ERM-Maturity Assessement (ERMMA): Definition von ERM-Best-Practice-Reifegraden und deren Messung in Unternehmen

Walter S.A. Schwaiger[1] und Michael Brandstätter[1]
(unter Mitwirkung von Theresa Fröschl, Maximilian Irro)

[1] Institut für Managementwissenschaften, TU Wien,
Theresianumgasse 27, 1040 Wien, Österreich
walter.schwaiger@tuwien.ac.at

Wien, Januar 2019

Table of Contents

1 Einführung

Im unternehmensweiten Risikomanagement (Enterprise Risk Management, kurz: ERM) geht es B) um die Identifikation und Messung von verschiedenartigen Risiken im Unternehmenskontext sowie C) deren Steuerung in isolierten Managementsystemen (isolierte Steuerung) bzw. in traditionellen Managementsystemen (integrierte Steuerung), welche um den Aspekt des Risikos erweitertet werden. Diese Trennung basiert auf einer informationalen Perspektive, der zufolge zwischen der Generierung von Risikoinformationen (B) und dessen Verwendung (C) unterschieden wird. Um sicherzustellen, dass die jeweiligen Aktivitäten im Unternehmen nicht zufällig, sondern systematisch ablaufen, bedarf es eines übergeordneten „Master Minds" in Form einer ERM-Governance (A). Die buchstabenmäßige Kennzeichnung der drei ERM-Bestandteile soll anzeigen, dass die ERM-Governance (A) konzeptionell über dem Provider der Information (B) und dessen User (C) steht. Diese 3-teilige Grundstruktur des ERM-Systems wird im vorliegenden Beitrag von zentraler Bedeutung sein.

Im von der Funk Stiftung (Hamburg) geförderten Forschungsprojekt „Unternehmensweites Risikomanagement in österreichischen Unternehmen – Eine ERM-Reifegradanalyse" wurde am Institut für Managementwissenschaften der TU Wien ein Fragebogen zur Messung der Reifegrade von in Unternehmen der Nicht-Finanzdienstleistungsbranche implementierten ERM-Systemen entwickelt. Zur elektronisch gestützten Durchführung der Befragung wurde eine Online-Applikation des Fragebogens in moderner Informationstechnologie erstellt und nach Durchführung der Befragung wurden die Ergebnisse mit dem Software-Paket „R" statistisch ausgewertet.

Im Unterschied zu klassischen Befragungen, wobei allen teilnehmenden Unternehmen mehr oder minder ad hoc formulierte Fragen in gleicher Reihenfolge gestellt werden, weisen sich der im Projekt entwickelte Fragebogen und die durchgeführte Befragung insbesondere durch folgende Besonderheiten aus:

- Die im Fragebogen gestellten Fragen werden nicht ad hoc formuliert. Vielmehr werden die Fragen unter Verwendung des *Predictive Validity Framework (PVF)* (Bisbe, Batista-Foguet and Chenhall, 2007, pp. 812–814) deduktiv aus explizit über beobachtbare Indikatoren modellierten Konstrukten für die verschiedenen Ausgestaltungsformen von ERM-Systemen abgeleitet.
- Die im Fragebogen gestellten Fragen beziehen sich nicht auf unterschiedliche Grade von ERM-Implementierungen, welche anhand einer mehrteiligen (polytomen) Likert-Skala gemessen werden. Vielmehr wird mit den Fragen das Vorliegen der den 5 Reifegraden von ERM-System-Ausgestaltungen zugewiesenen Indikatoren anhand von zweiteiligen (dichotomen) Ja/Nein Antwortmöglichkeiten gemessen.
- Die Indikatoren der 5 Reifegrade von ERM-System-Ausgestaltungen repräsentieren durch ihre konsekutive Anordnung die progressiv zunehmenden Reifegradstufen eines Entwicklungsmodells (progressive levels in the maturity framework of Humphrey, 1988, p. 74). Dadurch werden nicht allen Unternehmen die gleichen Fragen gestellt. Vielmehr werden den Unternehmen nur solange Fragen gestellt, solange bei ihnen die für die konsekutiven Reifegrade geforderten Attribute vorliegen.
- Die teilnehmenden Unternehmen müssen nicht bis zur Auswertung der Studie warten, um Ergebnisse zu erhalten. Vielmehr werden den Unternehmen unmittelbar

nach Beendigung der Befragung die erreichten Reifegrade und die damit verbundenen Indikatoren sowie die für den nächsten Reifegrad noch fehlenden Indikatoren mitgeteilt.
- Die Befragung ist kein einmaliges, d.h. statisches Unterfangen. Vielmehr können die Unternehmen jährlich ihre aktuellen Reifegrade ermitteln, und somit die Entwicklung ihrer Reifegrade im Zeitablauf monitoren.

Die hinter diesen Besonderheiten stehende neuartige Online-Messmethodik zum Self Assessment von ERM-System-Reifegraden entstand nicht ad hoc. Vielmehr wurde sie gezielt konzipiert und implementiert, um die hinter dem Forschungsprojekt stehende Zielsetzung „**Konzeptionierung, Operationalisierung und IT-Implementierung eines Self Assessment-Tools sowie dessen Verwendung zur Messung der Reifegrade der in den Unternehmen eingerichteten ERM-Systeme, welche den teilnehmenden Unternehmen die Identifikation von Schwachstellen ermöglicht, Hinweise für Verbesserungen der Reifegrade gibt und das Monitoring der Reifegrade im Zeitablauf ermöglicht**“ zu erreichen. Zu diesem Zweck waren folgende Problem- bzw. Aufgabenstellungen zu bewältigen:

i. Konzeptionalisierung und Operationalisierung eines Entwicklungsmodells für die Reifegrade von ERM-Systemen
ii. Model Driven Development (MDD) einer web-basierten Online Software-Applikation
iii. Verfügbarmachung der Online-Applikation für die teilnehmenden Unternehmen auf einem Server der TU Wien
iv. Statistische Analyse der von den teilnehmenden Unternehmen gemessenen Reifegraddaten.

In diesem Artikel werden diese zur Zielerreichung zu bewältigenden Problem- bzw. Aufgabenstellungen des Forschungsprojekts, welches nachfolgend als *ERM-Maturity Assessments-(ERMMA)-Projekt* bezeichnet wird, und die damit verbundenen Beiträge präsentiert, u.z. der wissenschaftliche Beitrag (i.e. neuartiges Entwicklungsmodell zur Reifegradmessung), der praktische Beitrag (i.e. Online Tool zur Messung und zum Monitoring der Reifegrade) sowie empirische (i.e. statistische fundierte Einblicke in vorliegende Reifegrade und deren Ursachen) Beitrag. Der Artikel ist in vier Hauptkapitel gegliedert: Dem ERMMA-Messmodell sind zwei Kapitel gewidmet, u.z. zur Erörterung der theoretischen Grundlagen, der in der Literatur verfügbaren Ansätze zur (E)RM-Reifegradmessung und der Anforderungen (Kapitel 2) sowie der deduktiven Spezifikation von Best Practice-Reifegraden für progressive (konsekutive) ERM-System-Ausgestaltungen (Kapitel 3). In Kapitel 4 wird die ERMMA-Applikation, welche den teilnehmenden Unternehmen als *ERMMA-Monitoring Tool* zur Verfügung steht, vorgestellt, und im Kapitel 5 werden die ERMMA-Ergebnisse präsentiert und erörtert.

2 ERMMA-Messmodell: Grundlagen, Literatur-Review und Anforderungen

Das unternehmensweite Risikomanagement ist ein nicht direkt beobachtbares Konstrukt. In der von Bisbe et al. (2007) festgelegten Variante vom Predictive Validity Framework geht es um die zur Messung derartiger latenter Variablen zu verwendenden Modelle, und in Strukturgleichungsanalysen (Jöreskog and Sörbom, 1993) werden die erstellten Messmodelle in Strukturmodelle eingebunden, um multidirektionale Zusammenhänge zwischen den latenten und den direkt beobachtbaren, d.h. manifesten Variablen zu analysieren. Ein sehr einfaches, lineares Strukturgleichungsmodell in Form eines Regressionsmodells ist z.B., wenn statistisch untersucht wird, inwiefern die über ein Messmodell gemessenen Reifegrade von ERM-Ausgestaltungen (latente Variable) von der Unternehmensgröße (manifeste Variable) abhängt.

In der Sprache des Predictive Validity Frameworks, i.e. in der PVF-Sprache werden (nicht beobachtbare, d.h. latente) *Konstrukte* anhand von *Indikatoren* modellhaft *konzeptionalisiert* und anhand von *Indikatorvariablen operationalisiert* und dadurch *messbar* gemacht. Folglich galt es im ERMMA-Projekt bei der Spezifikation des ERM-Entwicklungsmodells ein Messproblem für das nicht beobachtbare ERM-Konstrukt zu lösen. Die dabei entwickelte Lösung wird als *ERM-Maturity Assessment-(ERMMA)-Messmodell* bezeichnet.

Die Einbeziehung der ERM-Entwicklungsperspektive machte zusätzlich notwendig, ein *progressiv gestuftes Messmodell* für die verschiedenen Reifegrade von ERM-System-Ausgestaltungen einzurichten. In einem progressiv gestuften Messmodell werden mit Zunahme der Reifegrade kumulativ zusätzliche Indikatoren einbezogen, sodass sich ein konsekutiver Anstieg der Reifegrade (Cumulative Stage Model) ergibt. „*Within existing maturity models a common design principle is to represent maturity as a number of cumulative stages where higher stages build on the requirements of lower stages with 5 representing high maturity and 1 low. This practice was made popular by the CMM and appears to have wide practical acceptance.*“ (de Bruin *et al.*, 2005, p. 4). Progressiv gestuften Messmodellen wohnt ein normativer Charakter inne, welcher sich in der Zur-Verfügungsstellung einer „Landkarte“ für gezielte Verbesserungen zeigt. „*A prescriptive model … indicates how to approach maturity improvement … i.e. enables the development of a road-map for improvement.*“ (de Bruin *et al.*, 2005, p. 2).

2.1 Vom Risikomanagement (ISO-RM) zum Enterprise Risk Management (COSO-ERM)

Im ISO-Risikomanagement-Standard (ISO-RM, 2011) wird ein *Risikomanagement-Prozess* definiert, welcher aus der Risikobeurteilung – mit den drei Bestandteilen in Form der Risikoidentifikation, der Risikoanalyse und der Risikobewertung – und der Risikobewältigung besteht. Aus organisationaler Perspektive zeigt sich diese Zweiteilung als problematisch. Denn eigentlich gehört die Risikobewertung gemeinsam mit der Risikobewältigung zur *Risikosteuerung*, welche die Steuerungsmaßnahmen

aufgrund der in der *Risikoidentifikation* und Risikoanalyse (*Risikomessung*) generierten Risikoinformationen selektiert und einsetzt. Weiters suggeriert die im Standard skizzierte Risikobewältigung, dass diese von traditionellen Managementsystemen, d.h. Planungs- und Kontrollsystemen losgelöst ist und vom Risikoeigner (Risk Owner) in einem sich auf das jeweilige Risiko beziehenden (Risiko-)Managementsystem erfolgt. Dabei wird in Abhängigkeit von den quantitativen Eigenschaften des Risikos dieses entweder vermindert, beseitigt, vermieden oder verringert (ISO-RM, 2011, p. 14). Zugleich wird aber im *Grundsatz b)* gefordert, dass Risikomanagement Bestandteil aller Organisationsprozesse ist: „*Risikomanagement ist keine selbständige Tätigkeit, welche von den Hauptaktivitäten und Kernprozessen der Organisation losgelöst ist. Es ist Bestandteil der Verantwortung der obersten Leitung und ein integrierter Teil aller Organisationsprozesse, einschließlich der strategischen Planung und aller Projekte und Veränderungsprozesse.*“ (ISO-RM, 2011, p. 15).

Das Problem lässt sich einfach lösen, wenn die Risikosteuerung (Verwendung von Risikoinformationen) sich nicht nur auf isolierte Risiko-Managementsysteme beschränkt, sondern auch die bereits in den Unternehmen eingesetzten (traditionellen) Planungs- und Steuerungssysteme, welche um den Aspekt des Risikos zu risikobasierten Systemen erweitert werden, umfasst. Dies entspricht auch der Intention des ISO-Standards und es lässt sich einfach konzipieren, indem das im ISO-Standard definierte Risikomanagement um das Konzept der *risikobasierten Planung und Steuerungssysteme* ergänzt wird, sodass die verschiedensten Möglichkeiten zur Risikosteuerung inkludiert sind. Mit dieser Erweiterung ergibt sich die in Abbildung 1 dargestellte 3-dimensionale Grundstruktur von ERM-Systemen, welche als *ISO/COSO-ERM-System-Modell* bezeichnet wird, mit den Dimensionen A) ERM-Governance, B) Risiko-Managementsystem und C) Risiko-basierte Planung und Steuerungssysteme.

