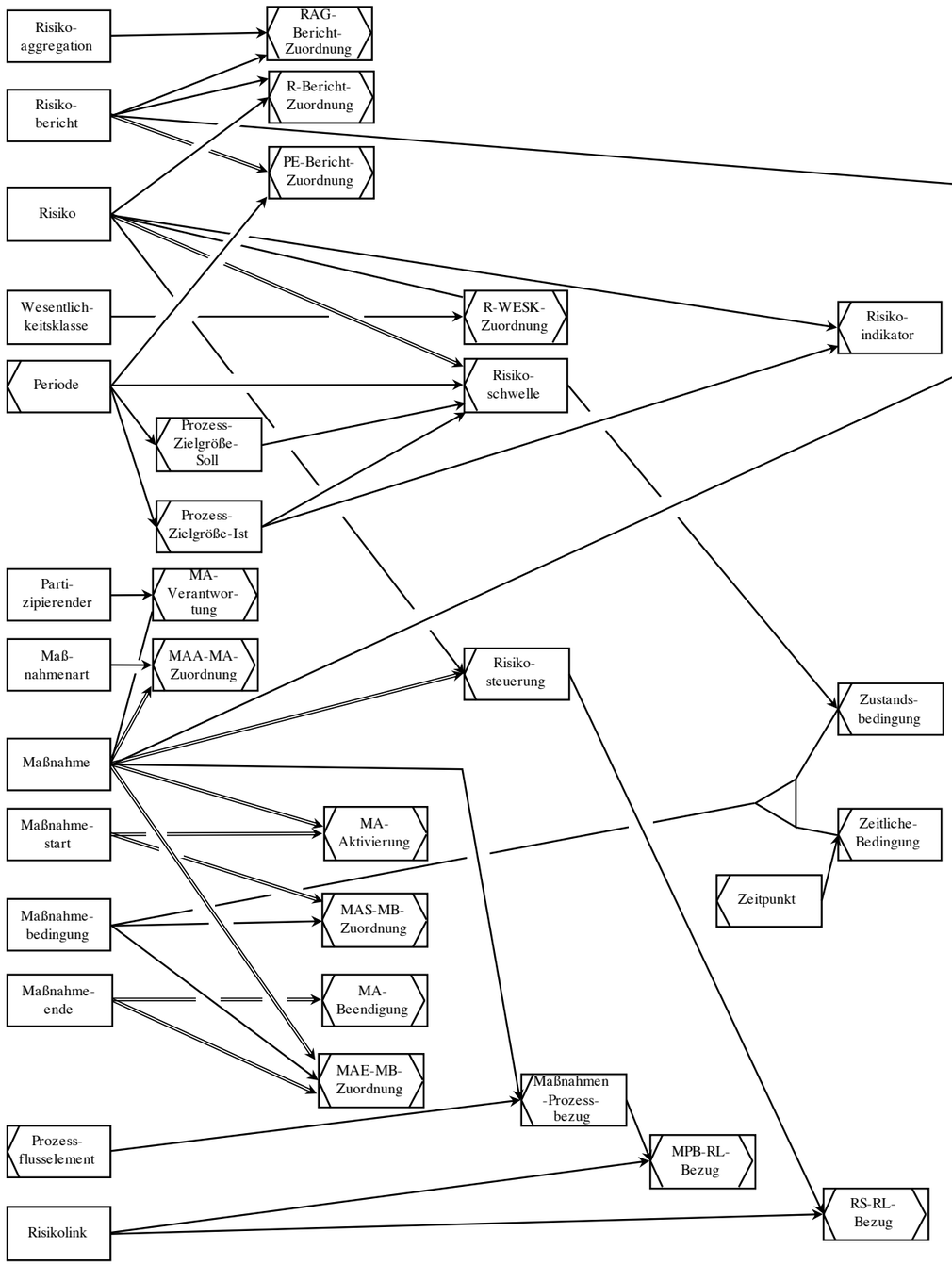
RMIS-Funktion (F-ID, Bezeichnung)
Funktionszugriff (F-ID, Rollen-ID)
Rolle (Rollen-ID, Bezeichnung)
Benutzerrechte (M-ID, Rollen-ID)
Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Abteilung (A-ID, Bezeichnung)
Planstelle (PLS-ID, A-ID, Bezeichnung)
M-PLS-Zuordnung (M-ID, PLS-ID)
Abteilungsleitung (A-ID, M-ID, Start-Z-ID, Ende-Z-ID)
Periodenart (PA-ID, Art)
Zeitpunkt (Z-ID, Zeitpunkt)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
Prozess (P-ID, Bezeichnung)
Ist-Prozess (IP-ID, P-ID)
Soll-Prozess (SP-ID, P-ID)
Aktivität (AK-ID, IP-ID, PE-ID, Bezeichnung)
Aktivitätsattribut (AKA-ID, AK-ID, Bezeichnung, Wert)
Schnittstelle (SST-ID, Bezeichnung)
Schnittstellenparameter (SST-P-ID, SST-ID, Bezeichnung, Wert)
Import (SST-ID, AK-ID)
Strategisches Ziel (SZ-ID, Bezeichnung)
Unternehmensplangröße (PG-ID, PE-ID, SZ-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Ist-Funktion (IFLK-ID, IP-ID, PE-ID, Bezeichnung)
Ist-Operator (IFLK-ID, Junktor)
Ist-Sequenzfluss (IFLK-ID, Vorgänger-IFLK-ID, Nachfolger-IFLK-ID)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozessflusselement (PFE-ID, P-ID, SP-ID, Bezeichnung)
Flussknoten (FLK-ID, PFE-ID)
Datenelement (D-ID, PFE-ID, Bezeichnung, Typ)
Sequenzfluss (Vorgänger-FLK-ID, Nachfolger-FLK-ID, Bezeichnung)
Operator (FLK-ID, Bezeichnung, Junktor)
Ereignis (FLK-ID, Bezeichnung, BPMN-Ereignisart)
Funktion (FU-ID, FLK-ID, Bezeichnung, BPMN-Funktionstyp)
Assoziation (D-ID, FU-ID, Bezeichnung)
Partizipierender (PART-ID)
Partizipierender Mitarbeiter (PART-ID, M-ID)
Partizipierende Abteilung (PART-ID, A-ID)
Prozessverantwortung (PART-ID, P-ID)
Prozess-Teilverantwortung (PART-ID, PFE-ID)

