TECHNISCHE UNIVERSITÄT WIEN

Diplomarbeit

Verbesserung des Enterprise Risk Managements: Theoretische Fundierung und praktische Umsetzung

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

Diplom-Ingenieurs (Dipl. Ing. oder DI)

eingereicht an der TU Wien, Fakultät für Maschinenwesen und Betriebswissenschaften

von

Philipp DIBELKA

Mat.Nr.: 0965787

unter der Leitung von

Univ.Prof. Mag.rer.soc.oec. Dr.rer.soc.oec. Walter SCHWAIGER, MBA

Institut für Managementwissenschaften, E330

Arbeitsbereich Finanzwirtschaft und Controlling

Wien, 16. März 2019

Ich nehme zur Kenntnis, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

Diplomarbeit

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass die vorliegende Arbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen von mir selbstständig erstellt wurde. Alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur, sind in dieser Arbeit genannt und aufgelistet. Die aus den Quellen wörtlich entnommenen Stellen, sind als solche kenntlich gemacht.

Das Thema dieser Arbeit wurde von mir bisher weder im In- noch Ausland einer Beurteilerin/einem Beurteiler zur Begutachtung in irgendeiner Form als Prüfungsarbeit vorgelegt. Diese Arbeit stimmt mit der von den Begutachterinnen/Begutachtern beurteilten Arbeit überein.

Wien, 16. März 2019 _____

Unterschrift

Danksagung

Ich möchte allen Personen, die mich während meines Studiums und nun bei der Erstellung dieser Masterarbeit unterstützt haben, meine größte Dankbarkeit entgegenbringen.

Zuerst möchte ich mich bei Herrn Univ.Prof. Mag. Dr. Walter Schwaiger, der meine Arbeit betreut hat, herzlich bedanken. Schon bei der Auswahl des Themas stand er mir zur Seite und war von Beginn an sehr interessiert. Wir hatten viele interessante und auch lustige Gespräche und Diskussionen zum Thema Risikomanagement, seine umfangreiche Fachkompetenz, sowie seine Geduld und Hilfsbereitschaft, waren mir eine große Unterstützung. Im Zuge meines Studiums habe ich viele Lehrveranstaltungen bei Herrn Prof. Schwaiger absolviert und unter anderem auf dem Gebiet des Risikomanagements mein Wissen vertieft.

Weiters bedanke ich mich bei dem nicht namentlich genannten Risikomanager des Unternehmens, an das die Industrie-EWF angelehnt wurde. Er war sehr interessiert, betreute mich sehr gut und gewissenhaft und brachte mir auch vieles aus außerhalb des Risikomanagements bei. Danke auch an die Geschäftsführung, die diese Arbeit überhaupt erst ermöglichte und an meine zahlreichen Gesprächs- bzw. Interviewpartner.

Der größte Dank gebührt meinen Eltern Eva und Peter, die mir stets während des gesamten Studiums zur Seite standen und mich unterstützten. Auch wenn es einmal schleppend voranging, brachten sie mir Verständnis und Vertrauen, aber auch Freiraum entgegen.

Vielen Dank auch an meine Freundin Ella, die mich vor allem in den entscheidenden Phasen meines Bachelors und Masters motivierte und mir mit großer Hingabe ihre Unterstützung entgegenbrachte.

Kurzfassung

Im Zuge dieser Masterarbeit soll das bestehende Risikomanagement-System der an ein reales Unternehmen angelehnten Industrie-EWF analysiert werden. Mit Hilfe des ERMMA-Messmodells (ein intelligenter Fragebogen), das auf der ISO/COSO-Definition von „Enterprise Risk Management“ basiert, sowie zahlreicher Gespräche und Interviews, werden die einzelnen RM-Funktionen in Reifegrade (von 1 bis 5) eingeteilt. Anhand dieser Bewertung werden die zu verbessernden RM-Bereiche ausgewählt.

Ausgehend vom aktuellen Stand wird ein Konzept für ein unternehmensweites Risikomanagement-System modelliert, das auf der Optimierung des RM-Prozesses selbst, dessen Organisation, der Erhöhung des Risikoverständnisses durch Schulungen und der Integration von Risiko in die Unternehmensstrategie basiert. Die Umsetzung dieser Verbesserungen ermöglicht es der Industrie-EWF, das Bewusstsein für Risiko in allen Hierarchieebenen zu verschärfen, potentielle Fehlerquellen zu minimieren und einen unternehmensweiten Überblick über die auftretenden Risiken zu erhalten.

Abstract

In the process of this master thesis, the existing risk management system of Industrie-EWF, which is based on a real company, is to be analyzed. With the help of the ERMMA measurement model (an intelligent questionnaire), which is based on the ISO/COSO definition of "Enterprise Risk Management", as well as numerous discussions and interviews, the individual RM functions are divided into maturity levels (from 1 to 5). On the basis of this evaluation, the RM areas to be improved are selected.

Based on the current status, a concept for a company-wide risk management system is modelled, which is based on the optimization of the RM process itself, its organization, the increase of risk understanding through training and the integration of risk into the company strategy. The implementation of this concept enables Industrie-EWF to increase awareness of risk at all hierarchical levels, to minimize potential sources of error and to obtain a company-wide overview of the risks that arise.

Inhaltsverzeichnis

1 Einleitung

Problemstellung

In der Industrie-EWF[1] wurde vor wenigen Jahren mit der Einführung eines Risikomanagement-Systems begonnen. In einzelnen Bereichen (z.B. in der Produktion) wird dies schon sehr gut umgesetzt, in anderen jedoch noch nicht. Bisher herrscht eine Silo-Betrachtung von Risiken vor, die durch Verbesserungen auf Prozess- und Organisationsebene in ein ERM[2]-System umgestaltet werden soll.

Das inkludiert B) die Identifikation und Messung (Generierung von Risikoinformationen) verschiedener Risiken, C) deren Steuerung (Verwendung von Risikoinformationen) in isolierten Managementsystemen (isolierte Steuerung) bzw. in traditionellen Managementsystemen (integrierte Steuerung). Diese Systeme sollen um den Aspekt des Risikos erweitert werden. Um einen systematischen Ablauf der Aktivitäten zu gewährleisten, bedarf es außerdem A) eines „Master Minds“ in Form einer ERM-Governance. Die Kennzeichnung der ERM-Bestandteile durch Buchstaben bedeutet, dass die ERM-Governance konzeptionell über der Informationsgenerierung und deren Verwendung steht [Schwaiger, Brandstätter, 2019, S. 2].

Vor allem der RM-Prozess (B), das Risikoverständnis sowie die Risikoorganisation und die Risikostrategie (alle drei A) sollen im Zuge der Verbesserung des ERM-Systems optimiert werden, da in ihnen das größte Potential steckt.

[1] An ein reales Unternehmen angelehntes Beispiel (EWF = eine wirkliche Firma)
[2] Enterprise Risk Management → unternehmensweites Risikomanagement

Forschungsmethode

Die Basis für diese Arbeit bildet das „Action Research Model“ (AR-Modell). Das AR-Modell besteht aus vier zyklischen Schritten, denen ein zusätzlicher Schritt vorangestellt ist, nämlich die Diagnose, die das Problem zu Beginn erfasst und den IST-Zustand darstellt. Der Forscher und der Praktiker (in diesem Fall der Verfasser dieser Arbeit und der Risikomanager) arbeiten eng zusammen, um gemeinsam das Problem zu identifizieren und Lösungsvorschläge erarbeiten zu können [French, 2009, S. 191-193]. In der folgenden Abbildung findet sich eine Darstellung dieses Prozesses:

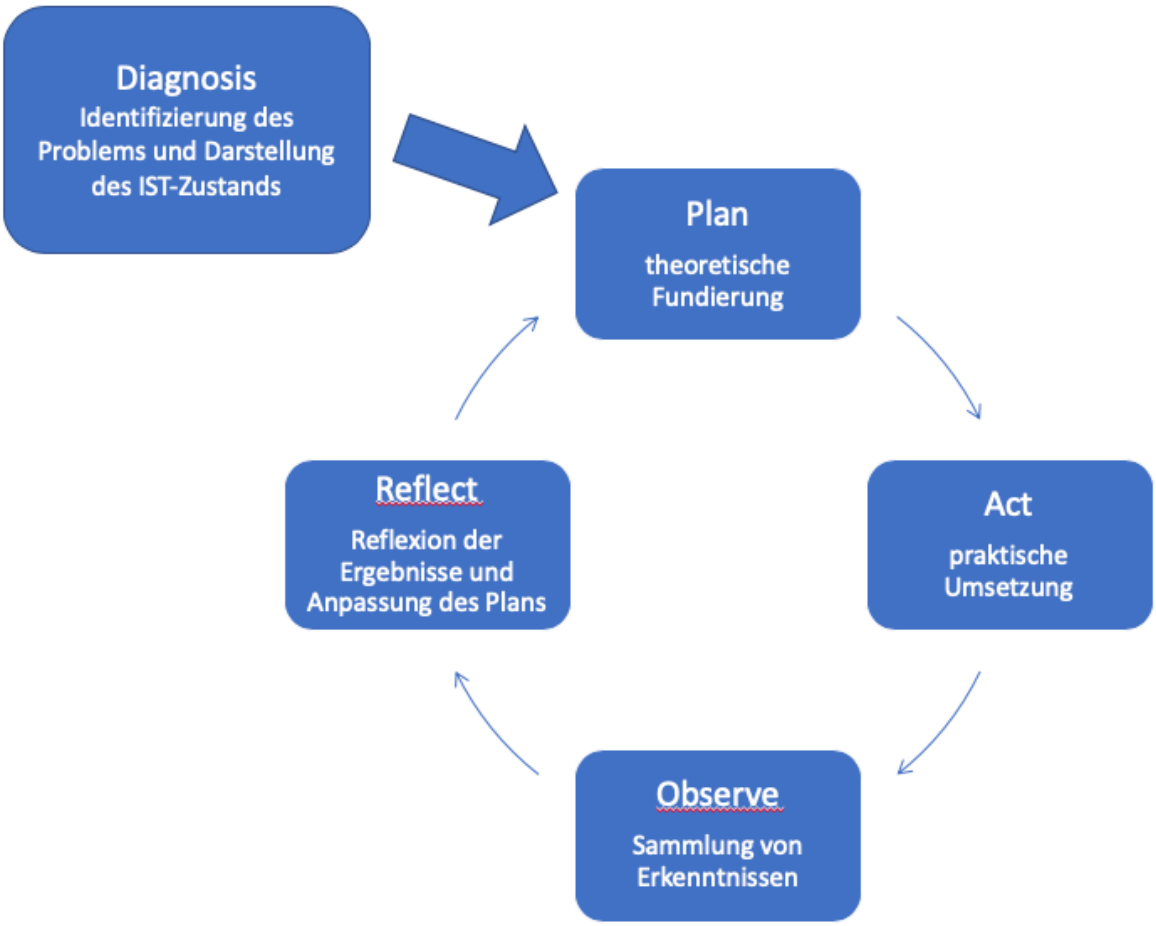


Abbildung 1: Action research model, eigene Darstellung nach Quelle: [French, 2009, S. 193]

Zu Beginn, im vorangestellten Schritt der **Diagnose**, wird das Problem identifiziert und der IST-Zustand dargestellt. In dieser Arbeit geschieht dies mit Hilfe des ERMMA[3]-Messmodells, das die einzelnen RM-Funktionen analysiert und deren Stärken und Schwächen aufzeigt.

[3] Enterprise Risk Management Maturity Assessment

Zusätzlich werden Gespräche und Interviews geführt und zahlreiche Dokumente gesichtet, um einerseits die Ergebnisse des ERMMA-Modells zu validieren und andererseits die Darstellung des IST-Zustands möglichst detailliert durchführen zu können. Diese Erkenntnisse bilden bereits die Basis für den AR-Zyklus, da hier auch (unter Einbeziehung des Risikomanagers) festgelegt wird, welche RM-Funktionen verbessert werden sollen.

Im ersten Schritt des Zyklus wird die **Planung** durchgeführt, also eine theoretische Fundierung der jeweiligen RM-Funktion. Mit Hilfe von Modellen aus Büchern, Zeitschriften, Normen, etc. werden die theoretischen Aspekte aufgezeigt und so eine Basis für den nächsten Schritt gebildet.

Nach der Planung folgt das **Handeln**, welches die praktische Umsetzung der zuvor beschriebenen theoretischen Inhalte beinhaltet. Nach Absprache mit dem Risikomanager über die Vorgehensweise und dem Austausch von Informationen wird das gewonnene Wissen aus der Theorie praktisch umgesetzt.

Der dritte Schritt im Kreislauf ist die **Beobachtung** und Sammlung von Erkenntnissen aus dem Handlungsprozess. So können die Ergebnisse evaluiert werden und Abweichungen festgestellt werden. So wird die Basis für die Reflexion geschaffen [French, 2009, S. 194].

Die **Reflexion** der Ergebnisse ist der letzte Schritt im Zyklus des AR-Modells. In dieser Phase kann eine Anpassung der restlichen Schritte durchgeführt werden, damit sie im neuerlichen Durchlauf des Zyklus den gesamten Prozess wieder vorantreiben und verbessern [French, 2009, S. 194].

Im Zuge dieser Arbeit wird das Problem diagnostiziert, ein Plan für die Durchführung mit Hilfe der theoretischen Fundierung erstellt, welcher dann in der Handlungsphase in die Praxis umgesetzt wird.

Die letzten beiden Schritte des AR-Modells, die Beobachtung und Reflexion, werden erst nach der Fertigstellung dieser Arbeit durchgeführt, wenn klar ist, zu welchen Ergebnissen und Veränderungen die Implementierungen der empfohlenen Verbesserungen geführt haben.

Zusammenfassend werden also folgende Forschungsmethoden in dieser Arbeit verwendet:

- Action-Research-Modell als Grundgerüst und -struktur für die Durchführung der Arbeit
- ERMMA-Messmodell, Gespräche und Interviews zur Identifizierung des Problems und möglichst genauen Darstellung des IST-Zustands
- Literaturrecherche als theoretische Fundierung für die Optimierungsempfehlungen

Erwartete Ergebnisse

Die Erwartung an diese Arbeit ist, mit Hilfe von Fachliteratur Empfehlungen für die Verbesserung der RM-Funktionen RM-Prozess, Risikoverständnis, RM-Schulung, Risikoorganisation und Risikostrategie zu entwickeln, welche den Reifegrad der einzelnen Funktionen erhöhen und die Basis für die Verbesserung des ERM-Systems bilden. Besonders die Standardisierung des RM-Prozesses und die Aggregation der Risiken beim Risikomanager soll einen großen Mehrwert für die Industrie-EWF bringen. Es wird erwartet, dass die Implementierung der empfohlenen Maßnahmen innerhalb von 1-3 Jahren durchgeführt werden kann. Der Gesamt-Reifegrad soll sich um mindestens eine Stufe erhöhen.

Vorstellung der Industrie-EWF

Die Industrie-EWF ist ein fiktives Familien-Industrieunternehmen, das an ein reales Unternehmen angelehnt ist.

Das Hauptgeschäft der Industrie-EWF besteht in der Entwicklung und Herstellung von Produkten, die in verschiedenste Branchen verkauft werden. Dabei wird jährlich mit über 2.500 Mitarbeitern ein Unternehmensumsatz von über 500 Mio. Euro erwirtschaftet. Auch in der Automobilbranche ist die Industrie-EWF fest verankert, was verschärfte Bedingungen mit sich bringt. Einerseits gilt es, viele Zertifizierungen und Normen zu erfüllen, andererseits sind Toleranzen bei der Herstellung viel genauer. Auch die Zusammenarbeit mit den Kunden ist im Automobilbereich speziell, weil man sehr oft in Kontakt steht.

Eigenheiten eines Familienunternehmens

Grundsätzlich lässt sich bei eigentümergeführten Familienunternehmen nicht sagen, dass es klar definierte Unterschiede zu anderen Unternehmen gibt (außer natürlich die Führung durch Eigentümer).

Aus Gesprächen mit Mitarbeitern der Industrie-EWF ergaben sich jedoch einige Eigenheiten, die hier aufgeführt werden:

1. *Langfristiges Denken über Generationen hinweg* – dieses Vorgehen spiegelt sich in mehreren Unternehmensbereichen wider:
    a. Es wird nach einer langfristigen Strategie gehandelt. In managergeführten Unternehmen kann es passieren, dass Topmanager mit 5-Jahres-Verträgen auch nur 5 Jahre in die Zukunft denken. Nach dieser Zeit können jedoch durchaus Probleme sichtbar werden, die aus diesem kurzfristigen Denken entstanden sind. In der Industrie-EWF wird weiter in die Zukunft gedacht, was zur Folge hat, dass auch Mitglieder der obersten Führungsebenen länger im Unternehmen bleiben.
    b. Die langfristige Bindung von Mitarbeitern führt auch dazu, dass über Jahrzehnte angehäuftes Wissen im Unternehmen bleibt und an die nächste Generation weitergegeben wird. Um Mitarbeiter dazu zu motivieren, möglichst ihr gesamtes Arbeitsleben in der Industrie-EWF zu verbringen, werden hohe soziale Standards und eine starke Bindung und Affinität der Menschen zum Unternehmen gelebt.