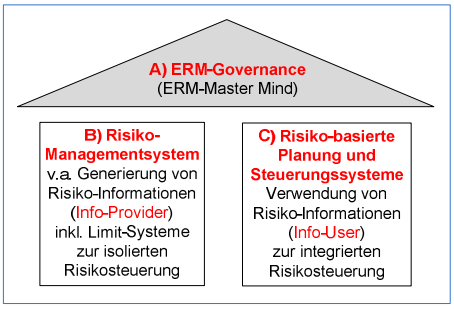

ABBILDUNG 1: ISO/COSO-ERM-SYSTEM-MODELL – 3-DIMENSIONALE GRUNDSTRUKTUR

In dieser Grundstruktur zeigt sich der ISO-Konnex insofern, als dass sich das Risiko-Managementsystem (linke Säule in Abbildung 1) weitestgehend mit dem ISO-Verständnis vom Risikomanagement-Prozess deckt. Folglich bezieht es neben der Generierung von Risikoinformationen auch die isolierte Steuerung einzelner Risiken seitens operativ tätiger Risikoeigner ein. Die rechte Säule des ERM-Systems steht für die risikobasierte(n) Planung und Steuerungssysteme, wobei die Risikosteuerung durch bereichsverantwortliche Manager als Risikoeigner erfolgt, indem die im Risikomanagement-Prozess generierten Risikoinformationen in die von ihnen zu verantwortenden

Managementsysteme integriert werden. Diese Säule sowie das auf die beiden Säulen gesetzte „Dach“ in Form der ERM-Governance stellt den Konnex zum COSO-ERM-Framework (COSO-ERM, 2017) her, welches die diesbezüglichen Spezifikationen enthält, u.z.:

1) Die Risikobasiertheit der Planung und Steuerungssysteme (rechte Säule) zeigt sich in der expliziten Formulierung der gemeinsamen Betrachtung von Wertschöpfung (Performance) und Risiko. Das dem COSO-ERM zugrundeliegende „Performance/Risiko-Postulat“ (*Risk Profile*) wird im mit *Risk Profil Illustrations* titulierten Anhang C) des Frameworks ausführlich erläutert.
2) Die *Risk Governance and Culture* (Master Mind/Dach) stellt im COSO-ERM-Framework eine eigenständige Komponente dar: „*Risk Governance and Culture together form a basis for all other components of enterprise risk management. Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.*“ (COSO-ERM, 2017, p. 27).
3) Weiters ist der explizit formulierte Unternehmenskontext bereits in der ERM-Definition enthalten: „*The culture, capabilities and practices, integrated with strategy-setting and its execution that organizations rely on to manage risk in creating, preseverving, and realizing value.*“ (COSO-ERM, 2017, p. 10).
4) Schließlich werden im Anhang B) des Frameworks auch noch organisationale Aspekte des Risikomanagements erörtert, welche inhaltlich stark an das *3-Lines of Defense-Modell* vom Institute of Internal Auditors (IIA-3LoD, 2013) angelehnt ist, allerdings ohne auf den Konnex hinzuweisen.

Die auf dem ISO-RM-Standard und dem COSO-ERM-Framework aufbauende 3-dimensionale Grundstruktur des ISO/COSO-ERM-System-Modells (siehe Abbildung 1) bildete im ERMMA-Projekt das Grundkonzept, auf welchem das ERMMA-Reifegrad-Modell aufgesetzt wurde. Zur Identifikation von Indikatoren für die hinter den verschiedenen Reifegraden stehenden ERM-System-Ausgestaltungen wurde die einschlägige ERM-Fachliteratur analysiert.

2.2 Literatur-Review: Reifegradmodelle für (unternehmensweites) Risikomanagement

Durch die große Bedeutung des Capability Maturity Models (CMM) beginnt die Darstellung der Literatur-Recherche-Ergebnisse mit diesem Modell sowie dessen Weiterentwicklung zum Capability Maturity Model Integration (CMMI). Anschließend wird auf dessen Übertragung in den Risikomanagement-Kontext eingegangen, und es werden weitere Reifegradmodelle zum Risikomanagement erörtert.

Das *Capability Maturity Modell (CMM)*, welches auf dem *Maturity Model* von Humphrey (1988) basiert, bezieht sich auf Prozesse im Bereich der Software-Entwicklung. Im CMM-Modell sind fünf konsekutive (kumulative) Reifegrade definiert, u.z. 1) Initial (Prozesse sind nur vereinzelt oder überhaupt nicht definiert), 2) Repeatable (Prozesse unterliegen einem einfachen Monitoring), 3) Defined (Prozesse sind

unternehmensweit definiert), 4) Managed (Prozesse werden mit quantitativen Kennzahlen gesteuert) und 5) Optimizing (Prozesse unterliegen einem kontinuierlichem Verbesserungsprozess). Die 5 Reifegrade sind inhaltlich mit Indikatoren belegt, welche im Wesentlichen anhand von dichotomem Variablen, d.h. mit Ja/Nein zu beantwortenden Fragen gemessen werden (Zubrow *et al.*, 1994).

Das *Capability Maturity Modell Integrated (CMMI)* generalisiert das CMM-Modell und erweitert somit dessen Anwendungsbereich auf viele Einsatzgebiete. In der aktuellen Version (CMMI, 2010) unterscheidet das CMMI zwischen zwei Ansätzen der Prozessverbesserung, u.z. der Continuous Representation, welche Capability Levels misst und sich auf die Verbesserung einzelner Prozesse in ausgewählten Bereichen (Process Area) bezieht, und der Stage Representation, welche Maturity Levels misst und sich auf die Verbesserung ähnlicher Prozesse in mehreren Bereichen bezieht. In der in der Praxis häufiger zur Anwendung kommenden Stage Representation sind fünf konsekutive (kumulative) Reifegrade definiert, u.z. 1) Initial (Definitionen liegen nur vereinzelt oder überhaupt nicht vor) , 2) Managed (Prinzipien des Projektmanagements kommen zur Anwendung), 3) Defined (der Fokus wechselt von der Einzelbetrachtung zur Betrachtung der gesamten Organisation), 4) Quantitatively Managed (Verwendung von Mess- und Benchmark-Systemen zur gezielten Steuerung), 5) Optimizing (Vorliegen eines kontinuierlichen Verbesserungsprozesses). Die konsekutive (kumulative) Anordnung der Reifegrade erfordert, dass zur Erreichung höherer Stufen stets alle dafür geforderten Indikatoren (Goal) erfüllt sein müssen. „*To reach a particular level, an organization must satisfy all of the goals of the process area or set of process areas that are targeted for improvement, regardless of whether it is a capability or a maturity level.*" (CMMI, 2010, p. 22). Im Unterschied zum CMM-Modell werden zur Operationalisierung der Reifegradindikatoren nicht mehr dichotome Variablen verwendet. Stattdessen werden polytome Variablen in Form einer 10-stufigen CMMI-Questionnaire-Skala verwendet (Blanchette and Keeler, 2005, p. 7).

Das Risk Maturity Model von Hillson (1997) bezieht sich explizit auf das CMM-Modell: „*Each level is clearly characterized and defined, enabling organizations to assess themselves against an agreed scale. Having discovered its CMM level, an organisation can then set clear targets for improvement, aiming towards the next level of capability and maturity.*" (Hillson, 1997, p. 36). Hillson adaptiert das CMM-Modell für den Kontext der Risiko(-Management)-Implementierung, indem er für jede seiner vier Dimensionen, i.e. Kultur, Prozess, Erfahrung und Applikation die vier Reifegrade, i.e. naïve, novice, normalized und natural anhand von Indikatoren spezifiziert. Hillson bleibt auf der konzeptionalen Ebene, zumal er den Indikatoren der 16 Dimension/Reifegrad-Konstrukte keine operationalen Variablen (Indikatorvariablen) zuweist.

Beasely et al. (2005) definieren ein n-dimensional/5-stufiges Reifegradmodell für die ERM-Implementierung, wobei die 5 Implementierungsstufen definiert sind von „*(1) no plans exist to implement ERM*" bis „*(5) complete ERM is in place*". Im Unterschied zu Hillson sind die Dimensionalität des Modells und die Indikatoren des ERM-Systems nicht präzise definiert. Das ERM-System wird in Anlehnung an das COSO-ERM-Rahmenwerk von 2004 vage definiert, sodass dessen Interpretation den Befragungsteilnehmern überlassen bleibt.

Monda/Giorgino (2013) verbessern die Messung der ERM-Implementierungsgrade durch die Spezifikation eines 3-dimensional/kontinuierlichen Reifegradmodell für die ERM-Implementierung anhand von Best Practice-Ansätzen in den 3 Dimensionen, u.z. Risikokultur, Organisation und Prozess. Anstatt einer diskreten Skala messen sie die Qualitäten der ERM-Implementierungen anhand des kontinuierlichen ERM-Index (ERMi). Für die Spezifikation ihres 3-dimensionale Reifegradmodells und der Kalibrierung der Modellparameter führen sie eine Delphi-Studie durch. Die Implementierungsgrade werden von den Befragungsteilnehmern anhand von 2- bis 4-teiligen Anwortskalen bestimmt. Zur Aggregation werden die Antworten mit den in der Delphi-Studie erhobenen Gewichtungen für die verschiedenen Antwortmöglichkeiten multipliziert und anschließend die sich ergebenden Produkte summiert.

Cienfuegos (2013) entwickelt ein 5-dimensional/5-stufiges Reifegradmodell für die Implementierung von Risikoüberlegungen in der Gemeindeverwaltung. Dabei nimmt er explizit Bezug auf die in der Organisationswissenschaft verwendeten Stufenmodelle (Damsgaard and Scheepers, 1999; Stubbart and Smalley, 1999). Überraschend ist aber, dass er das Stufenmodell zur Definition der 5 Stufen des Risikomanagementprozesses verwendet, u.z. context and objectives, identification, analysis and measurement, decision or control sowie implementation, review and feedback. Die 5 Reifegrade werden anhand des CMM-Modells definiert, u.z. initial, repeatable, defined, managed und optimized. Die Ausprägungen der Implementierungsgrade werden in der Befragung anhand einer 5-teiligen Antwortskala gemessen.

Lundqvist (2015) entwickelt ein 2-dimensional/4-stufiges Reifegradmodell für ERM-Implementierungen, wobei das ERM-System anhand von 2 latenten Dimensionen (Komponenten) definiert wird, u.z. dem traditionellen Risikomanagement und der Risk Governance. Die 4 Implementierungsgrade reichen von 0 bis 3, d.h. von „*non-existent*“ bis „*robustly implemented*“. Zur Analyse der Bestimmungsfaktoren setzt sie die erklärende Faktoranalyse ein, wobei sie die sich aus der Analyse ergebenden Faktorladungen mit exogenen („environmental/contingent“) Variablen (z.B. Größe des Unternehmens) in eine kausale Beziehungen bringt und die statistische Signifikanz der Beziehungen testet.

Vanini (2016) verweist aus das von Hillson (1997) entwickelte Reifegradmodell für das Risikomanagement und konzipiert in Anlehnung an das CMMI-Reifegradmodell ein 5-dimensional/5-stufiges Messmodell hinsichtlich der Reifegrade der Integration von Risikomanagement und Controlling. *Das „Risk Management Integration Maturiy Model (RiskMIMM)“ basiert auf einem Selbstanalysefragebogen des Arbeitskreises „Risikomanagement und Controlling“ der Risk Management Association e.V. (RMA) und des Internationalen Controllervereins e.V. (ICV)*, welches den Prozess der Integration anhand der 5 Dimensionen organisiert, u.z. Strategie/Steuerung, Instrumente, Organisation/Prozesse, Personal und Technik/IT. (2016, S. 172). Im Beitrag wird auch auf Ergebnisse eingegangen, welche in einer unter den Mitgliedern der RMA gemeinsam mit Leschenko durchgeführten Befragung erzielt wurden. Durch die Verwendung von Fragen als Ausgangspunkt hat das RiskMIMM allerdings keine explizit formulierten Indikatoren für die Reifegrade.

Gleißner (2016) bezieht sich auf Vanini und stellt ein 6-stufiges Reifegradmodell als Ergänzung vor, *das insgesamt die Risikomanagementfähigkeit eines Unternehmens*

betrachtet, speziell im Hinblick auf (1) Erfüllung gesetzlicher Anforderungen und (2) erreichter ökonomischer Nutzen. (2016, S. 31). Dieses Reifegradmodell ist für Selbsttests konzipiert, und es ordnet die Reifegrade nach 1) kein Risikomanagement, 2) Schadensmanagement, 3) regulatorisches Risikomanagement, 4) ökonomisches Risikomanagement (entscheidungsunterstützend), 5) integriertes wertorientiertes Risikomanagement und 6) embedded Risikomanagement (holistisch). Bei der „Risikomanagementfähigkeit" in der höchsten Reifegradstufe handelt es sich somit um eine risikoorientierte (2015) bzw. finanzwirtschaftlich basierte Unternehmenssteuerung (2001), wobei Risikoüberlegungen zentraler Bestandteil aller Entscheidungssysteme, d.h. Planungs- und Steuerungssysteme des Unternehmens sind. Für die Durchführung des Selbsttests sind Fragen zur Messung der Reifegrade formuliert. Wie im Risk-MIMM-Modell werden aber die hinter den Fragen stehenden Indikatoren nicht explizit spezifiziert.

Die ERM-Literatur-Recherche wurde durchgeführt, um Anregungen hinsichtlich der Indikatoren für die hinter den verschiedenen Reifegraden stehenden ERM-System-Ausgestaltungen zu erhalten. Die verschiedenen Modellierungen zeigten eine breite Palette an möglichen Ansätzen und Vorgehensweisen. Für den Zweck der ERM-System-Ausgestaltungen erweist sich das am CMM-Modell angelehnte 4-dimensional/4-stufige Risk Maturity Model (RMM-Modell) von Hillson als am Aufschlussreichsten. Die 4 Dimensionen sowie 4 Reifegrade des Modells kennzeichnen ein 4-dimensional/4-stufiges Konstrukt, welches aus 16 Dimension/Reifegrad-Konstrukten besteht. Durch die progressive Spezifikation der Indikatoren über die Reifegrade ist das RMM-Modell ein Entwicklungsmodell, welches normative Anhaltspunkte zur Verbesserung der Reifegrade gibt.