Abbildung 119: SERM Übersicht I



Risiko (R-ID, Bezeichnung, Beschreibung)
Risikoart (RA-ID, Bezeichnung)
R-RA-Zuordnung(R-ID, RA-ID)
Mitarbeiter (M-ID, Vorname, Nachname, Benutzername, Passwort)
Partizipierender (PART-ID)
Risk Owner (PART-ID, R-ID)
Risiko-Prozessziel-Einfluss (R-ID, PZGS-ID)
Prozessflusselement (PFE-ID, P-ID, SP-ID, Bezeichnung)
Prozess-Risikobezug (PRB-ID, PFE-ID, R-ID)
Risiko-Prozessbezug (RPB-ID, R-ID, PFE-ID)
Risikolink (RL-ID, Name)
Risikolinkquelle (RL-ID, RLQ-ID)
Risikolinksenke (RL-ID, RLS-ID)
PRB-RL-Bezug (PRB-ID, RL-ID)
RPB-RL-Bezug (RPB-ID, RL-ID)
RKO-RL-Bezug (RKO-ID, RL-ID)
Risiko-RL-Bezug (UWZ-ID, RL-ID)
U-W-Zusammenhang (UWZ-ID, Bezeichnung)
Prämisse (PR-ID, UWZ-ID)
P-Bestandteil (PR-ID, R-ID)
Prämissenlogik (PR-ID, Risiko1-ID, Risiko2-ID, Junktor)
Konklusion (KO-ID, UWZ-ID)
K-Bestandteil (KO-ID, R-ID)
Konklusionslogik (KO-ID, Risiko1-ID, Risiko2-ID, Junktor)
Risikomaß (RM-ID, PE-ID, R-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Funktion (F-ID, Bezeichnung, Typ)
Funktionsparameter (FP-ID, F-ID, Bezeichnung, Ausprägung)
Risikoverteilung (R-ID, PE-ID, F-ID)
Risikokorrelation(RKO-ID, PE-ID, Risiko1-ID, Risiko2-ID, Vorzeichen, Korrelationskoeffizient)
Risikoaggregation (RAG-ID, Bezeichnung, Aggregationsverfahren)
R-RAG-Zuordnung (RAG-ID, R-ID)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID)
RAG-Quantifizierung (RAG-ID, PE-ID, F-ID)
Aggregations-Risikomaß (ARM-ID, PE-ID, RAG-ID, Bezeichnung, Konfidenzniveau, Vorzeichen, Ausprägung, Einheit)
Monte-Carlo-Simulation (MCS-ID, F-ID, Bezeichnung)
MC-Szenario (MCSZ-ID, PZGS-ID, MCS-ID, Zielgrößenszenariowert)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Historische-Simulation (HS-ID, F-ID, Bezeichnung, Referenzwert)
HS-Abfolge (HSA-ID, Vorgänger-PZGI-ID, Nachfolger- PZGI-ID, relative-Änderung, absolute Änderung)
HS-HSA-Zuordnung (HS-ID, HSA-ID)
Expertenschätzung (ES-ID, M-ID, R-ID)