2. *Einstellung zu Risiko*: Die Eigentümer der Industrie-EWF handeln sehr risikoavers. Es werden keine größeren Risiken eingegangen, sondern der Fokus auf die Kernkompetenz – die Entwicklung und Herstellung von Industrieprodukten – gelegt. Neue Geschäftsbereiche und Innovationen werden zwar laufend erschlossen, jedoch nie, wenn der Ausgang ungewiss ist.
3. *Familiärer Umgang*: Durch die langfristige Bindung der Mitarbeiter entstand in der Industrie-EWF ein sehr familiärer Umgang und ein sehr gutes Miteinander. Das spiegelt sich z.B. im Umgangston wider – jeder ist „per Du“. Außerdem werden viele Aktivitäten gemeinsam unternommen, an denen auch die Geschäftsführung teilnimmt.

2 ERMMA-Messmodell: Theoretische Grundlagen und Anwendung in Industrie-EWF

2.1 ERMMA: Theoretische Grundlagen

2.1.1 Enterprise Risk Management in der Theorie

Die Grundstruktur für das ERMMA-Modell kommt aus dem ISO/COSO-ERM-System-Modell, das auf dem ISO-RM-Standard und dem COSO-ERM-Framework aufbaut. In der folgenden Abbildung wird diese Grundstruktur dargestellt:

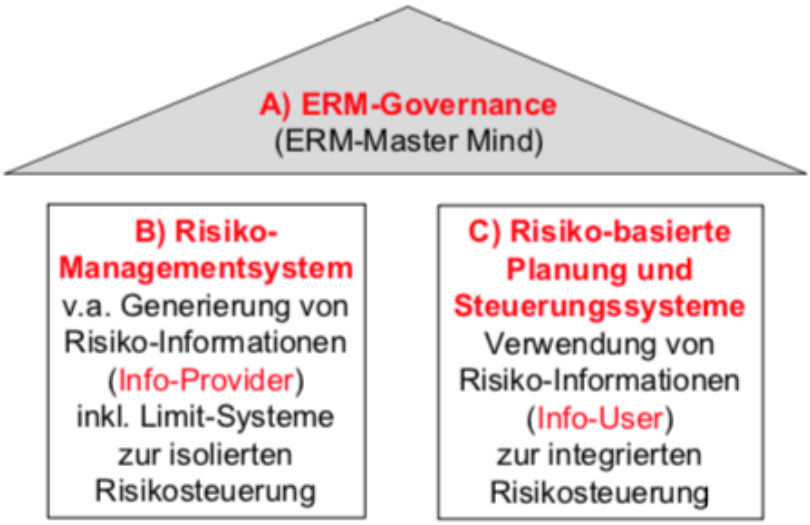


Abbildung 2: Grundstruktur des ISO/COSO-ERM-System-Modells, Quelle: [Schwaiger et al., 2019, S. 5]

Die in der ISO 31000:2009 beschriebenen Standards[4] werden um die Forderung ergänzt, dass die Risikosteuerung sich nicht auf einzelne isolierte Management-Bereiche beschränken, sondern auch in die bereits vorhandenen Planungs- und Steuerungssysteme integriert werden soll [Schwaiger et al., 2019, S. 5].

[4] Anmerkung: In dieser Norm setzt sich der RM-Prozess aus der Risikobeurteilung (Identifikation, Analyse, Bewertung) und der Risikobewältigung zusammen. Die Risikobewertung sollte jedoch gemeinsam mit der Risikobewältigung Teil der Risikosteuerung sein [Schwaiger et al., 2019, S. 4-5].

Das Risikomanagement-System, also die linke Säule, deckt sich weitgehend mit dem ISO-Verständnis des RM-Prozesses, während die rechte Säule und das aufgesetzte „Dach“ die Verbindung zum COSO-ERM-Framework (2017), welches die folgenden Spezifikationen enthält, herstellt [Schwaiger et al., 2019, S. 6]:

1. Die ausdrückliche Erwähnung der Risikobasiertheit der Planung- und Steuerung bedeutet eine gemeinsame Betrachtung von Wertschöpfung und Risiko.
2. Die ERM-Governance stellt eine eigenständige Komponente dar: Während die Risikopolitik die Bedeutung und Aufsichtsverantwortung für das Risikomanagement im Unternehmen festlegt, stellt die Risikokultur ethische Werte, Verhaltensweisen und das Verständnis von Risiko dar [COSO, 2017, S. 6].
3. Die organisationale Struktur wird stark an das 3-Lines-Of-Defense-Modell [IIA, 2013] angelehnt.

2.1.2 Aufbau des Fragebogens

Um den IST-Zustand des Risikomanagements zu analysieren und sich einen Überblick verschaffen zu können, wurde mit der Industrie-EWF der vom Institut für Managementwissenschaften (IMW) der TU Wien entwickelte ERMMA-Reifegradtest durchgeführt.

Dieser Test ist ein intelligenter Fragebogen, der sich durch folgende Besonderheiten von klassischen Fragebögen abhebt [Schwaiger et al., 2019, S. 2-3]:

- Die gestellten Fragen werden nicht ad hoc formuliert, sondern mit Hilfe des Predictive Validity Frameworks (PVF)[5] deduktiv für die verschiedenen Formen von ERM-Systemen aus explizit über beobachtbare Indikatoren modellierten Konstrukten abgeleitet.
- Mit den Fragen wird anhand von zweiteiligen (dichotomen) Ja/Nein-Antwortmöglichkeiten das Vorliegen der Indikatoren, die den fünf Reifegraden von ERM-Systemen zugeteilt sind, gemessen.
- Die Indikatoren sind konsekutiv angeordnet. Sie spiegeln die progressiven Reifegradstufen wider. Es werden also nur solange Fragen gestellt, solange die Voraussetzungen für die folgenden Reifegrade erfüllt werden.

[5] Siehe [Bisbe, Batista-Fouget, Chenhall, 2007, S. 812-814]

- Der Fragebogen kann regelmäßig wiederholt werden, um die Entwicklung der Reifegrade zu überprüfen.

Die Intelligenz des Fragebogens besteht also darin, Fragen an zuvor gegebene Antworten anzupassen. So erhält jedes Unternehmen, das den Test durchführt, einen zugeschnittenen Fragebogen. Die Fragen orientieren sich zu Beginn am ersten von fünf Reifegraden. Das bedeutet, dass zuerst überprüft wird, ob Reifegrad 1 erreicht wurde, erst danach werden Fragen zu Reifegrad 2 gestellt. Genauso verhält es sich in der Folge mit höheren Reifegraden. Der Fragebogen wird also länger, wenn in den einzelnen Bereichen ein hoher Reifegrad erreicht wird.

2.1.3 Erklärung des Reifegradmodells

Das Reifegradmodell des ERMMA-Fragebogens orientiert sich an dem 4-stufigen Risk Maturity Model (RMM) von Hillson (1997). Dieses Modell wiederum basiert auf dem von Humphrey (1988) entwickelten sogenannten Capability Maturity Model (CMM) aus der Software-Entwicklung. Im CMM sind die folgenden fünf konsekutiven Reifegrade definiert [Schwaiger et al., 2019, S. 6-7]:

1. Initial – Prozesse sind gar nicht oder nur vereinzelt definiert.
2. Repeatable – Prozesse unterliegen einem einfachen Monitoring.
3. Defined – Prozesse sind unternehmensweit definiert.
4. Managed – Prozesse werden mit quantitativen Kennzahlen gesteuert.
5. Optimizing – Prozesse unterliegen einem kontinuierlichen Verbesserungsprozess.