2.3 ERM-Entwicklungsmodell: Mehrdim./Mehrstufiges Messmodell – Anforderungen

Das RMM-Modell von Hillson erfüllt die Zielsetzung des ERMMA-Projekts hinsichtlich des angestrebten Entwicklungsmodells. Die zur Erstellung des Modells gewählte Vorgehensweise ist intuitiv aber fachlich wenig fundiert. Zur Beseitigung dieses Versäumnisses wurde im ERMMA-Projekt ein wissenschaftlicherer Ansatz gewählt, indem in Anlehnung an die Methodik des Predictive Validity Frameworks das Messmodell erstellt wurde. In der *PVF-Methodik* (Bisbe, Batista-Foguet and Chenhall, 2007, pp. 790–791) wird zwischen der konzeptionalen und der operationalen Betrachtung des Messmodells unterschieden. Auf der konzeptionalen Ebene geht es insbesondere um die *Kontextualisierung*, die *Dimensionierung* und die *Charakterisierung* des zu messenden Konstrukts sowie die *Konzeptionalisierung* (inkl. Validierung) des Messmodells, wohingegen es auf der operationalen Ebene um die *Operationalisierung* (inkl. Validierung) des konzeptionalisierten Messmodells geht. Nachfolgend werden die an ERM-Entwicklungsmodelle zu stellenden Anforderungen und deren Umsetzung im ERMMA-Projekt anhand der auf der konzeptionalen und operationalen Ebene anfallenden Agenden erörtert.

Ad Kontextualisierung des zu messenden Konstrukts) Der Kontext des zu messenden Konstrukts ergibt sich aus der Zielsetzung des ERMMA-Projekts, u.z. ein ERM-

Entwicklungsmodell für die Reifegrade von ERM-System-Ausgestaltungen zu erstellen. Inhaltlich geht es dabei um eine differenzierte Betrachtung von ERM-Systemen, wozu das ISO/COSO-ERM-System-Modell einen guten Ausgangspunkt darstellt. Sowohl im Prüfungsstandard der Wirtschaftprüfer (IDW-PS981, 2017) als auch im Revisionsstandard der Internen Revision (DIIR-RS2, 2015) wird auf das COSO-ERM-Framework Bezug genommen. „*Die durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden Corporate Governance Systeme – Internes Kontrollsystem (IKS), Risikomanagementsystem (RMS), Internes Revisionssystem (IRS) und Compliance Management System (CMS) – sind weder im Gesetz noch in der Literatur eindeutig definiert. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme lehnt sich dieser IDW Prüfungsstandard an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement an.*“ (IDW-PS981, 2017, p. 3). Dadurch haben das COSO-ERM-Framework und das diesbezüglich definierte ISO/COSO-ERM-Modell auch eine große praktische Bedeutung. Die praktische Relevanz wiederum macht das ISO/COSO-ERM-System-Modell zu einem *Best Practice-Modell*.

Beim am ISO/COSO-ERM-System-Modell ausgerichteten ERM-Entwicklungsmodell geht es um die Bestimmung (Assessment) von Reifegrade (Maturity), weshalb das damit einhergehende Konstrukt als *ERMMA-Konstrukt* bezeichnet wird. Neben der inhaltlichen Abgrenzung (Festlegung der Domäne) wird bei der Kontextualisierung auch noch die Intention des zu messenden Konstrukts festgelegt. Die Intention des Messmodells (Doty and Glick, 1994) bestimmt dessen Verwendung als Klassifikations- oder Typifizierungsschema. Bei der Klassifikation geht es vornehmlich um bestmögliche Zuordnungen zu klar unterschiedenen Gruppierungen, während bei der Typifizierung zweckorientierte Überlegungen (z.B. hinsichtlich der Performance) im Vordergrund stehen. Beim ERM-Entwicklungsmodell (Konstrukt) ist die Generierung von konkreten *Zuordnungsregeln* vordergründig, womit klar ist, dass es im ERMMA-Projekt um die Etablierung eines *Klassifikationsschemas* geht.

Ad Dimensionierung des zu messenden Konstrukts) Zur Konkretisierung der Zielsetzung des ERMMA-Projekts, u.z. ein ERM-Entwicklungsmodell für die Reifegrade von ERM-System-Ausgestaltungen zu entwickeln, wird das 3-dimensionale ISO/COSO-ERM-System-Modell für die Definition des ERM-Systems und das 5-stufige CMM-/CMMI-Reifegrad-Modell für die Definition der Reifegrade verwendet. Durch die Einbeziehung des ERM-System-Modells ergibt sich ein *mehrdimensionales Konstrukt* (Giere, Wirtz and Schilke, 2006), und die zusätzliche Einbeziehung des Reifegradmodells etabliert ein *mehrdimensional/mehrstufiges Konstrukt*. Konkret ergibt sich ein *3-dimensional/5-stufiges ERMMA-Konstrukt* für das ISO/COSO-ERM-basierte ERM-Entwicklungsmodell.

Die Mehrdimensionalität des Konstrukts geht mit einer *konzeptionalen Abstraktion* einher, wobei das 3-dimensionale ERM-System auf einer höheren Abstraktionsebene als die 3 sie formierenden Dimensionen steht. Werden die 3 Dimensionen jeweils anhand von Indikatoren konzeptionalisiert, dann entspricht dies einer Abstraktion 1. Ordnung und die 3 Dimensionen sind Konstrukte 1. Ordnung. Der Übergang von den 3 Dimensionen auf das ERM-System entspricht einer Abstraktion 2. Ordnung und das ERM-System ist ein Konstrukt 2. Ordnung.

Die Mehrstufigkeit des Konstrukts geht mit einer zusätzlichen *konzeptionalen Differenzierung* einher, wobei das 3-dimensional/5-stufige ERMMA-Konstrukt nicht mehr nur aus 3 Dimensionskonstrukten, sondern aus 15 Dimension/Reifegrad-Konstrukten gebildet wird. Die bei der Mehrdimensionalität angesprochene Abstraktion bleibt erhalten. Sie bezieht sich nunmehr anstatt auf die 3 Dimensionskonstrukte auf die 15 Dimension/Reifegrad-Konstrukte.

Durch die Dimensionierung des ERMMA-Konstrukts und der mit dem Konstrukt intendierten Klassifikation, welche in der Konstrukt-Kontextualisierung festgelegt wurde, ist numehr auch der *ERMMA-Klassifikationsrahmen* in Form einer 3x5-Matrix festgelegt.

Ad Charakterisierung des zu messenden Konstrukts) Durch die Unbeobachtbarkeit des 3-dimensional/5-stufigen ERMMA-Konstrukts gilt es dessen 15 Dimension/Reifegrad-Konstrukte jeweils mit beobachtbaren Indikatoren zu belegen. Durch die Einbeziehung der Indikatoren gesellt sich nun eine dritte Entität zu den beiden schon vorhandenen Entitäten, u.z. dem Konstrukt und den Dimensionen. Das mehrdimensional/mehrstufige Konstrukt wird charakterisiert (typisiert), indem die epistemologischen Korrespondenzbeziehungen zwischen den Entitäten hinsichtlich ihres formativen bzw. reflektiven Typs (Diamantopoulos and Winklhofer, 2001) festgelegt werden. Zumal das 3-dimensional/5-stufige ERMMA-Konstrukt durch die 15 Dimension/Reifegrad-Konstrukte definiert (formiert) wird, sind alle Beziehungen der 15 Konstrukte zum ERMMA-Konstrukt vom formativen Typus. Das ERMMA-Konstrukt hat folglich 15 *formative Dimension/Reifegrad-Konstrukte*, und es ist ein *formatives mehrdimensional/mehrstufiges Konstrukt*. Analoges wie für die Beziehungen zwischen dem ERMMA-Konstrukt und den Dimension/Reifegrad-Konstrukten gilt auch für die Indikatoren anhand derer die Dimension/Reifegrad-Konstrukte definiert werden. Auch dabei liegen definitorische Beziehungen vor, sodass die Dimension/Reifegrad-Konstrukte *formative Indikatoren* haben, und es sich bei ihnen hinsichtlich ihrer Indikatoren um *formative Dimension/Reifegrad-Konstrukte* handelt. Durch die Verschachtelungen der beiden formativen Beziehungen ist das ERMMA-Konstrukt ein *formatives Konstrukt 2. Ordnung*, welches aus formativen Dimension/Reifegrad-Konstrukten 1. Ordnung mit formativen Indikatoren besteht.

Beachtenswert an dieser Charakterisierung des ERMMA-Konstrukts ist, dass nicht kausale Beziehungen vorliegen, welche in der Literatur üblicherweise verwendet werden. Stattdessen werden *definitorische Beziehungen* verwendet. Kennzeichen derartiger Beziehungen ist, dass die vier Kausalitätsbedingungen (Edwards and Bagozzi, 2000, p. 177) nicht vorliegen, u.z. 1) Ursache und Wirkung sind getrennte Entitäten, 2) Ursache und Wirkung stehen in einer Beziehung (zumeist in probabilistischer Form), 3) Ursache ist Wirkung zeitlich vorgelagert und 4) Elimination von rivalisierenden Erklärungen.

Schließlich ist noch eine Besonderheit bei den formativen Indikatoren zu beachten. Die sich aus dem CMM- und CMMI-Modell ergebende Anforderung, dass zur Erfüllung eines Reifegrads alle diesbezüglichen Indikatoren vorliegen müssen, entspricht einer *multiplikativen Verknüpfungen* der Indikatoren (MacKenzie, Podsakoff and Podsakoff, 2011, p. 302). Im Sinn der auf Aristoteles zurückgehenden philosophische Logik werden die Dimension/Reifegrad-Konstrukte durch *notwendige und*

hinreichende Bedingungen definiert: Das Vorliegen aller Indikatoren ist notwendig und gemeinsam hinreichend.

Ad Konzeptionalisierung und Validierung des Messmodells) Nunmehr geht es nicht mehr um das zu messende Konstrukt, sondern um das für seine Messung zu verwendende Messmodell. Zur Messung des ERMMA-Konstrukts bedarf es der Spezifikation von Indikatoren für alle seine Dimension/Reifegrad-Konstrukte, wobei es Fehlspezifikationen der Indikatoren über die Reifegrade (Stage) und Fallstricke (Pitfall) zu vermeiden gilt. „*Many of the published stage models were presented without defining their stages, without showing evidence of transformations, without explaining the use of stages, and apparently without understanding fully the pitfalls of stage models.*" (Stubbart and Smalley, 1999, p. 284).

Bei der inhaltlichen Spezifikation des ERMMA-Klassifikationsschemas (use of stages) wurden dieser Probleme vermieden, indem progressiv über die Reifegrade angeordnete Indikatoren bestimmt wurden. Dies stellte eine große Herausforderung dar, zumal sich die Progression über alle zu messenden Dimension/Reifegrad-Konstrukte des ERMMA-Konstrukts bezieht. Durch die klare Zuordnung der Indikatoren zu den einzelnen Konstrukten sind diese eindeutig definiert. Durch multiplikativ verknüpfte Indikatoren, deren Vorliegen innerhalb der Dimension/Reifegrad-Konstrukte eine notwendige und gemeinsam hinreichende Bedingung für die Erfüllung des Reifegrads ist, sind auch die Übergänge zwischen den Reifegradstufen eindeutig definiert.

Ein großer Fallstrick (pitfall) bei mehrstufigen Messmodellen ist der „Zirkelschluss". Eine zirkuläre Argumentation entsteht, wenn die Ergebnisse des Messmodells im Rahmen einer Strukturgleichungsanalyse in kausale Beziehungen zu manifesten Variablen gesetzt werden, wobei die manifesten Variablen auch Indikatoren des Messmodells sind. „*A causal model goes beyond merely detecting patterns of activity or behavior that imply descriptive stages... The main challenge for scholars lies in identifying and explaining the underlying processes that account for stages without resorting to circular reasoning. A tautology occurs when stages are used to "explain" observations, which are actually features of the stages themselves. For example, you can't explain your son's "defiance of authority" by the fact that he is a teenager, if defiance of authority is one of the characteristics that defines "teenager".*" (Stubbart and Smalley, 1999, pp. 278–279). Zur Vermeidung des Zirkularitätsproblems wurde bei der Spezifikation des ERMMA-Klassifikationsschemas darauf geachtet, dass keine als Bestimmungsfaktoren vorgesehenen Variablen (z.B. Institutionalisierung von Risikomanagern im Unternehmen oder Tätigkeitsdauer von im Unternehmen eingerichteten Institutionen) als Indikatoren des Messmodells verwendet wurden.

Weitere Besonderheiten bei der Spezifikation der Indikatoren für das ERMMA-Klassifikationsschema ergeben sich aus der Verwendung des daraus abgeleiteten ERMMA-Fragebogens im Rahmen eines Online Self Assessments. Durch das Online Assessment gibt es keine Person, die als „Fragensteller" in Erscheinung tritt. Folglich sind auch diesbezüglich subjektive Beeinflussungsmöglichkeiten ausgeschlossen, und die *Objektivität* der Messung ist sichergestellt. Zur Wahrung der *Reliabilität*, derzufolge eine wiederholte Messung zu gleichen Messergebnissen führen sollte, wird gesichert, indem durch die Indikatoren *Fakten* und nicht *Einstellungen* gemessen werden. Zudem wird bei der Faktenmessung noch darauf geachtet, dass erstens die

Entscheidung über das Vorliegen bzw. Nicht-Vorliegen der Fakten möglichst objektiv und einfach getroffen werden kann, und dass zweitens die Wahrscheinlichkeit für „ehrliche“ Antworten durch eine (potentielle) Überprüfbarkeit der Fakten möglichst hoch ist.