Abbildung 120: SERM Übersicht II



Risikoaggregation (RAG-ID, Bezeichnung, Aggregationsverfahren)
Risikobericht (RB-ID, Bezeichnung)
RAG-Bericht-Zuordnung (RB-ID, RAG-ID)
R-Bericht-Zuordnung (R-ID, RB-ID)
M-Bericht-Zuordnung (MA-ID, RB-ID)
PE-Bericht-Zuordnung (PE-ID, BE-ID)
Wesentlichkeitsklasse (WESK-ID, Bezeichnung)
Risiko (R-ID, Bezeichnung, Beschreibung)
R-WESK-Zuordnung (WESK-ID, R-ID)
Periode (PE-ID, PA-ID, Start-Z-ID, Ende-Z-ID, Bezeichnung)
Prozess-Zielgröße-Soll (PZGS-ID, PE-ID, PG-ID, P-ID, SP-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Prozess-Zielgröße-Ist (PZGI-ID, IP-ID, PE-ID, Bezeichnung, Vorzeichen, Ausprägung, Einheit, monetäre Bewertung, Währung)
Risikoschwelle (RS-ID, R-ID, PE-ID, PZGS-ID, PZGI-ID, Vergleichszeichen, Vorzeichen, Differenz-Schwellenwert)
Risikoindikator (RIN-ID, PZGI-ID, R-ID, PE-ID, Bezeichnung, Vergleichszeichen, Vorzeichen, Indikatorwert)
Partizipierender (PART-ID)
MA-Verantwortung (PART-ID, MA-ID)
Maßnahme (MA-ID, Bezeichnung, Kosten, Währung)
Maßnahmenart (MAA-ID, Bezeichnung, Beschreibung)
MAA-MA-Zuordnung (MAA-ID, MA-ID)
Risikosteuerung (RS-ID, MA-ID, R-ID, Vorzeichen, WSK-Wirkung, Ausmaßwirkung)
Maßnahmestart (MS-ID)
MA-Aktivierung (MA-ID, MS-ID)
Maßnahmeende (ME-ID)
MA-Beendigung (MA-ID, ME-ID)
MAE-MB-Zuordnung (ME-ID, MB-ID)
MAS-MB-Zuordnung (MS-ID, MB-ID)
Maßnahmebedingung (MB-ID, Bezeichnung)
Zustandsbedingung (MB-ID, RM-ID, Vergleichszeichen, Vorzeichen, Bedingungswert)
Zeitliche-Bedingung (MB-ID, Z-ID, Vergleichszeichen)
Zeitpunkt (Z-ID, Zeitpunkt)
Prozessflusselement (PFE-ID, P-ID, SP-ID, SL-ID, Bezeichnung)
Maßnahmen-Prozessbezug (MPB-ID, MA-ID, PFE-ID)
Risikolink (RL-ID, Name)
RS-RL-Bezug (RS-ID, RL-ID)
MPB-RL-Bezug (MPB-ID, RL-ID)

Abbildung 121: SERM Übersicht III