Das Klassifikationsschema der Reifegrade wird für den ERMMA-Reifegradtest an das Risikomanagement angepasst und im Artikel „Wie reif ist das Enterprise Risk-Management Ihres Unternehmens?“ [Schwaiger, 2017] ausführlich beschrieben. Dabei wurden drei Dimensionen mit jeweils drei Subdimensionen (basierend auf ausführlicher Literaturrecherche) definiert. Für jede Dimension bzw. Subdimension gibt es fünf Reifegrade, die den Fortschritt eines Unternehmens in der jeweiligen Risikomanagement-Funktion beschreiben. In der Praxis existiert auch noch ein sechster Reifegrad (Reifegrad 0), der jedoch nur aussagt, dass in dem Bereich die Voraussetzungen für Reifegrad 1 nocht nicht erreicht wurden.

In der folgenden Tabelle befindet sich eine Erklärung der Dimensionen mit ihren Subdimensionen und einer kurzen Beschreibung der Reifegrade:

Dimension	Sub-Dim.	Reifegrade				
		RG 1	**RG 2**	**RG 3**	**RG 4**	**RG 5**
A: ERM-Governance	A1: Risiko-strategie A2: Risiko-verständnis A3: Risiko-organisation	Prozess-Per-spektive in partiellen Bereichen (Silo-Sicht)	Prozess-Perspektive inkl. Prüfung und Management (single loop)	Unternehmensweite (holistische) Perspektive	Unternehmens-übergreifende (corporate) Perspektive (double loop)	Vom Top-Manage-ment interaktiv gemanagte Systeme
B: Risiko-Management-system	B1: RM-Prozess B2: RM-Schulungssystem B3: RM-Informations-system	Risikomgt.-Prozess	Risikomanagement-System (single loop)	Unternehmens-weites Risikomanagement-System	Unternehmens-übergreifendes Risikomanagement-System (double loop)	
C: Risiko-basierte Planungs- und Steuerungs-systeme	C1: Strategisches Management C2: Finanzielles Management C3: Operatives Management	Risiko-Limit Systeme	Key-Risk-basierte Planung (inkl. Strategie- bzw Zielfestlegung	Key-Risk-basierte Steuerungssysteme (z.B. Performance-Management)	Management-Systeme mit risiko-adjustierten Performance-Kennzahlen	

Tabelle 1: ERMMA-Klassifikationsschema, eigene Darstellung nach Quelle: [Schwaiger, Hilscher, Brandstätter, 2017, S. 181]

Die drei Dimensionen stellen die Generierung von Risikoinformationen (B), deren Nutzung (C) sowie die über diesen beiden Dimensionen stehende Governance (A) – das „Master Mind" – dar. Da diese Dimensionen nicht direkt gemessen werden können, werden die bereits erwähnten Indikatoren mit bestimmten Antworten zu Fragen im Fragebogen verknüpft. Werden diese Antworten angekreuzt, sieht das System die dazugehörigen Indikatoren als erfüllt an. Da zu jedem Reifegrad mehrere Indikatoren gehören, führt am Ende eine Kombination der erfüllten Indikatoren zu dem jeweiligen Reifegrad in den einzelnen Subdimensionen.

Der Nachteil des ERMMA-Reifegradtests besteht darin, dass aufgrund der Abstimmung des Tests keine Antworten rückgängig gemacht werden können, also nicht zurückgegangen

werden kann. Besteht im Nachhinein der Verdacht, dass einzelne Fragen falsch oder ungenau beantwortet wurden, muss der Test also nochmals durchgeführt werden.

2.2 ERMMA: Anwendung in Industrie-EWF

2.2.1 Ergebnisse für Industrie-EWF

Im Falle der Industrie-EWF wurden die Fragen vom Leiter des „Strategic Performance Managements“ beantwortet, der direkt der Geschäftsführung (GF) unterstellt ist und im Unternehmen der Hauptverantwortliche für das Risikomanagement ist.

Nach Beantwortung aller Fragen wird eine 9-seitige PDF-Datei (ERMMA-Report) mit den Ergebnissen des ERMMA-Reifegradtests erstellt. Darin befinden sich sämtliche Fragen (inklusive Antworten), die den jeweiligen Reifegrad bestimmt haben. Außerdem eine Liste mit allen Subdimensionen, dem erreichten Inhalt und dem ausstehenden Inhalt, mit dem der nächsthöhere Reifegrad erreicht werden würde. Die Ergebnisse des Tests (vor allem die Reifegrade jener Dimensionen, die verbessert werden sollen) werden ausführlich besprochen, um sicherzustellen, dass die Ergebnisse auch wirklich den IST-Zustand widerspiegeln.

Im Fall des Unternehmens liegt der ERMMA-Gesamt-Score bei 1,34. Das Ergebnis wird in Abbildung 1 dargestellt. Damit nimmt es den relativen Rang 48 / 100 ein. Der relative Rang bedeutet, dass 47% der betrachteten Unternehmen ein besseres und 51% ein schlechteres Ergebnis haben.

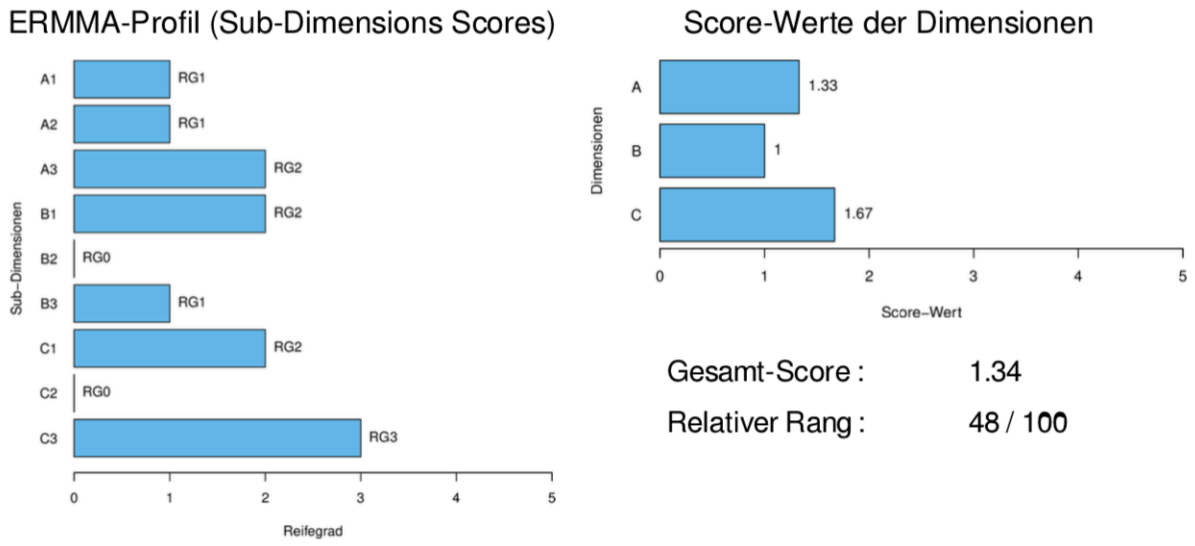


Abbildung 3: Ergebnis des ERMMA-Reifegradtests

Der Gesamt-Score von 1,34 errechnet sich aus dem Durchschnitt der erreichten Werte in den drei Dimensionen A, B und C, wobei die Dimensionen alle gleich gewichtet sind. Die Ergebnisse

der drei Dimensionen ergeben sich wiederrum aus dem Durchschnitt der in den Subdimensionen erreichten Werte.

In Dimension A, der „ERM-Governance“, wurde ein Score von 1,33 erreicht, in Dimension B, dem „Risikomanagementsystem“, ein Score von 1 und in Dimension C, den „risikobasierten Planungs- und Steuerungssystemen“ ein Score von 1,67. Die unterschiedlichen Werte in den einzelnen Dimensionen zeigen, dass beispielsweise die Generierung von Risikoinformationen (Dimension B) noch einen niedrigeren Reifegrad aufweist als deren Nutzung in den Planungs- und Steuerungssystemen (Dimension C).

Im ERMMA-Report wird nun für jede der drei Hauptdimensionen angeführt, welcher Reifegrad (durch welche Inhalte) bereits erreicht wurde. Weiters beinhaltet er den ausstehenden Inhalt für den nächsthöheren Reifegrad. In den folgenden Abbildungen befinden sich diese Beschreibungen.

Begonnen wird mit **Dimension B**, der **Generierung der Risikoinformationen**.