Schließlich gilt es bei der Konzeptionalisierung des ERMMA-Messmodells neben der Objektivität und Reliabilität auch noch die *Validität* durch Gültigkeitsprüfungen sicherzustellen. Hinsichtlich der anzuwendenden Gültigkeitsprüfungen ist der formative Charakter des ERMMA-Konstrukts von zentraler Bedeutung. Bei formativen (definitorischen) Dimensionen bzw. Indikatoren werden die Konstrukte anhand der Dimensionen und Indikatoren definiert. Folglich ist die *Konstruktvalidität* gegeben (Petter, Straub and Rai, 2007, p. 643) und es bedarf nur der *Inhaltsvalidierung*. Die inhaltliche Validierung des ERMMA-Konstrukts erfolgte in zweifacher Weise: Erstens wurde das ERMMA-Konstrukt auf dem ISO/COSO-ERM-*Best Practice-Modell* aufgesetzt, und zweitens wurden *Pilot Tests* mit Risikomanagern großer Unternehmen und mit ausgewiesenen ERM-Experten durchgeführt, u.z. in zwei Plenums- und einer Vielzahl von Einzelbesprechungen. Das in den Besprechungen erhaltene Feedback wurde sukzessive zur Verbesserung des im ERMMA-Projekt iterativ entwickelten Klassifikationsschemas genutzt.

Ad Operationalisierung und Validierung des Messmodells) Nach Durchführung der vorangegangenen Agenden kommt es jetzt, d.h. bei der Operationalisierung des Messmodells zur Erstellung des konkreten ERMMA-Fragebogens. Bei den im Fragebogen gestellten Fragen handelt es sich um die *Indikatorvariablen* anhand derer die Indikatoren des konzeptionalisierten ERMMA-Messmodells (ERMMA-Klassifikationsschemas) operationalisiert und somit operativ messbar gemacht werden.

Bei der „Übersetzung“ der Indikatoren in konkrete Fragen geht es nicht nur um die Formulierung von Fragen, sondern auch um die Benennung der mit den jeweiligen Fragen verbundenen Antwortmöglichkeiten. Hinsichtlich der Antwortmöglichkeiten hat sich beim Übergang vom CMM- auf das CMMI-Modell eine Veränderung ergeben. Im CMM-Modell wurde eine zweigeteilte (dichotome) Skala verwendet, sodass das Vorliegen der befragten Fakten mit Ja/Nein zu beantworten war (Zubrow *et al.*, 1994). Ein möglicher Kritikpunkt an der dichotomen Mess-Skala ist folgender. „*Another disadvantage is that this questionnaire is limited on the number of responses that can be selected (only two options "Yes" or "No") and it limits the information to two extreme ends (Yes if the practice is performed and No if the practice is not performed). Therefore, it does not leave room for intermediate points. For example, the questionnaire does not provide options to capture the cases where the practices are performed but rarely documented or when they are not documented at all.*“ (Cuevas, Serrano and Serrano, 2004, p. 111). Möglicherweise wurde im CMMI-Modell diesem Kritikpunkt Rechnung getragen als in diesem Modell auf eine mehrgeteilte, d.h. polytome Mess-Skala in Form der 10-stufigen CMMI-Questionnaire-Skala umgestellt wurde (Blanchette and Keeler, 2005, p. 7). In öffentlich verfügbaren Self Assessment-Versionen gibt es für das CMMI-Modell auch Varianten mit weniger Antwortmöglichkeiten, z.B. die 5-stufige Skala zwischen „*definitely no (0 points) and definitley yes (5 points)*“ in der Variante für das CMMI Level 2 Self Assessment (Yucalar and Erdogan, 2009, p. 44).

Diesem an der dichotomen Mess-Skala geäußerten Kritikpunkt wurde im ERMMA-Projekt klar widersprochen. Die mehrgeteilte Skala eröffnet nur Ermessenspielräume bei der Beantwortung der Fragen. Das eigentliche Problem liegt in einer unpräzisen Fragestellung. Denn bei einer klar formulierten, sich auf das Vorliegen von Fakten beziehenden Fragestellung ist die dichotome Antwortskala genau das Richtige. Folglich beziehen sich die im ERMMA-Fragebogen gestellten Fragen auf das Vorhandensein der durch die Indikatoren definierten Fakten, welche mit Ja/Nein zu beantworten sind. Darüber hinaus hat die dichotome Messskala gegenüber mehrgeteilten Skalen auch den Vorteil, dass dadurch die *Base Level-Instabilität* gesenkt wird (Dolnicar/Grün 2007, S. 1304), was insbesondere für die beim Monitoring des Reifegrads im Zeitablauf durchzuführenden Messungen bedeutsam ist.

Die Überprüfung hinsichtlich Reliabilität und Validität der Fragen (inklusive dichotomen Antwortmöglichkeiten) des ERMMA-Fragebogens erfolgte zugleich mit der Überprüfung des ERMMA-Klassifikationsschema in den Plenums- und Einzelbesprechungen mit Risikomanagern und ERM-Experten. Darüber hinaus zeigt sich die PVF-Methodik auch diesbezüglich als äußert hilfreich, zumal die deduktive Bestimmung der Fragen aus den schon vorher festgelegten Indikatoren bereits während der Erstellung der Fragen laufend Plausibilitätsprüfungen hinsichtlich Reliabilität und Validität ermöglichte.

3 ERMMA-Messmodell: Klassifikationsschema und Fragebogen

In diesem Kapitel wird das im ERMMA-Projekt entwickelte Messmodell präsentiert, u.z. zuerst das konzeptionalisierte ERMMA-Messmodell in Form des Klassifikationsschemas und sodann das operationalisierte ERMMA-Messmodell in Form des Fragbogens.

3.1 Konzeptionalisiertes ERMMA-Messmodell: Klassifikationsschema

Das 3-dimensionale ISO/COSO-ERM-System-Modell (siehe Abbildung 1) definiert das ERM-System und legt die 3 Dimensionen des ERMMA-Messmodells fest. Die fünf Reifegrade des 3-dimensional/5-stufigen ERMMA-Messmodells enthalten progressiv gestufte Ausgestaltungen des ERM-Systems, welche sich an der CMMI-Skala (CMMI, 2010) von 1) initial, 2) managed, 3) defined, 4) quantitatively managed und 5) optimizing orientiert. Intuitiv können die Reifegrade auch mit dem Schulnotensystem in Verbindung gebracht werden. Bei Vorliegen des Reifegrads 1 liegen die Mindestvoraussetzungen vor, was der Note Genügend entspricht. Die höheren Reifegrade gehen mit besseren Noten einher, und die beste Note ist ein „Römischer Einser (I)“.

Die mit zunehmenden Reifegraden stufenweise besser werdenden Ausgestaltungen des ERM-Systems orientieren sich inhaltlich an Komponenten des ISO-RM-Standards (ISO-RM, 2011) und des COSO-ERM-Frameworks (COSO-ERM, 2017). Die niederen Reifegrade orientieren sich am Risikomanagement-Prozess (inkl. isolierter Risikosteuerung) des ISO-Standards, und die höheren Reifegrade orientieren sich an der

unternehmensweiten sowie unternehmensübergreifenden Perspektive des COSO-Frameworks. Der höchste Reifegrad beinhaltet das Konzept „Interaktives Management“ (Interactive Control System), welches auf Simons (1995) zurückgeht. Kennzeichen des Interaktiven Managements ist die aktive Einwirkung des Top Managements auf die verschiedenen Managementbereiche mit der Absicht, Schwachstellen in den jeweiligen Planungs- und Steuerungssystemen zu identifizieren und sodann mit den zuständigen Managern zu beseitigen.

Tabelle 1 zeigt das auf der konzeptionalen Ebene bestimmte progressiv gestufte ERMMA-Messmodell in Form des 3-dimensional/5-stufigen Klassifikationsschemas. Die 15 Dimension/Reifegrad-Konstrukte des Klassifikationsschemas sind textuell beschrieben und bezeichnen von links nach rechts die qualitativ anspruchsvoller werdenden Ausgestaltungen des ERM-Systems in den 5 Reifegraden der drei Dimensionen A), B) und C).

TABELLE 1: ERMMA-KLASSIFIKATIONSCHEMA – BESCHREIBUNG DER KONSTRUKTE

Dimensionen		Reifegrade				
		RG 1	RG 2	RG 3	RG 4	RG 5
	A. ERM-Governance A1: Risikostrategie A2: Risikoverständnis A3: Risikoorganisation	Prozess-Perspektive in partiellen Bereichen (Silo-Sicht)	Prozess-Perspektive inkl. Prüfung und Management (single loop)	Unternehmensweite (holistisch-differenzierte) Perspektive	Unternehmensübergreifende (corporate) Perspektive (double loop)	Vom Top-Management interaktiv gemanagte Systeme
	B. Risiko-Management-system B1: RM-Prozess B2: RM-Schulungssystem B3: RM-Informationssyst.	Risiko-management-Prozess	Risiko-management-Prozess (inkl. Monitoring und Review) (single loop)	Unternehmensweit standardisierter RM-Prozess (inkl. …)	Unternehmensweiter und -übergreifender RM-Prozess (inkl. …) (double loop)	
	C. Risikobasierte Planung und Steuerungssysteme C1: Strateg. Management C2: Financ. Management C3: Operat. Management	Risiko-Limit-Systeme in partiellen Bereichen	Key Risk-basierte Planung (inkl. Strategie- bzw. Zielfestlegung)	Key Risk-basierte Steuerungssysteme (i.e. Performance-Mangement)	Management-Systeme mit Risiko-adjustierten Performance-Kennzahlen	

Die sich auf das Risikomanagementsysteme beziehende Dimension B) bietet eine gute Möglichkeit für den gedanklichen Einstieg in das ERMMA-Klassifikationsschema. Als Ausgangspunkt wird exemplarisch der Risikomanagement-Prozess gewählt. Im einfachsten Fall (Reifegrad 1, kurz: RG 1) werden in einem solchen Prozess Risiken identifiziert (1. Indikator), gemessen (2. Indikator) und in isolierten Systemen gesteuert (3. Indikator). Die in Klammern gesetzten Hinweise zeigen an, dass mit der Beschreibung des Dimension/Reifegrad-Konstrukts konkrete Indikatoren einhergehen, mit welchen die Konstrukte konzeptionalisiert, d.h. auf der konzeptionalen Ebene definiert werden. Zur Erfüllung des zweiten Reifegrads (RG 2) wird zusätzlich gefordert, dass der Risikomanagement-Prozess selbst auch gemanagt wird, indem er einer

Überwachung/Monitoring inkl. Anpassung (4. Indikator) und einer Überprüfung/Review (5. Indikator) unterzogen wird. Die fünf, in den ersten beiden Reifegraden verwendeten Indikatoren decken sich weitgehend mit dem dem ISO-Standard zugrundeliegenden Verständnis von einem gemanagten Risikomanagement-Prozess. Die Zweiteilung des Prozesses in die beiden Reifegrade liefert erstens die von progressiv gestuften Messmodellen geforderte Progression über die Reifegrade und korrespondiert zweitens mit den ersten beiden Reifegraden des CMMI-Modells.

Im Reifegrad 3 (RG 3) kommt die unternehmensweite Perspektive des COSO-ERM-Frameworks ins Spiel. In einem unternehmensweit ausgestalteten ERM-System ist der Risikomanagement-Prozess standardisiert, sodass es eine Vorlage gibt nach der der Prozess in den unterschiedlichen Unternehmensbereichen eingesetzt werden kann. Im COSO-ERM ist der Prozess generisch definiert, sodass er in den unterschiedlichen Bereichen situativ angepasst implementiert werden kann. Dieser generische, d.h. holistisch-differenzierte Ansatz (6. Indikator) ist wichtig, zumal in den verschiedenen Bereichen unterschiedliche Risikotypen vorliegen, welche auch unterschiedliche Identifikations-, Mess- und Steuerungsmethoden erfordern. In diesem Zusammenhang ist die von Mikes/Kaplan (2014) eingeführte Unterscheidung von vermeidbaren Risiken (preventable risk), Geschäftsrisiken (strategy execution risk) und externen Risiken (external risk) wichtig, zumal sie den Aspekt der unterschiedlichen Steuerbarkeit von Risiken und somit Risikotypen-abhängige Risikopolitiken einführt. Neben dem generischen Zugang liegt beim unternehmensweit ausgelegten ERM-System auch eine sich auf das gesamte Unternehmen beziehende Koordination (7. Indikator) vor, sodass die Risikomanagement-Prozesse in den verschiedenen Bereichen periodisch koordiniert ablaufen. Durch die unternehmensweite Standardisierung deckt sich der Reifegrad auch mit dem Verständnis vom Reifegrad 3 im CMMI-Modell.

Im Reifegrad 4 des CMMI-Modells wird ein quantitatives Prozessmanagement gefordert. Diese Anforderung liegt auch im Reifegrad 4 (RG 4) des Risikomanagement-Prozesses vor, indem eine unternehmensübergreifende Aggregation der Risiken (8. Indikator) sowie die Einbeziehung von realisierten Risiken (9. Indikator) und nicht-realisierten Chancen (10. Indikator) gefordert wird. Im Reifegrad 5 (RG 5) wird die CMMI-Modell postulierte Optimizing-Eigenschaft durch ein Interaktives (Simons, 1995) Prozessmanagement (11. Indikator) erreicht, wobei der unternehmensweite und -übergreifende Risikomanagement-Prozess nicht nur diagnostisch im Sinne eines Single und Double Loop-Managementsystems genutzt wird, sondern zudem vom Top Management interaktiv forciert und gemangt wird.