Sub-Dimension	Erreichter Reifegrad	Erreichter Inhalt	Ausstehender Inhalt für höheren Reifegrad
B1 : RM-Prozess	**RG2**	In ausgewählten Unternehmensbereichen ist ein Risikomanagement-Prozess (Identifikation, Messung, Bewertung und Steuerung von Risiken) implementiert, inkl. Monitoring und Prüfung	In allen wichtigen Unternehmensbereichen ist ein unternehmensweit koordinierter Risikomanagement-Prozess (Identifikation, Messung, Bewertung und Steuerung von Risiken) implementiert, inkl. Monitoring und Prüfung
B2 : RM-Schulungssystem	**RG0**	Schulungs- bzw. Fortbildungsaktivitäten hinsichtlich des Risikomanagements sind nicht ausreichend, um einen positiven Reifegrad zu erreichen	Die Verantwortlichen für den Risikomanagement-Prozess (z.B. Risikomanager) bilden sich weiter hinsichtlich einer angemessenen Funktionsweise des Risikomanagement-Prozesses und die Verantwortlichen (z.B. operative Belegschaft als Risikoeigener) für die Steuerung von operativen Risiken werden hinsichtlich der Steuerung ihrer jeweiligen Risiken geschult
B3 : RM-Informationssystem	**RG1**	Risikomanagement-Prozesse werden softwaremäßig (z.B. MS Excel) zumindest in ausgewählten Unternehmensbereichen unterstützt	Die softwaremäßige Unterstützung von Risikomanagement-Prozessen wird zumindest in ausgewählten Unternehmensbereichen überwacht und bei Bedarf angepasst, sowie hinsichtlich der Angemessenheit und Wirksamkeit überprüft.

Abbildung 4: ERMMA-Feedback Dimension B

Man kann erkennen, dass der Gesamt-Score von 1 in Dimension B vor allem dem niedrigen Reifegrad in B2 geschuldet ist. Reifegrad 0 bedeutet, dass kein RM-Schulungssystem existiert. Um einen höheren Reifegrad zu erreichen, muss sich einerseits der Risikomanager

weiterbilden, andererseits müssen die „Risk Owner“ (beispielsweise der Prozessverantwortliche auf operativer Ebene) bezüglich der Steuerung ihrer Risiken geschult werden. Auf Grund der Affinität des Risikomanagers zu Innovationen und neuen Konzepten bzw. Aufgaben hat er sich bereits gut informiert und auch selbst weitergebildet.

In Dimension B3, dem Informationssystem, wurde ein Reifegrad von 1 erreicht. Das bedeutet, dass Risikomanagement-Prozesse in dem unternehmenseigenen IT-System dargestellt werden und auch anderwärtig softwaremäßig (MS-Excel) unterstützt werden. Um höhere Reifegrade erreichen zu können, müssen alle Unternehmensbereiche einbezogen werden, außerdem muss das RM-Informationssystem von der Internen Revision (IR) auf Angemessenheit und Vollständigkeit überprüft werden.

Der RM-Prozess (Dimension B1) hat bereits den Reifegrad 2 erreicht. In bestimmten Unternehmensbereichen werden Risiken identifiziert, gemessen, bewertet und gesteuert. Vor allem im operativen Bereich existiert bereits ein detaillierter Risikomanagement-Prozess, der auch überprüft bzw. überwacht wird. Wird dieser Prozess noch besser unternehmensweit durchgeführt und koordiniert, können hier schnell höhere Reifegrade erreicht werden.

In der folgenden Abbildung ist das Ergebnis des ERMMA-Tests in **Dimension C**, den **risikobasierten Planungs- und Steuerungssystemen**, ersichtlich.

Sub-Dimension	Erreichter Reifegrad	Erreichter Inhalt	Ausstehender Inhalt für höheren Reifegrad
C1 : Strategisches Management-System	**RG2**	✓ Im strategischen Management werden – im Risikomanagement-Prozess identifizierte und gemessene – Key Risks bei der Planung oder der Strategie- bzw. Zielfestlegung einbezogen, sowie neben Risiken auch Chancen betrachtet	✗ Im strategischen Management werden im Risikomanagement-Prozess identifizierte und gemessene Key Risks gesteuert
C2 : Finanzielles Performance-Management-System	**RG0**	Finanzielle Entscheidungen basieren nicht auf Risikoinformationen und orientieren sich nicht an definierten Risiko-Limits	✗ Einzelne, im Risikomanagement-Prozess identifizierte und gemessene Risiken werden im Finanz- und Erfolgsmanagement anhand von Risiko-Limiten gesteuert
C3 : Operatives Prozess-Management-System	**RG3**	✓ Im operativen Management werden im Risikomanagement-Prozess identifizierte und gemessene Key Risks gesteuert	✗ Im operativen Management werden risikoadjustierte Performance-Kennzahlen (z.B. Six-Sigma-Qualitätsziele) verwendet

Abbildung 5: ERMMA-Feedback Dimension C

Auch hier findet sich eine Subdimension mit Reifegrad 0 – das finanzielle Performance-Management. Diese Einschätzung wurde allerdings im Nachhinein korrigiert, da sehr wohl

Risiko-Limits verwendet werden. Im finanziellen Performance-Management wurde also ein Reifegrad von 1 erreicht. In einem Unternehmen in der Größe der Industrie-EWF würde man erwarten, dass diverse finanzielle Risiken (Kreditrisiken, Währungsrisiken) auftreten. Dies ist jedoch aus den folgenden Gründen nicht der Fall und erklärt ebenfalls den geringen Fokus auf Risiko im finanziellen Performance-Management:

- Nur bei großen Investitionen (z.B. die Akquisition eines neuen Werks) wird eine Fremdfinanzierung in Betracht gezogen. Diese Finanzierungshilfen sind jedoch selten und werden auch immer sehr schnell zurückgezahlt.
- 90 bis 95 Prozent der Geschäfte werden in Euro abgewickelt. Aus diesem Grund sieht man auch hier keinen Anlass, sich intensiv mit Risiken zu beschäftigen, die Geschäfte in unterschiedlichen Währungen auf Grund der Wechselkurse mit sich bringen.

In Subdimension C1, dem strategischen Managementsystem, konnte der Reifegrad 2 erreicht werden. In der Planung bzw. der strategischen Zielfestlegung werden Key Risks, die im RM-Prozess identifiziert wurden, einbezogen. Außerdem werden neben Risiken auch Chancen betrachtet.

Im operativen Prozess-Managementsystem (Dimension C3) konnte bereits Reifegrad 3 erreicht werden. Dies spiegelt auch den guten RM-Prozess aus Dimension B1 wider. Eine weitere Integration von risikoadjustierten Performance-Kennzahlen könnte hier den Reifegrad noch erhöhen, wobei erwähnt werden sollte, dass dies teilweise schon gemacht wird (beispielsweise durch Six Sigma Qualitätsziele).

Als letzte Dimension wird das Ergebnis der **ERM-Governance** (**Dimension A**) dargestellt.

Sub-Dimension	Erreichter Reifegrad	Erreichter Inhalt	Ausstehender Inhalt für höheren Reifegrad
A1 : Risikostrategie	**RG1**	In zumindest ausgewählten Unternehmensbereichen sind die Risikotragfähigkeit und der Risikoappetit hinsichtlich bestandsbedrohender Entwicklungen sowie die Risikopolitik hinsichtlich des gewünschten Umgangs mit Risiken klar definiert	Die partiell dokumentierten Risikostrategien (Risikotragfähigkeit, Risikoappetit und Risikopolitik) werden überwacht und gesteuert und von einer unabhängigen Instanz bzgl. ihrer Einhaltung geprüft
A2 : Risikoverständnis	**RG1**	In ausgewählten Bereichen des Unternehmens liegt eine dokumentierte Risiko-Definition des Top-Managements vor	Die Risikodefinitionen des Top-Managements beinhalten die Unterscheidung von reinen Risiken (nur Verlustpotentiale) und spekulativen Risiken (Chance/Risiko-Kombinationen)
A3 : Risikoorganisation	**RG2**	Im Risikomanagement des Unternehmens sind Personen (z.B. Risikomanager) für die Überwachung und Anpassung des Risikomanagement-Prozesses verantwortlich	Die für das Risikomanagement verantwortlichen Personen (z.B. Risikomanager) verwenden bei der Überwachung und Anpassung des Risikomanagement-Prozesses in allen wichtigen Bereichen des Unternehmens durchaus unterschiedliche Konzepte (z.B. Einbeziehung von Betrugsrisiken im Compliance-Management bzw. von Chancen im Währungsrisiko-Management). Außerdem wird die Verankerung des Risikomanagements in allen Managementbereichen vom Top-Management unterstützt.

Abbildung 6: ERMMA-Feedback Dimension A

Hier wurde in jeder Subdimension mindestens der Reifegrad 1 erreicht.

Eine Risikostrategie (A1) ist grundsätzlich vorhanden, jedoch wird nicht überprüft, wie gut sie funktioniert und ob eventuell nicht genutzte Chancen zu einem noch besseren Ergebnis führen könnten. Wird diese unabhängig geprüft und zielorientierte Risikostrategien für die einzelnen Management-Bereiche definiert, kann hier auch Reifegrad 3 erreicht werden. Im Fall des Unternehmens werden die Ziele für Reifegrad 4 sogar teilweise erfüllt, die Risikostrategie ist stets im Einklang mit den Unternehmenszielen.

Das Risikoverständnis (A2) ist trotz des erreichten Reifegrads 1 im Top-Management sicherlich vorhanden, jedoch nicht sehr umfassend dokumentiert. Großes Verbesserungspotential besteht hier bei den Prozessverantwortlichen, die letzten Endes das Risikomanagement auf Prozessebene durchführen sollen. Chancen und Risiken werden einbezogen, jedoch keine Zielkategorien nach Normen (z.B. COSOII) verwendet.

In der dritten Dimension A3, der Risikoorganisation, wurde laut des ERMMA-Tests der Reifegrad 2 erreicht. Dieses Ergebnis muss korrigiert werden, da durch die fehlende Interne Revision keine Prüfung der Risikoorganisation stattfindet. Der Reifegrad ist also 1. Das bedeutet, dass es einen Risikomanager gibt, der für die Überwachung und Anpassung des RM-Prozesses verantwortlich ist. Der Verantwortliche ist jedoch erst seit kurzer Zeit explizit Risikomanager, deswegen nimmt er noch nicht so großen Einfluss auf die RM-Prozesse in den einzelnen Bereichen. Stattdessen fällt das in den Verantwortungsbereich der Leiter der jeweiligen Bereiche. Mit einer besseren Verankerung des Risikomanagers in allen Bereichen, sowie einer Prüfung durch die IR kann auch hier Reifegrad 3 oder sogar Reifegrad 4 erreicht werden.

2.2.2 Praktische Umsetzung in Industrie-EWF

Nach der Analyse des bestehenden Systems mithilfe des ERMMA-Reifegradtests wurde mit dem Risikomanager der Industrie-EWF besprochen, in welchen Bereichen Vorschläge bzw. Konzepte für eine Verbesserung der jeweiligen RM-Funktion gewünscht sind. Da die hier ausgearbeitete Lösung auf das Unternehmen zugeschnitten sein soll, ist es nicht zielführend, jede einzelne Dimension aus dem ERMMA-Reifegradtest auf einen hohen Reifegrad zu bringen. Folgende Dimensionen werden im Zuge der Arbeit genau betrachtet, analysiert und dazugehörige Konzepte erstellt, mit denen eine Verbesserung in der jeweiligen Dimension erreicht werden kann:

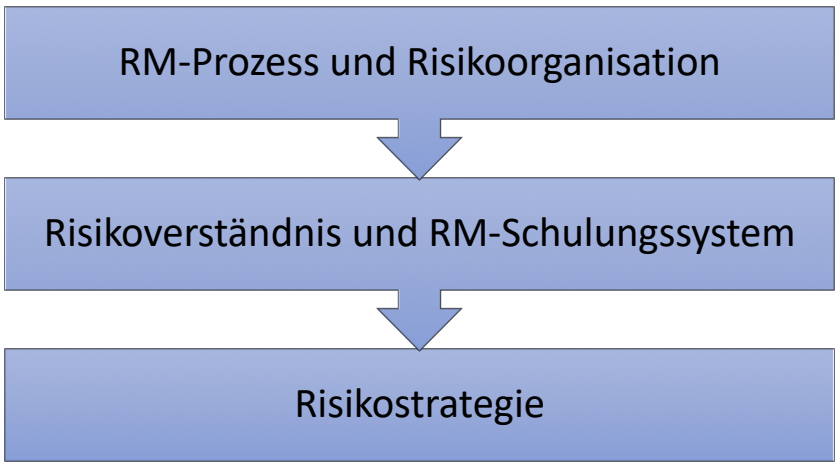


Abbildung 7: Vorgehensstruktur für Ausarbeitung der Verbesserungen

- *Risikomanagement-Prozess (B1) und Risikoorganisation (A3):* Ziel ist ein standardisierter RM-Prozess mit einem unternehmensweites RM-System, das regelmäßig angepasst und geprüft wird. Im Zuge des unternehmensweiten RM-Sytems wird auch die Organisation des Risikomanagements unternehmensweit verankert.
- *Risikoverständnis (A2) und Risikomanagement-Schulungssystem (B2):* Für ein unternehmensweites RM-System, das auch von den Mitarbeitern gelebt wird, muss das Verständnis für Risiko über alle Unternehmensbereiche hinweg verbessert werden. Dies soll durch die Integration des Themas Risiko in das bestehende Schulungssystem erreicht werden. Mitarbeiter (und vertiefend auch die Prüforgane – IKS und IR) sollen mit Hilfe von Schulungen ein besseres Bewusstsein und Verständnis für Risiko erlangen.

- *Risikostrategie (A2):* So wie eine generelle Unternehmensstrategie für die gesamte Industrie-EWF bzw. Strategien für einzelne Unternehmensbereiche bereits entwickelt und gelebt werden, soll auch die Risikostrategie darin integriert werden.

Alle Teile der Dimension C, die risikobasierten Planungs- und Steuerungssysteme, erfüllen bereits die Anforderungen der Industrie-EWF. Aus diesem Grund ist kein Anlass gegeben, diese Systeme zu verändern bzw. zu verbessern.

In der folgenden Tabelle wird überblicksmäßig dargestellt, wie sich die Reifegrade verändern können, wenn die Vorschläge aus dieser Arbeit umgesetzt werden:

Hauptdimension	Subdimension	Reifegrad IST	Reifegrad NEU
ERM-Governance	Risikostrategie	1	2
	Risikoverständnis	1	4
	Risikoorganisation	1	3
Risiko-Management-System	RM-Prozess	2	4
	RM-Schulungssystem	0	3
	RM-Informationssystem	1	1
Risiko(basierte) Planungs- und Steuerungssysteme	Strategisches Management-System	2	2
	Finanzielles Performance-Management-System	1	1
	Operatives Prozess-Management-System	3	3
Gesamt-Score		**1,33**	**2,56**

Tabelle 2: Veränderung der Reifegrade im Zuge der Verbesserungsvorschläge

Der neue Reifegrad von 2,56 würde eine Verbesserung im relativen Rang von 48 auf 18 mit sich bringen. Das würde bedeuten, dass 17% der Unternehmen besser als die Industrie-EWF bewertet werden, 71% jedoch schlechter.

In der folgenden Abbildung wird der Optimierungsprozess, der von einer Silo-Betrachtung der Risiken und einem partiellen Risikomanagement mit einem ERMMA-Score von 1,33 über die Optimierung der einzelnen Subdimensionen hin zu einem unternehmensweiten RM-System mit einer ganzheitlichen Risikobetrachtung und einem ERMMA-Score von 2,56 geht, dargestellt.