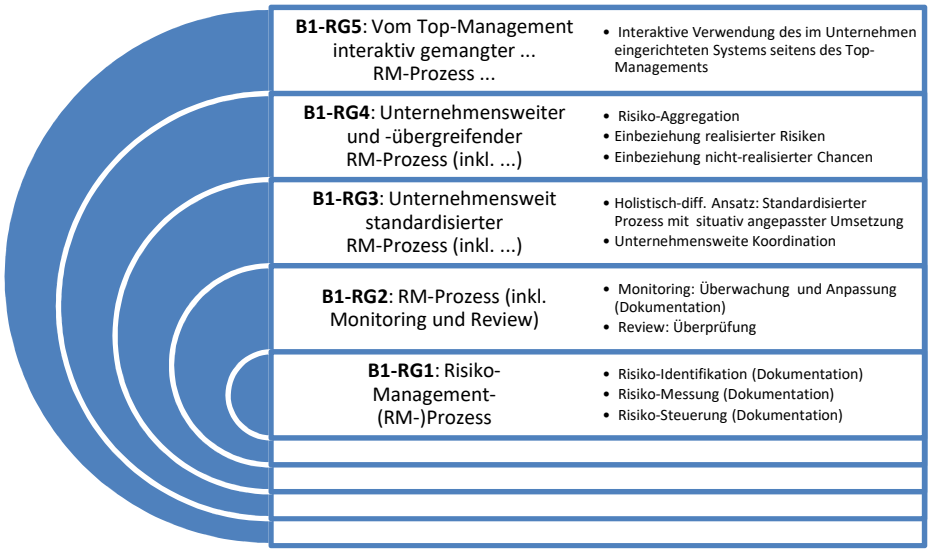

ABBILDUNG 2: ERMMA-KLASSIFIKATIONSSCHEMA – INDIKATOREN FÜR DEN RM-PROZESS

Die soeben erfolgte Erörterung der 11 Indikatoren bezieht sich genau genommen auf den Risikomanagement-Prozess, welcher stellvertretend für das in der Dimension B) vorliegende Risikomanagementsystem verwendet wurde. In Abbildung 2 wird der diesbezügliche Ausschnitt des ERMMA-Klassifikationsschemas graphisch anhand von konzentrischen Kreisen dargestellt. Er beinhaltet die 11 Indikatoren, welche zur Messung der 5 Reifegrade verwendet werden. Durch die sukzessiv umfassender werdenden Kreise ist die progressive Anordnung der zur Reifegradmessung verwendeten Indikatoren auch bildlich zu sehen. Aus mengentheoretischer Sicht handelt es sich bei der progressiven Anordnung der Indikatoren um ein über die Reifegrade *geordnetes Mengensystem*. Die Gruppierung der Indikatoren in den Reifegraden stellt eine Partition der Menge aller Indikatoren dar. Bei kumulativer Betrachtung über die Reifegrade zeigen sich *feiner werdende Partitionen*, zumal sukzessive mehr Reifegrad-Teilmengen aus der Menge aller Indikatoren abgespaltet werden.

Bei genauer Betrachtung des in Tabelle 1 abgebildeten ERMMA-Klassifikationsschemas ist zu sehen, dass in allen 3 Dimensionen jeweils noch 3 Sub-Dimensionen eingerichtet sind. Diese Erweiterung dient zur Einbeziehung weitergehender Aspekte in die Reifegradmessung. In der Dimension B) ist neben dem Risikomanagement-Prozess auch noch das sich auf das Risikomanagement beziehende Schulungs- bzw. Informationssystem als eigene Sub-Dimension eingerichtet. Durch diese Erweiterung wird der Reifegrad des in der Dimension B) gemessenen Risikomanagementsystems umfassend anhand von 3 (Sub-)Reifegraden gemessen, u.z. für den Risikomanagement-Prozess, das Schulungs- und das Informationssystem. Rechentechnisch wird der Reifegrad für die Dimension anhand des arithmetischen Durchschnitts der drei (Sub-)Reifegrade bestimmt. Durch die Einbeziehung der Sub-Dimensionen erhöht sich auch die Ordnung des ERMMA-Konstrukts, welches somit ein *9-subdimensional/5-stufiges Konstrukt 3. Ordnung* ist. Allen Sub-Dimensionen liegt eine progressive Reifegradstruktur

zugrunde. Das Verständnis für progressive Strukturen sollte anhand der Erläuterung für den Risikomanagement-Prozess gelegt worden sein. Folglich und zur Reduktion des Erläuterungsbedarfs werden nachfolgend die Dimensionen C) und A) nur auf Dimensionsebene und in Kurzform erläutert.

In der Dimension C geht es um die Integration der im Risikomanagement-Prozess generierten Risikoinformationen in bereits im Unternehmen eingesetzte (traditionelle) Managementsysteme. Die diesbezüglichen Reifegrade richten sich nach dem Grad der Integration, wobei der isolierten Risikosteuerung (ISO-RM-Standard) der Grad 0 und der integrierten Risikosteuerung (COSO-ERM-Framework) positive Grade zugewiesen werden. Konkret werden zur Bestimmung der ersten 4 Reifegrade folgende Integrationsgrade unterschieden:

- Grad 0: es liegt keine Integration vor, sodass nur Risikolimit-Systeme in ausgewählten Bereichen eingesetzt werden, wobei einzelnen Risikoarten gemessen und bezüglich der Einhaltung der gesetzten Limits gesteuert werden.
- Grad 1: es liegt eine Integration in die Planungssysteme vor (z.B. Einbeziehung von Risiken bei Investitionsentscheidungen und Bandbreitenplanung).
- Grad 2: es liegt eine Integration in die Performance Management Systeme vor (z.B. mehrperiodiges stochastisches Cost Volume Profit-Management inkl. Signifikanzanalyse von Abweichungen).
- Grad 3: die Integration erfolgt durch Verwendung von risikobasierten Performance-Kennzahlen (z.B. Return on Risk Adjusted Capital, kurz: RoRaC).

Beim 5. Reifegrad liegt wiederum ein Interaktives Management vor, wobei das Top Management in Interaktionen mit dem Bereichsmanagement die Angemessenheit der risikobasierten Planung und Steuerungssysteme hinterfragt und etwaige Verbesserungsmöglichkeiten sucht. Bei genauer Betrachtung von Tabelle 1 zeigt sich, dass auch die Dimension C) 3 Sub-Dimensionen besitzt, u.z. das strategische Management, das finanzielle Management und das operative Management. Die für die Dimension C) erläuterte progressive Reifegradanordnung bezieht sich auf alle drei Managementbereiche.

Ein funktionierendes ERM-System ist kein Zufallsprodukt. So sind hohe Reifegrade in den Dimensionen B) und C) keine Glückssache. Vielmehr bedarf es dazu konkreter Planungen und Vorkehrungen, welche der ERM-Governance (Dimension A), wobei es sich um den „Master Mind“ zur ERM-System-Ausgestaltung handelt, folgen. Die Reifegrade der ERM-Governance beziehen sich auf die im Top Management vorherrschenden Perspektiven (Einstellungen) auf das unternehmensweite Risikomanagement. Durch die zentrale Verankerung des ISO/COSO-ERM-System-Modells orientiert sich die Bestimmung der Perspektiven ebenfalls am ISO-RM-Standard und am COSO-ERM-Framework. Im Reifegrad 1 erachtet das Top Management das Risikomanagement nur für ausgewählte Bereiche als relevant. Im Reifegrad 2 wird auch die Relevanz hinsichtlich des Monitoring und der Überwachung des Risikomanagements gesehen. Somit richtet sich im Reifegrad 2 die Perspektive des Top Management nach dem ISO-RM-Standard. Auf dem Reifegrad 3 besitzt das Top Management eine unternehmensweite (holistisch-differenzierte) Perspektive, sodass Komponenten des COSO-ERM-Frameworks berücksichtigt werden. Die Komplettierung der COSO-ERM-

Komponenten erfolgt auf Reifegrad 4, wobei dem Top Management auch eine unternehmensübergreifende Portfoliobetrachtung wichtig ist. Auf Reifegrad 5 hat das Top Management auch Pläne für das Interaktive Management des ERM-Systems und wendet diese auch an, um die Angemessenheit des Systems im Zeitablauf zu sichern.

Die Messung der Reifegrade für die ERM-Governance erfolgt in 3 Sub-Dimensionen, u.z. Risikostrategie, Risikoverständnis und Risikoorganisation. Die *Risikostrategie* ist definiert nach dem IDW-Prüfungsstandard (IDW-PS981, 2017) und umfasst die *Risikotragfähigkeit*, den *Risikoappetit* und die *Risikopolitik*. Die 5 Reifegrade für die Risikostrategie richten sich nach den beim Top Management vorliegenden Perspektiven (Einstellungen), sodass auch diese nach dem ISO-RM-Standard und dem COSO-ERM-Framework ausgelegt sind. Gleiches gilt für die progressive Anordnung der Reifegrade zur Messung vom Risikoverständnis (hinsichtlich der Steuerbarkeit und dem Management der verschiedenen Risikotypen) und der Risikoorganisation (hinsichtlich der Verankerung von Risikomanagement-Institutionen und -funktionen in der Auf- und Ablauforganisation des Unternehmens).

3.2 Operationalisiertes ERMMA-Messmodell: Fragebogen

Beim ERMMA-Klassifikationsschema handelt es sich um das konzeptionalisierte Messmodell, welches die zur Messung der nicht beobachtbaren Dimension/Reifegrad-Konstrukte spezifizierten Indikatoren beinhaltet. Durch die Einbeziehung von jeweils 3 Sub-Dimensionen in allen 3 Dimensionen liegt ein 9-sub-dimensional/5-stufiges Klassifikationsschema vor. Im Rahmen der Operationalisierung wird dieses Klassifikationsschema in einen Fragebogen übersetzt. Zu diesem Zweck sind für jeden Indikator geeignete Fragen und die dazugehörigen Antwortmöglichkeiten zu formulieren.

Die zur Operationalisierung der Indikatoren verwendeten Fragen sind in Tabelle 2 auszugsweise für die *Sub-Dimension B1) Risikomanagement-Prozess* zu sehen. Dabei zeigt sich auch, dass es sich bei den im Fragebogen gestellten „Fragen" zumeist um Aussagen (Statement, Item) handelt, welche der *Booleschen Logik* mit Ja (true) oder Nein (false) zu beantworten sind. Bei den Fragen zum Reifegrad 1 (RG1) und der ersten Fragen zum 2. Reifegrad (RG2) handelt es sich um *Multiple Choice-Fragen*. Bei diesem Fragentyp wird das Ankreuzen eines Bereichs als Ja gewertet wird. Die nachfolgenden Fragen sind *Single Choice-Fragen*. Bei diesem Fragentyp ist explizit zwischen Ja und Nein zu wählen.

TABELLE 2: ERMMA-FRAGEBOGEN – B1) RM-PROZESS (AUSZUG)

RG1	* Risiken sind identifiziert und dokumentiert für die Bereiche: Beschaffung, Produktion, Vertrieb, Finanzwesen, Andere Bereiche. * Methoden zur Messung von Risiken sind dokumentiert für die Bereiche ... * Maßnahmen zur Bewertung und Steuerung von Risiken sind dokumentiert für die Bereiche ...
RG2	* Die Überwachung und bei Bedarf erforderliche Anpassung (Monitoring) des Risikomanagement-Prozesses sind dokumentiert für die Bereiche …

	* Die Interne Revision (oder sonstige interne bzw. externe Instanz) überprüft den Risikomanagement-Prozess und dessen Monitoring hinsichtlich Angemessenheit und Wirksamkeit zumindest in ausgewählten Unternehmensbereichen
RG3	* Risiken sind unternehmensweit, d.h. für alle wichtigen Bereiche im Unternehmen dokumentiert und werden mit verschiedenen Methoden (z.B. Top-down und Bottom-up) identifiziert * ... * Bei der Überwachung und Anpassung (Monitoring) des Risikomanagement-Prozesses in den verschiedenen Bereichen werden durchaus unterschiedliche Konzepte verwendet (z.B. Einbeziehung von Betrugsrisiken im Compliance-Management bzw. von Chancen im Währungsrisiko-Management) * ...
RG4	* Die Interne Revision (oder sonstige interne bzw. externe Instanz) überprüft den unternehmensweit sowie -übergreifend (inkl. Risikoaggregation) eingerichteten Risikomanagement-Prozess und dessen Monitoring hinsichtlich Angemessenheit und Wirksamkeit * …
RG5	* Das Top-Management debattiert und diskutiert mit den Eigentümern bzw. Aufsichtsräten periodisch die Eignung des Risikomanagement-Prozesses und dessen Monitoring, welche unternehmensweit und -übergreifend (inkl. Risikoaggregation) eingerichtet sind

Durch die Fragen im ERMMA-Fragebogen wird das Vorliegen der im ERMMA-Klassifikationsschema spezifizierten Fakten-bezogenen Indikatoren mit der Booleschen Logik gemessen. So misst z.B. die erste für den Reifegrad 1 gestellte Frage (Tabelle 2) „Risiken sind identifiziert und dokumentiert für die Bereiche: Beschaffung, Produktion, Vertrieb, Finanzwesen, Andere Bereiche“ ob die Risikoidentifikation (Indikator für den Reifegrad 1 in Abbildung 2) in einzelnen Unternehmensbereichen vorliegt. Zumal die Frage auf identifizierte Risiken und deren Dokumentation Bezug nimmt, ist sie objektiv beantwortbar und die Korrektheit der Antwort ließe sich durch Überprüfung der Dokumentation auch feststellen.

Im Vergleich zur Spezifikation der progressiv angeordneten Indikatoren bei der Konzeptionalisierung des ERMMA-Messmodells ist die Formulierung der Fragen (inkl. Antwortmöglichkeiten) bei der Operationalisierung des konzeptionalisierten Messmodells vergleichsweise einfach. Zudem lässt sich durch die Vorabspezifikation der Indikatoren auch die Gültigkeit der Fragen bereits bei ihrer Erstellung plausibilitätsmäßig und sprachlich prüfen. Diese Vorteile, welcher sich durch die Verwendung der PVF-Methodik zur Erstellung des ERMMA-Fragebogens ergeben, fehlen, wenn die Fragen eines Fragebogen – wie es häufig der Fall ist – ad hoc und ohne Bezugnahme auf ein zugrunde liegendes Konstrukt bzw. Indikatoren erstellt werden.

Durch die Beantwortung der Fragen des ERMMA-Fragebogens werden für alle 9 Sub-Dimensionen die Reifegrade bestimmt. Die jeweils erreichten Reifegrade bedeuten, dass jeweils alle Indikatoren bis zu einem bestimmten Reifegrad vorliegen. Dies entspricht der multiplikativen Verknüpfung der reifegradspezifischen Indikatoren, wobei die Erfüllung aller Indikatoren eines Reifegrads notwendig und gemeinsam hinreichend für die Erreichung des Reifegrads ist. Die Reifegrade der 3 Dimensionen ergeben sich aus dem Durchschnitt der in den jeweiligen Sub-Dimensionen erreichten

Reifegrade, und der gesamthafte ERMMA-Score ergibt sich als Durchschnitt der Reifegrade in den 3 Dimensionen.

4 ERMMA-Online-Applikation: ERMMA-Monitoring-Tool

In einem klassischen mit der Wasserfall-Technik abgewickelten Software-Projekt würden zuerst alle Anforderungen an die Software definiert, welche dann sukzessive durch Programmierung abgearbeitet würden. Im ERMMA-Projekt war diese Vorgehensweise nicht möglich und auch gar nicht erwünscht. Vielmehr liefen die Erstellung des ERMMA-Messmodells und dessen IT-mäßigen Implementierung parallel ab. Ermöglicht wurde dies durch die Verwendung der agilen Programmiertechnik und des Model Driven Developments (Pastor *et al.*, 2008). Dabei wurden zuerst dem Predictive Validity Framework folgend die essentiellen Bestandteile des ERMMA-Modells bestimmt (Dimensionen, Reifegrade, Indikatoren und Indikatorvariablen) und sodann diesbezügliche Eingabe-, Informationsverarbeitungs- und Navigationsfunktionalitäten programmiert. Im Fortgang des Projekts wurden dann sukzessiv weitere Anforderungen spezifiziert und implementiert bis das Projekt mit der nun vorliegenden ERMMA-Online-Applikation abgeschlossen wurde.

4.1 ERMMA-Online-Applikation: User-Perspektive

Zur Nutzung des ERMMA-Online-Applikation benötigt der Benutzer lediglich einen Internet Browser. Nach Kontaktaufnahme mit der ERMMA-Homepage auf dem Institutsserver *https://ermma.imw.tuwien.ac.at* zeigt sich der in Abbildung 3 dargestellte Eröffnungsbildschirm.

Zur Nutzung der Applikation bedarf es lediglich der Registrierung, wozu eine gültige E-Mail-Adresse, ein Passwort und der Registrierungscode benötigt wird. Nach der Registrierung wird ein automatisch erstellter Benutzername an die vom Benutzer genannte E-Mail-Adresse zugestellt. Mit dem Benutzernamen und dem Passwort kann man sich dann auf der Homepage anmelden und das Assessment starten. Nach Beendigung des Self Assessments kann der *Assessment-Report* (inkl. Feedback-Informationen) in Form einer PDF-Datei heruntergeladen werden. Darüber hinaus kann das Assessment jährlich aktualisiert werden, um die Entwicklung des ERM-System-Reifegrads zu monitoren.

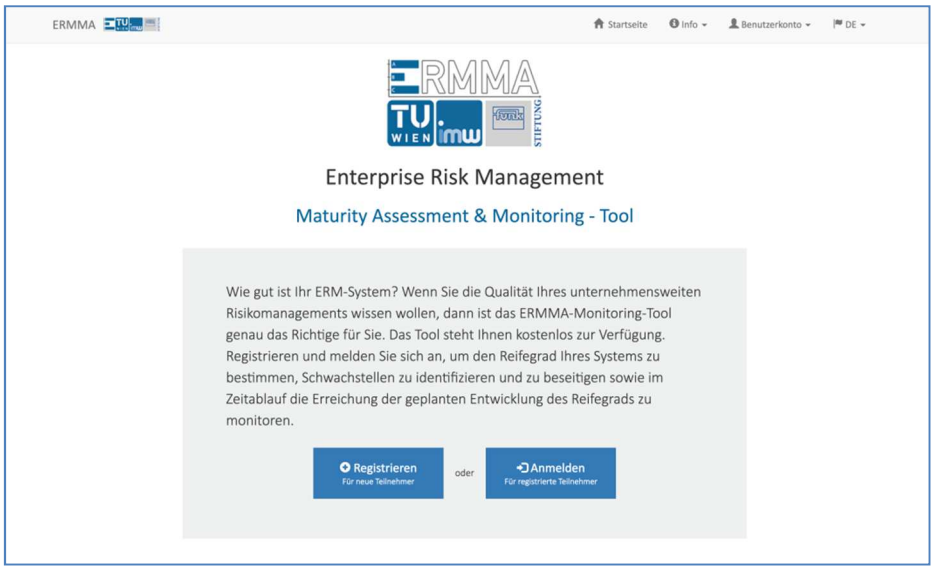

ABBILDUNG 3: ERM-MATURITY ASSESSMENT & MONITORING-TOOL

4.2 ERMMA-Online-Applikation: Feedback an teilnehmende Unternehmen

Das ERMMA-Online-Applikation ist eine auf einem TU Wien-Server laufende, web-basierte Applikation, welche von Unternehmen aus dem Nicht-Finanzdienstleistungsbereich kostenlos 1) zur Messung des Reifegrads des im Unternehmen eingerichteten ERM-Systems sowie 2) zum Monitoring der Reifegrad-Entwicklung im Zeitablauf eingesetzt werden kann. Somit ist die Applikation ein *ERMMA-Monitoring Tool*, mit welchem einerseits der Reifegrad des ERM-Systems bestimmt (Maturity Assessment) und andererseits die (zielgerichtete) Entwicklung des Reifegrads im Zeitablauf gemonitort (Maturity Monitoring) werden kann.

Ad Maturity Assessment) Abbildung 4 zeigt das erste Feedback (1), welches den teilnehmenden Unternehmen unmittelbar nach Beantwortung des ERMMA-Online-Fragebogens in elektronischer Form als PDF-Datei zur Verfügung gestellt wird. Es enthält die in den 9 Sub-Dimensionen erzielten Reifegrade, welche als *ERMMA-Profil* bezeichnet werden. Dieses Profil ist die zentrale Feedback-Information, welche den Unternehmen eine Rückmeldung über die Stärken und Schwächen in den einzelnen Sub-Dimensionen gibt und die Möglichkeit zu Priorisierung einzelner Sub-Dimensionen für künftige Entwicklungen bietet.

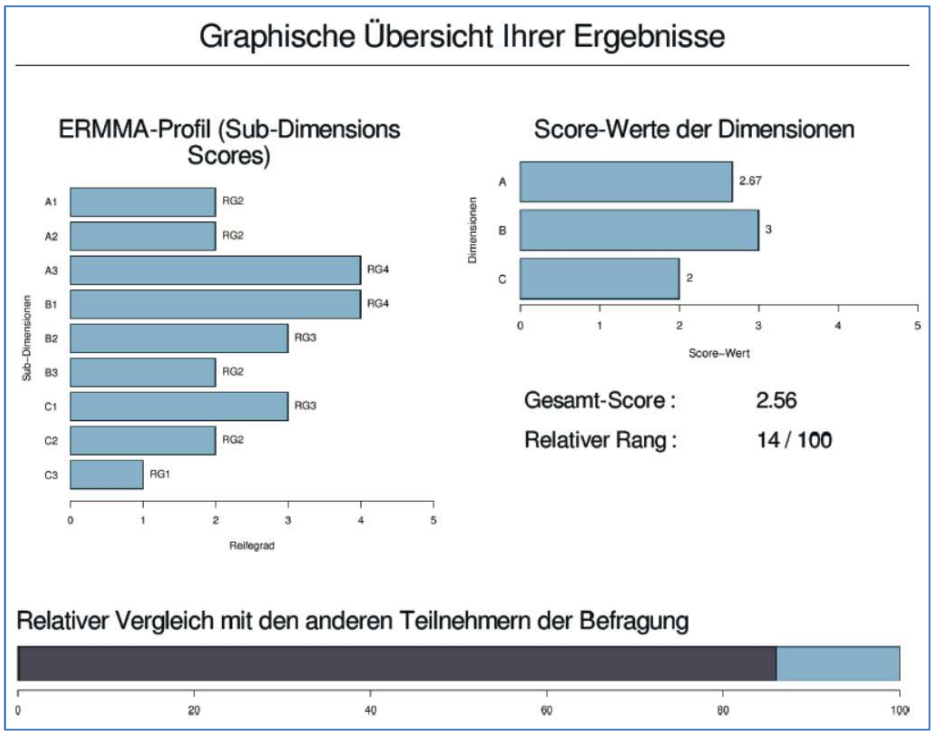

ABBILDUNG 4: FEEDBACK AN UNTERNEHMEN (1) – ERMMA-PROFIL UND REIFEGRADE

In Abbildung 4 sind die Reifegrade für die drei Dimensionen sowie der Gesamt-Score zu sehen, welche sich jeweils aus gleichgewichteten Durchschnittswerten der zugrunde liegenden (Sub-)Dimensionen ergeben. Unter dem Gesamt-Score wird die relative Positionierung (relativer Rang) des für das Unternehmen gemessenen Reifegrads gegenüber allen teilnehmenden Unternehmen angegeben. Der 14. Rang im Beispiel besagt, dass 13 % der Unternehmen einen besseren und 86 % einen schlechteren Reifegrad haben.

Abbildung 5 zeigt das zweite Feedback (2), welches konkrete Anhaltspunkte zur gezielten Weiterentwicklung des Reifegrad-Profils bzw. der daraus berechneten Reifegrade für die Dimensions- und Gesamtebene liefert. Es gibt Auskunft über die erreichten Inhalte sowie die für einen höheren Reifegrad noch ausstehenden Inhalte.

Ad Maturity Monitoring) Durch eine erneute Nutzung des ERMMA-Monitoring Tools im Zeitablauf lässt sich die Entwicklung des Reifegrads monitoren. Der neue Reifegrad in einem nachfolgenden Assessment ergibt sich durch Beantwortung der dann gestellten Fragen. Dabei kommt die *Intelligenz* des ERMMA-Fragebogens ins Spiel. Das Assessment startet nämlich nicht wieder am Anfang wie bei der ersten Einstufung. Vielmehr werden Fragen in Abhängigkeit der in den vorangegangenen Einstufungen ermittelten Indikatoren gestellt. Somit wird beim Folge-Assessments auf den jeweils individuellen Stand eines jeden Unternehmens eingegangen. Die sich im Zeitablauf ergebenden zeitlichen Entwicklungen der Reifegrade sowie der jeweiligen

relativen Ränge liefern gute Anhaltpunkte für die zielgerichtete Reifegrad-Steuerung. Das ERMMA-Monitoring liefert somit die notwendigen Informationen für das „Reifegrad-Controlling“, i.e. zur Erreichung des angestrebten Reifegrad-Profils bzw. der angestrebten Reifegrade.

Assessment für Dimension B : Risiko MGT System

Sub-Dimension	Erreichter Reifegrad	Erreichter Inhalt	Ausstehender Inhalt für höheren Reifegrad
B1 : RM-Prozess	RG4	Die Verantwortlichen (z.B. Risikomanager) für den Risikomanagement-Prozess (mit Monitoring) aggregieren Risiken über das gesamte Unternehmen (z.B. mit Simulationsmethoden unter Einbeziehung von Risikoverbundeffekten)	Das Top-Management debattiert und diskutiert mit den Eigentümern bzw. Aufsichtsräten periodisch die Eignung des Risikomanagement-Prozesses und dessen Monitoring, welche unternehmensweit und -übergreifend (inkl. Risikoaggregation) eingerichtet sind
B2 : RM-Schulungssystem	RG3	Die Verantwortlichen (z.B. Risikomanager) für den Risikomanagement-Prozess und dessen Monitoring bilden sich weiter hinsichtlich einer angemessenen Funktionsweise des unternehmensweit, d.h. in allen wichtigen Bereichen des Unternehmens eingerichteten Risikomanagement-Prozesses mit Monitoring	Die Verantwortlichen (z.B. Risikomanager) für den Risikomanagement-Prozess und dessen Monitoring bilden sich weiter hinsichtlich einer angemessenen Funktionsweise des unternehmensweit und -übergreifend (inkl. Risikoaggregation) eingerichteten Risikomanagement-Prozesses mit Monitoring
B3 : RM-Informationssystem	RG2	Die softwaremäßige Unterstützung von Risikomanagement-Prozessen wird zumindest in ausgewählten Unternehmensbereichen überwacht und bei Bedarf angepasst	Risikomanagement-Prozesse werden unternehmensweit, d.h. in allen wichtigen Unternehmensbereichen softwaremäßige (z.B. Risikomanagement- bzw. Governance Risk Compliance-Software) unterstützt

ABBILDUNG 5: FEEDBACK AN UNTERN. (2) – HINWEISE ZUR ERMMA-VERBESSERUNG

4.3 ERMMA-Online-Applikation: 3-Schicht-Architektur und Messmodell-Konfigurator

Die ERMMA-Online-Applikation wurde in einer modernen 3-Schicht-Architektur implementiert, wobei zwischen der graphischen Benutzeroberfläche (Graphical User Interface – kurz: GUI), der Ebene der Geschäftslogik (Business Logic) und der Datenebene (Persistenz) unterschieden wird. Die konkrete 3-Schicht-Architektur ist in Abbildung 6 zu sehen.

GUI-Schicht: Für den Zugang zur ERMMA-Applikation benötigen die Benutzer lediglich einen Internet Browser, welcher über das https-Protokoll auf die Web Applikation zugreift. Die GUI-Funktionalitäten werden über das Angular J(ava)S(cript)-Framework, welches intern mit dem Model (service)-View-Controller-Muster implementiert wird, verfügbar gemacht.