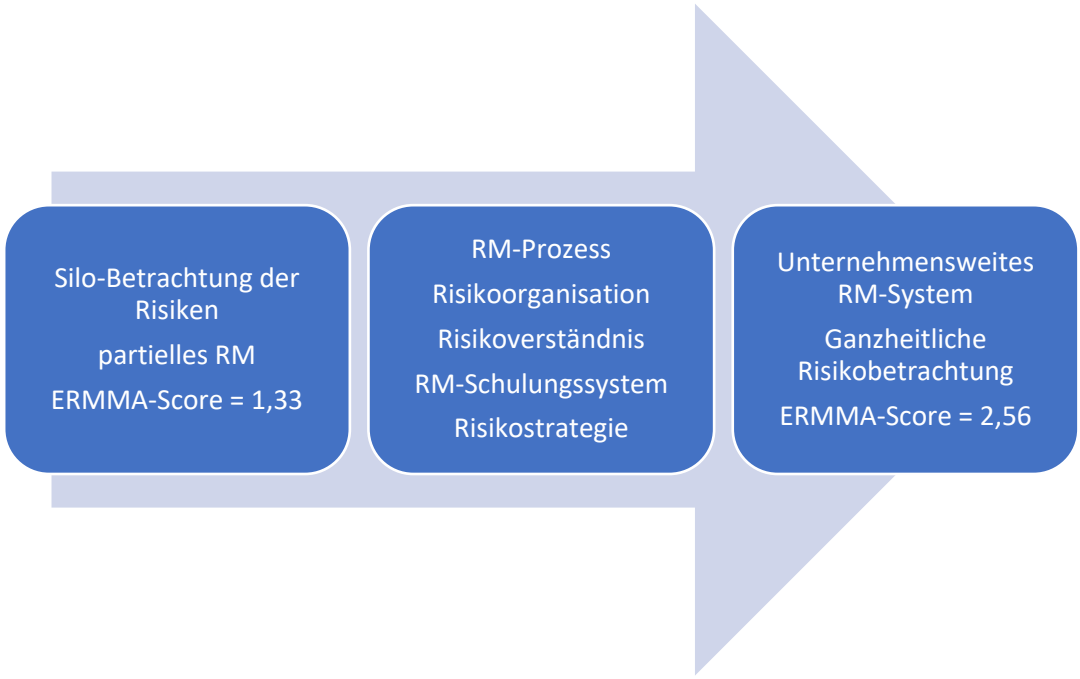


Abbildung 8: Beschreibung des Verbesserungsprozesses

3 ERM-Prozess und Organisation: Diagnose des IST-Zustands

Um verstehen zu können, wie und in welchem Umfang in der Industrie-EWF der RM-Prozess praktiziert wird, müssen mehr Informationen eingeholt werden, als aus dem ERMMA-Reifegradtest gewonnen werden können. Dafür werden verschiedene Methoden angewandt. Zuerst werden mit Hilfe des Risikomanagers Excel-Tabellen und andere Dokumente gesichtet, die im Zusammenhang mit verschiedenen Aspekten des Risikomanagements stehen, außerdem werden Interviews mit Personen, die direkt oder indirekt in das Risikomanagement der Industrie-EWF involviert sind, geführt. Das Ergebnis dieser Recherche führt zu der folgenden Darstellung des IST-Zustands.

Im Risikomanagement der Industrie-EWF werden einige wesentliche Methoden verwendet, um Risiken zu identifizieren, zu beurteilen bzw. zu bewerten und gegebenenfalls die richtigen Maßnahmen zu setzen. Diese werden hier kurz aufgelistet und dann im Folgenden noch detailliert beschrieben:

- Anlagenrisikobewertung – Auflistung der Produktionsanlagen, Bewertung nach bestimmten Kriterien, Kennzahl zur Risikobewertung
- Notfallmanagement – Risikokategorisierung aller Bereiche der Industrie-EWF mit Ursachen, Konsequenzen und Bewertung der Risiken
- Risikobewertung SUE – Auflistung und Bewertung sämtlicher Risiken im Bereich Sicherheit, Umwelt und Energie (SUE)
- Gefährdungsanalyse – Ermittlung, Beurteilung und Dokumentation der Gefahren an jeder Produktionsanlage
- Prozessrisiken – Auflistung aller Haupt- und Subprozesse des Unternehmens mit Prozessrisiken sowie Maßnahmen zur Vermeidung der Risiken
- Stakeholder-Analyse – Auflistung verschiedener Interessensgruppen mit Trends, Chancen/Risiken, Einfluss und Relevanz für die Industrie-EWF
- Führungsprozess – Jahresplan der Strategiemeetings, Zielvereinbarungsgespräche; Kontext- und Ist-Analyse → Risikobewertung → Strategie
- Risikobewertung und -verbesserung (Feuer- und Naturgefahren) – Bewertung des maximal möglichen Schadens durch Feuer- und Naturkatastrophen sowie empfohlene Maßnahmen zur Reduzierung des maximal möglichen Schadenswerts

Die wichtigste Rolle spielen dabei die Stakeholder-Analyse, die Anlagenrisikobewertung und das Notfallmanagement. In der folgenden Abbildung ist ersichtlich, dass bisher nur wenig Austausch von Informationen zwischen den einzelnen Funktionen stattfindet. Die einzelnen RM-Prozesse sind großteils voneinander getrennt und laufen parallel ab.

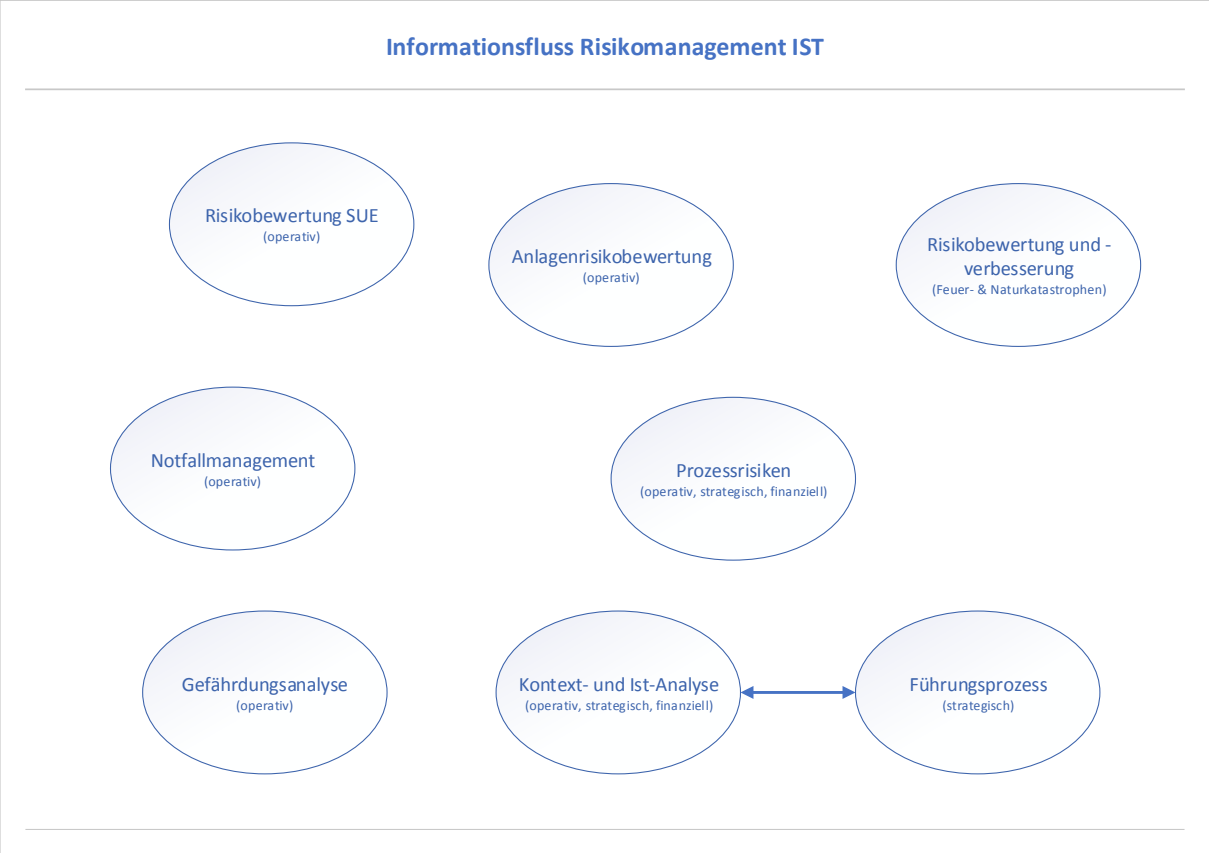


Abbildung 9: Informationsfluss Risikomanagement IST

Zum besseren Verständnis werden die einzelnen Methoden nun genauer beschrieben.

3.1 Risikomanagement der Produktionsanlagen: Diagnose des IST-Zustands

Die **Anlagenrisikobewertung** beinhaltet sämtliche Risiken der Produktion, die sich direkt auf Produktionsanlagen beziehen. Um die Einzelrisiken jeder Anlage bewerten zu können, sind bestimmte Informationen vonnöten. Teil der Anlagenrisikobewertung sind nicht nur große Maschinen, sondern alle Anlagen, beispielsweise auch Bohrmaschinen.