Geschäftslogik-Schicht: Die Geschäftslogik wird durch das Spring-Framework zur Verfügung gestellt, wobei in *Domain* die statischen Elemente (Entity Beans in JEE) und in *Service* (Session Beans in JEE) die dynamischen Elemente der Geschäftslogik abgelegt werden. Das *Repository* enthält die von Spring verfügbar gemachten Funktionalitäten für die Kommunikation mit der Datenbank, welche über die Java Persistence API (*JPA*) mit Hibernate’s Object Relational Mapping (*ORM*) Support vollzogen wird. Die Kommunikation mit der Benutzeroberfläche erfolgt über das Java Script Object Notation (Jason)-Format im http-Protokoll zwischen der REpresentational State Transfer (*REST*) Application Programming Interface (*API*) im Spring und dem *Service* in

Angular JS. Schließlich ist noch die Kommunikation zwischen dem Spring *Service* und dem R Server eingerichtet.

Persistenz-Schicht: Für die Speicherung der Daten wird die PostgreSQL-Datenbank verwendet, welche über die JPA mit der Geschäftslogik verbunden ist und das ORM von Hibernate umsetzt.

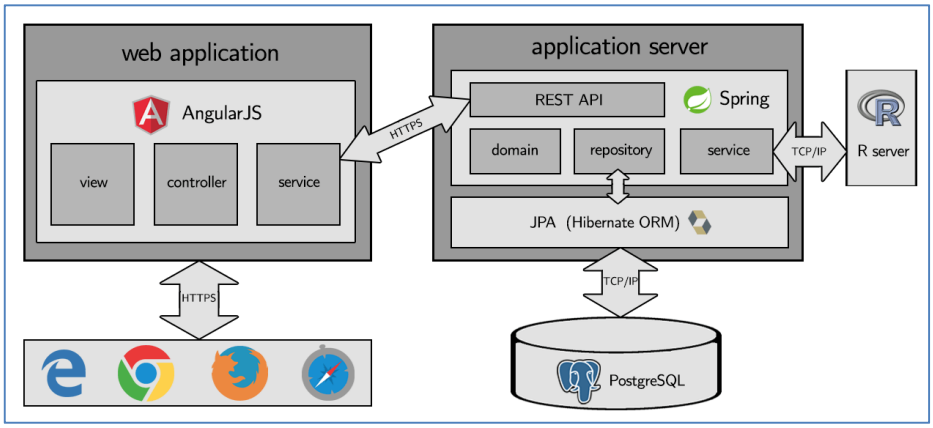

ABBILDUNG 6: ERMMA-ONLINE-APPLIKATION – 3-SCHICHT-ARCHITEKTUR

Der *Messmodell-Konfigurator* ist eine zusätzliche in der ERMMA-Online-Applikation eingerichtete Benutzeroberfläche, welche dem *Fragebogen-Designer* bei der Erstellung des ERMMA-Messmodells (Klassifikationsschema und Fragebogen) software-mäßig unterstützt. Abbildung 7 zeigt das Hauptmenü des Konfigurators. Bei der Spezifikation des Reifegradmodells können zwei Modellvarianten eingerichtet werden. 1) die *einfache Variante*, welche nur eine Dimension und einen durch eine Frage gemessenen Indikator pro Reifegrad zulässt, und 2) die *umfassende Variante*, wobei zwei und mehr Dimensionen mit jeweils beliebig vielen Indikatoren eingerichtet werden können. Bei der umfassenden Variante steht das Klassifikationsschema im Mittelpunkt, welches es zu dimensionieren, konzeptualisieren und operationalisieren gilt.

Zur Konfiguration des ERMMA-Fragebogens sind folgende 4 Arbeitspakete durchzuführen:

1) Dimensionierung des ERMMA-Klassifikationsrahmens, d.h. Festlegung der Anzahl der Dimensionen (3), Sub-Dimensionen (3 je Dimension) und Reifegraden (5),
2) Konzeptionalisierung des ERMMA-Messmodells, d.h. Festlegung der Indikatoren zur Messung der Dimension/Reifegrad-Konstrukte 1. Ordnung (45=3*3*5),
3) Operationalisierung des ERMMA-Messmodells, d.h. Formulierung der Indikatorvariablen (Fragen inkl. Antwortskala), welche zur Booleschen Messung der Indikatoren verwendet werden und
4) Anpassung der Benutzeroberfläche an den ERMMA-Kontext (Branding) sowie informationale Ausgestaltung des E-Mail Messaging-Systems.

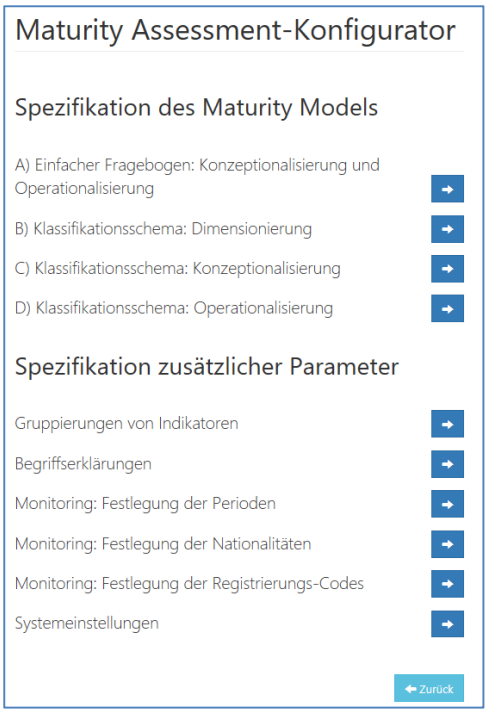

ABBILDUNG 7: MESSMODELL-KONFIGURATOR – HAUPTMENÜ

Von diesen 4 Arbeitspaketen werden die ersten 3 vom Messmodell-Konfigurator unterstützt. Das vierte Paket erfordert eine Anpassung im Programm-Code. Im Online-Betrieb der ERMMA-Applikation werden folgende Aufgaben automatisch ausgeführt:

1) Präsentation des ERMMA-Fragebogens auf der Benutzeroberfläche,
2) intelligente Navigation des Benutzers entsprechend seiner gewählten Antworten,
3) Speicherung der gegebenen Antworten und erzielten Reifegrade und
4) Download-Bereitstellung der Feedback-Information im PDF-Format.

5 ERMMA-Ergebnisse: Deskriptive und explorative Analysen

In diesem Kapitel werden die Ergebnisse der in Österreich durchgeführten ERMMA-Studie (2017) präsentiert. Für die Studie wurde die ERMMA-Online-Applikation für ein halbes Jahr bis Ende September 2017 freigeschaltet. Die während dieses Zeitraums eingegangen Rückmeldungen wurden im Statistikpaket R statistisch ausgewertet. Dabei wurden einerseits deskriptive Statistiken erstellt. Diese geben Einblicke in die Häufigkeiten der verschiedenen ERM-System-Reifegrade. Andererseits wurden kausale Zusammenhänge hinsichtlich der Bestimmungsfaktoren für die Reifegrade statistisch getestet.

5.1 Beschreibung der Stichprobe

An der ERMMA-Studie haben sich 71 Unternehmen beteiligt. Bei ca. der Hälfte der Unternehmen handelt es sich um Produktionsunternehmen. Die restlichen Unternehmen verteilen sich gleichermaßen über die verschiedenen Branchen (exkl. Finanzdienstleistungsindustrie). Die Stichprobe setzt sich hauptsächlich aus Kapitalgesellschaften (91.55 %) zusammen, wobei ca. ¾ der Unternehmen die Rechtsform einer GesmbH und ca. ¼ der Unternehmen die Rechtsform einer Aktiengesellschaft haben. 85.92 % der Unternehmen unterliegen einer externen Wirtschaftsprüfung. Mehr als die Hälfte der Unternehmen ist Eigentümer-geführt (59.15 %). Bezüglich der Anzahl der Mitarbeiter liegt eine annähernde Gleichverteilung über die Mitarbeiterklassen vor, d.h. 26.76 % (<49), 18.31 % (<499), 16.90 % (<999), 18.31 (<4999), 19.72 % (5000+). Folglich gibt die Stichprobe Einblicke in die ERM-System-Qualitäten von österreichischen Kapitalgesellschaften. Die Rücklaufquote und Repräsentativität der Studienteilnehmer kann nicht geprüft werden, zumal nicht bekannt ist, wie viele Unternehmen insgesamt zur Teilnahme eingeladen wurden. Die Einladungen wurden nämlich von den die Studie unterstützenden Partnern (Funk Österreich, Creditreform Österreich, IIA Österreich und EY Österreich) in elektronischer Form an ihre jeweiligen Kunden bzw. Mitglieder versendet.

5.2 Deskriptive Analyse

In der Studie hat sich die in Abbildung 8 in Form eines Boxplots gezeigte Verteilung der ERM-System-Reifegrade (ERMMA-Score) ergeben. Der fett eingezeichnete Strich beim Wert von 1.33 ist der Median (50%-Quantil) der Verteilung. Bei den beiden Begrenzungen der Fläche auf der linken (rechten) Seite beim Wert von 0.73 (1.95) handelt es sich um das 25%-Quantil (75%-Quantil). Der ganz links stehende Strich kennzeichnet den minimalen Score-Wert von 0.11 und der ganz rechts stehende Kreis zeigt den maximalen Score von 4.67. Die Form des Boxplots zeigt eine Rechtsschiefe an, zumal rechtseitig vom Median eine breitere Streuung als linksseitig vorliegt. Die kleinen Kreise kennzeichnen die Ausreißer. Diese kommen von den großen Unternehmen, welche vielfach hohe Score-Werte haben.

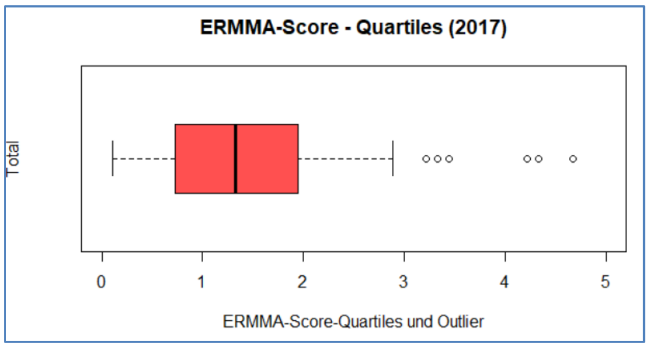

ABBILDUNG 8: ERMMA-SCORES – DESKRIPITVE STATISTIK

Abbildung 9 liefert tiefergehende Einblicke in die Bestandteile des (ERMMA)Scores, dessen Verteilung ganz rechts dargestellt ist. Links davon sind die Score-Verteilungen in den drei Dimensionen zu sehen, u.z. A-, B- und C-Score. Darüber hinaus zeigt die Grafik auch noch die Verteilungen der Scores in den 9 Sub-Dimensionen (A1 bis C3). Dabei zeigen sich interessante Details: Die B1-Sub-Dimension ist die Beste unter allen 9, zumal sie den höchsten Median aufweist. Der Grund dafür dürfte darin liegen, dass die großen Unternehmen häufig ihr Risikomanagementsystem extern prüfen lassen und bei derartigen Prüfungen üblicherweise der Risikomanagement-Prozess besonders eingehend geprüft wird. Die schlechtesten Sub-Dimensionen liegen vor in der Risikoorganisation (A3) und dem Schulungssystem (B2), wobei das erste Quartil jeweils Null beträgt. Dies zeigt Mängel in der organisationalen Umsetzung der ERM Governance und der durch Schulungen bewirkten nachhaltigen Verankerung von ERM-Kompetenzen innerhalb des Unternehmens an.

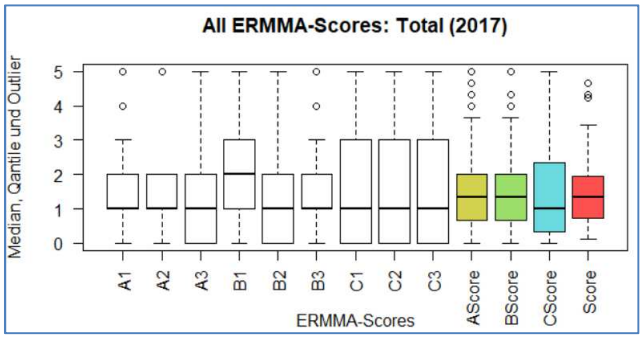

ABBILDUNG 9: (SUB-)DIM. ERMMA-SCORES – DESKRIPTIVE STATISTIKEN

5.3 Explorative Analyse

In der bisherigen deskriptiven Analyse wurde die Verteilung der mit dem ERMMA-Messmodell gemessenen Reifegrade hinsichtlich der Ausgestaltung des progressiv gestuften ERM-System-Konstrukts dargestellt. In der explorativen Analyse werden die Messergebnisse in kausalen Strukturmodellen hinsichtlich ihrer Abhängigkeit von exogenen Variablen (Bestimmungsgrößen) untersucht.

Abbildung 10 zeigt die durchschnittlichen Gesamt-Scores für verschiedene Teilmengen. Der links dargestellte Wert von 1.62 ist der Durchschnittswert über alle teilgenommenen Unternehmen (AUT). Beachtenswert ist, dass der Durchschnittswert von 1.62 aufgrund der Rechtsschiefe der ERMMA-Score-Verteilung höher als der Median von 1.33 ist. Der Durchschnittswert dient als Referenzpunkt zur Bewertung der sich für die verschiedenen Teilmengen ergebenden Werte, welche rechts davon eingezeichnet sind. Dabei zeigt sich, dass sich für Aktiengesellschaften (Joint Stock), Unternehmen mit mehr als 1000 Mitarbeitern (Employees 1000+), Nicht-Eigentümer-geführten Unternehmen (Non Ownership-managed) und für Unternehmen mit 5 und mehrjähriger Tätigkeitsdauer der Internen Revision (Internal Audit), Risikomanagement (RM) und

Compliance Management (CM) deutlich höhere Reifegrade im Vergleich zu ihren jeweiligen Komplementärgruppen ergeben.

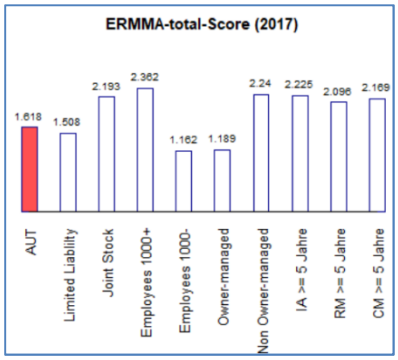

ABBILDUNG 10: ERMMA-SCORES – EXPLORATIVE STATISTIKEN

In Regressionsanalysen hat sich gezeigt, dass alle in Abbildung 10 gezeigten Unterschiede statistisch signifikant sind. Folglich liefert die ERMMA-Studie den empirischen Beleg, dass die Qualität des ERM-Systems in positiv kausaler Beziehung zu folgenden Bestimmungsfaktoren steht, u.z. zur Unternehmensgröße, der Nicht-Eigentümerführung, der Aktiengesellschaft-Rechtsform und der über die Dauer ihrer Existenz gemessenen Qualität der Internen Revision sowie der für das Risiko- und Compliance-Management eingerichteten Institutionen.

6 Konklusion und Ausblick

Im letzten Kapitel dieses Beitrags wurde das Ergebnis der in Österreich durchgeführten Untersuchung hinsichtlich der Reifegrade der in den Unternehmen eingerichteten ERM-System-Ausgestaltungen präsentiert. Der gesamthafte ERMMA-Score, welcher sich durch zweifache Durchschnittsbildung aus den Sub-Dimensions-Scores errechnet, stellt sozusagen die „Spitze des Eisbergs“ dar. Seine Verteilung ist aufgrund der hohen Scores der großen österreichischen Unternehmen rechtsschief.

Bei den Dimensions-Scores zeigt sich eine große Ähnlichkeit der Verteilung bei der ERM Governance (Dimension A) und beim Risikomanagementsystem (Dimension B). Zudem sind beide Verteilungen auch der Verteilung des ERMMA-Scores sehr ähnlich. Bei der Nutzung der Risikoinformation in der risikobasierten Planung und den risikobasierten Steuerungssystemen (Dimension C) zeigt sich aber ein großer Unterschied. Der Median der Dimension C) ist nämlich deutlich niedriger und das 75%-Quantil deutlich höher, was auf mehr Unternehmen mit niedrigeren Score-Werten und einer größeren Rechtsschiefe hindeutet. Insofern liefert die Studie einen statistisch fundierten Beleg dafür, dass die Nutzung der Risikoinformation (C) gegenüber der Generierung der Risikoinformation (B) in der Mehrzahl der Fälle weniger stark ausgeprägt und in die Richtung höherer Reifegrade deutlich mehr streut. D.h., hinsichtlich der Nutzung von Risikoinformationen zeigen sich in Österreichs Unternehmen die größten Unterschiede.

Das Zustandekommen der unterschiedlichen Dimensions-Scores erklärt sich aus den 9 Sub-Dimensions-Scores. Die Verteilungen Sub-Dimensions-Scores der Dimension A) und B) sind sich ähnlich. In beiden Dimensionen gibt es jeweils eine schwächere Sub-Dimension, u.z. die Risikoorganisation (A3) und das Schulungssystem (B2). Eine Besserstellung der Dimension B) zeigt sich im Risikomanagement-Prozess (B1), dessen Verteilung sich aufgrund eines höheren Medians und höheren 75%-Quantils positiv abhebt.

In der explorativen Analyse wurden die Bestimmungsgrößen (exogenen Variablen) für die ERMMA-Scores bestimmt. Zu diesem Zweck war die Vermeidung des Zirkelschlusses wichtig, indem bei der Konzeptionalisierung des ERMMA-Messmodells darauf geachtet wurde, dass die Bestimmungsgrößen im Messmodell nicht als Indikatoren eingehen. Die explorative Analyse lieferte den statistischen Beleg, dass die ERM-System-Reifegrade positiv abhängen von der Unternehmensgröße, dem Umstand, dass die Unternehmen nicht eigentümergeführt sind, die Rechtsform einer Aktiengesellschaft vorliegt und die Interne Revision sowie die für das Risiko- und Compliance-Management eingerichteten Institutionen mindestens 5 Jahre tätig sind.

Neben dem soeben zusammengefassten empirischen Beitrag wurde im ERMMA-Projekt durch die neuartige Online-Messtechnik zum Self Assessment von ERM-System-Reifegraden auch ein wissenschaftlicher Beitrag erzielt. Das in diesem Zusammenhang gesetzte Forschungsziel bestand in der Schließung der in der Literatur vorgefundenen Lücke hinsichtlich einer methodologisch fundierten Konezptionalisierung und Operationalisierung von Reifegradmodellen für ERM-System-Ausgestaltungen. Zur Schließung der Lücke wurde die Methodik des Predictive Validity Framewoks verwendet. Das damit erstellte ERMMA-Messmodell hat einerseits den ERM-Konnex durch dessen Fundierung mit dem Best Practice-Modell in Form des ISO/COSO-ERM-System-Modells, und andererseits ist es durch die Fakten-bezogenen Indikatoren und dichotomen Indikatorvariablen eine objektive, reliable und valide Messmethodik.

Schließlich wurde im ERMMA-Projekt durch die Verfügbarmachung der ERMMA-Online-Applikation als ERMMA-Monitoring-Tool auch ein wertvoller praktischer Beitrag erzielt. Dieses Tool bietet dem an der Studie teilnehmenden Unternehmen die Möglichkeit, anfänglich ihren Reifegrad erstmals zu bestimmen und sodann im Zeitablauf zu monitoren. Somit bietet das Monitoring-Tool eine wichtige Unterstützung für das „Reifegrad-Controlling“, mit welchem anfänglich die Schwachstellen im ERM-System identifiziert und aufgrund der gegebenen Feedback-Informationen konkrete Verbesserungen angestrebt werden können. Im Zeitablauf wird dann mit dem Monitoring-Tool die Entwicklung des Reifegrads gemessen, und bei Abweichungen zwischen den angestrebten und den tatsächlichen Score-Werten können dann die zur Beseitigung eingesetzten Korrektur- bzw. Anpassungsmaßnahmen ergriffen werden.

Aufgrund der großen praktischen Relevanz sowie der umfassenden theoretischen Fundierung hat die Funk Stiftung (Hamburg) ein Folgeprojekt finanziert, in dem die ERMMA-Studie auch auf Deutschland ausgeweitet wird. Zu diesem Zweck gilt es Anpassungen vorzunehmen, um die in Deutschland präziseren Vorschriften hinsichtlich Frühwarnsystem (KonTraG), Risiko-Governance (Gleißner and Wolfrum, 2017) und Unternehmensgröße adäquat einzubinden. Zur Erreichung der adäquaten Einbindung wird auch die Expertise der Risk Management Association (RMA) genutzt, indem das

ERMMA-Messmodell in Kooperation mit der RMA adaptiert und sodann die Befragung durchgeführt wird.

7 Referenzen

Beasley, M. S., Clune, R. and Hermanson, D. R. (2005) 'Enterprise risk management: An empirical analysis of factors associated with the extent of implementation', *Journal of Accounting and Public Policy*, 24(6), pp. 521–531. doi: 10.1016/j.jaccpubpol.2005.10.001.

Bisbe, J., Batista-Foguet, J. M. and Chenhall, R. (2007) 'Defining management accounting constructs: A methodological note on the risks of conceptual misspecification', *Accounting, Organizations and Society*, 32(7–8), pp. 789–820.

Blanchette, S. and Keeler, K. L. (2005) 'Self Assessment and the CMMI-AM - A Guide for Government Program Managers'.

de Bruin, T. *et al.* (2005) 'Understanding the Main Phases of Developing a Maturity Assessment Model', in *16th Australasian Conference on Information Systems*. Sydney.

Cienfuegos, I. (2013) *Developing a Risk Maturity Model for Dutch municipalities Ignacio*. University of Twente.

CMMI (2010) 'CMMI for Development, Version 1.3', *Technical Report, CMU/SEI-2010-TR-033, Carnegie Mellon University*.

COSO-ERM (2017) 'Enterprise Risk Management Integrating with Strategy and Performance', *Committee of Sponsoring Organizations of the Treadway Commission*.

Cuevas, G., Serrano, A. and Serrano, A. (2004) 'Assessment of the requirements management process using a two-stage questionnaire', *Fourth International Conference on Quality Software, 2004. QSIC 2004. Proceedings.*, pp. 110–116. doi: 10.1109/QSIC.2004.1357951.

Damsgaard, J. and Scheepers, R. (1999) 'A stage model of intranet technology implementation and management', *ECIS 1999 Proceedings*, (January 1999), pp. 100–116.

Diamantopoulos, A. and Winklhofer, H. M. (2001) 'Index Construction with Formative Indicators: An Alternative to Scale Development', *Journal of Marketing Research*, 38(2), pp. 269–277.

DIIR-RS2 (2015) 'Prüfung des Risikomanagementsystems durch die Interne Revision (RS Nr. 2). Revisionsstandard, Deutsches Institut für Interne Revision e.V.' Deutsches Institut für Interne Revision e.V.

Doty, D. H. and Glick, W. H. (1994) 'Typologies as a unique form of theory building: Towards improved understanding and modelling', *Academy of Management Review*, 19(2), pp. 230–251. doi: 10.5465/AMR.1994.9410210748.

Edwards, J. R. and Bagozzi, R. P. (2000) 'On the Nature and Direction of Relationships Between Constructs and Measures', *Psychological Methods*, 5(2), pp. 155–174. doi: 10.1037//1082-989X.5.2.

ERMMA-Studie (2017) *Messung und Analyse der ERM-Reifegrade von österreichischen Unternehmen*. Available at: https://www.imw.tuwien.ac.at/fileadmin/t/imw/fc/documents/ERMMA_Studie2017.pdf.

Giere, J., Wirtz, B. W. and Schilke, O. (2006) 'Mehrdimensionale Konstrukte', *Die*

Betriebswirtschaft, 66(2006), pp. 678–695.

Gleißner, W. (2015) 'Controlling und Risikoanalyse bei der Vorbereitung von Top-Management-Entscheidungen', *Controller Magazin (CM)*, pp. 4–12.

Gleißner, W. (2016) 'Reifegradmodelle und Entwicklungsstufen des Risikomanagements: ein Selbsttest', *Controller Magazin (CM)*, (6), pp. 31–36.

Gleißner, W. and Wolfrum, M. (2017) 'Risikotragfähigkeit, Risikotoleranz, Risikoappetit und Risikodeckungspotenzial', *Controller Magazin (CM)*, (6), pp. 77–84.

Hillson, D. (1997) 'Towards a Risk Maturity Model', *The International Journal of Project and Risk Management*, 1(1), pp. 33–45.

Humphrey, W. S. (1988) 'Characterizing the Software Process: A Maturity Framework', *IEEE Software*, 5(2), pp. 73–79.

IDW-PS981 (2017) 'Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW 981). Prüfungsstandard, Institut der Wirtschaftsprüfer in Deutschland e.V.' Institut der Wirtschaftsprüfer in Deutschland e.V.

IIA-3LoD (2013) 'The three lines of defense in effective risk management and control. Position Paper, Institute of Internal Auditors'.

ISO-RM (2011) 'Risikomanagement – Grundsätze und Leitlinien (ISO 31000:2009)'. DIN/ISO.

Jöreskog, K. G. and Sörbom, D. (1993) *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Chicago, IL, US: Scientific Software International.

Lundqvist, S. A. (2015) 'Why firms implement risk governance - Stepping beyond traditional risk management to enterprise risk management', *Journal of Accounting and Public Policy*. Elsevier Inc., 34(5), pp. 441–466. doi: 10.1016/j.jaccpubpol.2015.05.002.

MacKenzie, S. B., Podsakoff, P. M. and Podsakoff, N. P. (2011) 'Construct Measurement and Validation Procedures in MIS and Behavioral Research : Integrating New and Existing Techniques', *MIS Quarterly*, 35(2), pp. 293–334. doi: 10.2307/23044045.

Mikes, A. and Kaplan, R. R. S. (2014) *Towards a Contingency Theory of Enterprise Risk Management*, *Harvard Business School*. 13-063. Boston.

Monda, B. and Giorgino, M. (2013) 'An Enterprise Risk Management maturity model', in *Enterprise Risk Management Symposium*.

Pastor, O. *et al.* (2008) 'Model-driven development', *Informatik-Spektrum*, 31(5), pp. 394–407. doi: 10.1007/s00287-008-0275-8.

Petter, Straub and Rai (2007) 'Specifying Formative Constructs in Information Systems Research', *MIS Quarterly*, 31(4), p. 623. doi: 10.2307/25148814.

Schwaiger, W. S. A. (2001) *Finanzwirtschaftlich basierte Unternehmenssteuerung*. Wiesbaden: Deutscher Universitätsverlag.

Simons, R. (1995) *Levers of Control*, *Harvard Business School Press*. Boston: Harvard Business School Press.

Stubbart, C. and Smalley, R. (1999) 'The deceptive allure of stage models of strategic processes', *Journal of management inquiry*, 8, pp. 273–286. doi: 0803973233.

Vanini, U. (2016) 'Reifegrade der Integration von Risikomanagement und Controlling', *Controller Magazin (CM)*, (6), pp. 169–182.

Yucalar, F. and Erdogan, S. Z. (2009) 'A Questionnaire Based Method for CMMI Level 2', *Journal of Aeronautics and Space Technologies*, 4(2), pp. 39–46.

Zubrow, D. *et al.* (1994) 'Maturity Questionnaire', *Special Report, CMU/SEI-94-SR-7, Carnegie Mellon University: Software Engineering Institute*. Carnegie Mellon University (CMU)/Software Engineering Institute (SEI), pp. 1–57.