Erstens beinhaltet die Anlagenrisikobewertung Daten zur Identifizierung der Anlage. Zweitens wird eine Ausweichanlage angegeben, auf die, falls vorhanden, ausgewichen werden kann, wenn die Hauptanlage eine Störung hat oder eine planmäßige Wartung durchgeführt wird. Drittens wird eine Bewertung mithilfe von folgenden Kriterien vorgenommen:

- Risiko Produktion: Hier wird die Risikobewertung aus Produktionssicht durchgeführt. Dabei geht es immer um den Fall, dass die Maschine eine Störung vorweist und für einen längeren Zeitraum ausfällt. Die Bewertung wird jeweils vom Maschinenführer in Zusammenarbeit mit dem Instandhaltungsleiter in Form eines Interviews durchgeführt. Dabei wird in 3 Stufen bewertet:
    - 1 – unkritisch / Alternativanlagen sind vorhanden und sofort verfügbar
    - 2 – das Ausweichen auf Alternativanlagen ist mit geringem Aufwand (innerhalb von 2 Wochen) möglich
    - 3 – kritisch / keine Alternativanlage vorhanden
- Risiko Planung: Auch hier wird in 3 Stufen bewertet, diesmal allerdings aus der Sicht der Produktionsplanung. Dabei werden mechanische und elektrische Elemente (elektrisch – hauptsächlich die Steuerung) begutachtet. Außerdem fließt in die Bewertung die Verfügbarkeit von Ersatzteilen und die Auslastung der Anlage mit ein. Ein Ausfall kann auch dann als unkritisch bewertet werden, wenn keine Ausweichanlage vorhanden ist. Das kann daran liegen, dass sie nicht hoch ausgelastet ist oder die darauf gefertigten Produkte nicht sehr zeitsensibel sind.
    - 1 – unkritisch / Alternativanlagen sind vorhanden und/oder Ersatzteile schnell verfügbar
    - 2 – Anlage hat eine hohe Auslastung / permanenten 3-Schichtbetrieb
    - 3 – kritisch / Produkte können teilweise nur auf dieser Anlage gefertigt werden

- Anlagenzustand: Dabei geht es rein um den technischen Zustand der Anlagen sowie deren Einzelteile. Diese Bewertung wird wiederum vom Instandhaltungsleiter in Zusammenarbeit mit den Maschinenführern durchgeführt.
    - 1 – sehr gut
    - 2 – befriedigend
    - 3 – kritisch / Umbauten oder Reparaturen dringend erforderlich
- Antriebstechnik: Diese Bewertung betrifft rein die Antriebstechnik sowie die Steuerung der jeweiligen Maschine. Wieder wird in 3 Stufen bewertet:
    - 1 – unkritisch / Ersatzteile für Steuerung und Antrieb sind verfügbar
    - 2 – kritisch / Steuerungskomponenten sind Einzelstücke bzw. werden mehrfach verwendet
    - 3 – Steuerungskomponenten sind nicht verfügbar
- Wartungszahl: Die Wartungszahl errechnet sich aus dem aktuellen Jahr minus das Jahr der letzten Wartung (Bsp.: letzte Wartung = 2008, aktuelles Jahr = 2018 → Wartungszahl = 2018-2008 = 10)

Aus diesen einzelnen Bewertungen ergibt sich nach Aufsummieren eine Kennzahl und eine Strategie. In der folgenden Tabelle wird ein Beispiel angeführt.

Anlage	Ausweich-anlage	Risiko Produkt	Risiko Planung	Anlagen-zustand	Antriebs-technik	Wartungs-zahl	Kennzahl
A	C	2	1	1	1	6	11
B	D	3	2	2	3	0	10

Tabelle 3: Beispiel Anlagenrisikobewertung

In dem Beispiel ist ersichtlich, dass die Bewertung zwar funktioniert, jedoch keinen sofortigen Überblick bietet, wenn man sich nur die Kennzahl ansieht. Anlagen A hat eine höhere (und demnach kritischere) Kennzahl als Anlage B. Dennoch ist sie geringerem Risiko ausgesetzt, wie man in den einzelnen Bewertungskriterien sehen kann. Der Grund dafür ist die hohe Wartungszahl bei Anlage A. Sie besagt, dass die Anlage vor 6 Jahren das letzte Mal gewartet wurde. Da sie jedoch nirgends als kritisch eingestuft wird, besteht auch kein Grund dazu. Anlage B hingegen wurde zwar im aktuellen Jahr gewartet, weist aber in allen Bereichen ein höheres Risiko auf. Das kann verschiedene Gründe haben. Es kann sich um ein sensibles und wichtiges Produkt handeln, dass nur auf dieser Anlage gefertigt werden kann, außerdem kann

eine Steuerungskomponente nach der Wartung kaputt gegangen sein. Deshalb ist in diesem Fall die Kennzahl trügerisch.

Die Anlagenrisikobewertung dient operativ vor allem der Instandhaltung. So kann die Wartungsplanung gemeinsam mit Planung und Produktion abgestimmt werden. Außerdem bietet sie einen Überblick über sämtliche Anlagen bzw. Ausweichanlagen. Im Zuge der Quartalsplanung wird auch die Anlagenrisikobewertung vierteljährlich aktualisiert. An den Anlagen werden immer wieder bauliche oder steuerungstechnische Anpassungen vorgenommen, diese beeinflussen dann direkt die Kennzahl. Beispielsweise kann die Anpassung einer Anlage dazu führen, dass sie als Ausweichanlage dienen kann. Dies muss natürlich in der Anlagenrisikobewertung festgehalten werden.

3.2 Notfallmanagement: Diagnose des IST-Zustands

Im Notfallmanagement werden sämtliche Risiken angeführt, die im operativen Bereich auftreten können. Das geht von der Beschaffung von Vormaterial über die Produktion bis zur Strom- oder Gasversorgung oder einem WLAN-Ausfall. Die wichtigsten Risiken sind nach Bereichen wie folgt kategorisiert:

- Energieversorgung
- Arbeitskräftemangel
- Ausfall wichtiger Produktionsanlagen
- Hilfs- und Betriebsstoffe
- Vormaterial
- IT/EDV Ausfall (Hardware- und Softwareprobleme)
- Feldbeanstandungen Automotive Produkte

Innerhalb dieser Kategorisierung gibt es einzelne genauer definierte Bereiche. Beispielsweise findet man bei Energieversorgung Strom, Gas, Heizung, Wasser, Druckluft, Heizöl, Diesel usw. Zu jedem Risiko ist eine detailliertere Risikobeschreibung vorhanden. Diese gibt genau wieder, was passieren kann. Auch hier ein Beispiel: Zum Risiko „Stromversorgung Extern“ gehört die Risikobeschreibung „Elementarschäden, ungeplante Abschaltung EVU[6]“. Folgende Details werden weiter angeführt:

- Mögliche Auslöser / Ursachen
- Mögliche Auswirkungen / Konsequenzen
- Risk Owner (der jeweilige Prozessverantwortliche)

Sämtliche Bereiche werden dann bewertet. Dabei wird unterschieden in eine Nettorisikobewertung (unter Berücksichtigung der Maßnahmen) und eine Bruttorisikobewertung (ohne Berücksichtigung der Maßnahmen). Die Risikobewertung ist aufgeteilt in

- Auswirkung
- Eintrittswahrscheinlichkeit
- Risikoeinstufung

[6] Elektrizitätsversorgungsunternehmen

Weiters beinhaltet das Notfallmanagement eine überblicksmäßige Maßnahmenbeschreibung, die Definition einer verantwortlichen Person, die Umsetzung (ob und wann die Maßnahmen umgesetzt werden), den Status, die Standortrelevanz sowie die Information, ob ein Eskalationsprozess erforderlich ist. Ist ein Eskalationsprozess erforderlich, wird ebenfalls vermerkt, wo dieser beschrieben ist (beispielsweise wird das Vorgehen bei einem Problem mit der Gasversorgung genau in einem Notfallschutzplan beschrieben – Benachrichtigungsschema, Telefonnummern, Anweisungen).

3.2.1 Risikobewertung SUE

Die Risikobewertung SUE (= Sicherheit, Umwelt und Energie) beinhaltet sämtliche Risikoszenarien, die zu einer Personen-, Gesundheits- oder Umweltgefährdung oder einer Anrainerbelästigung führen können und ist Teil des Notfallmanagements. Diese Risiken werden vom Leiter des Notfallmanagements mit den verschiedenen Bereichsleitern identifiziert. Weiters werden sämtliche Produktionsprozesse in die einzelnen Schritte aufgetrennt und dort jeweils die ermittelten Risiken zugeordnet. So entsteht auch ein Überblick darüber, welche Szenarien in welchem Produktionsprozess eintreten können. Außerdem werden die möglichen Ursachen für die einzelnen Szenarien identifiziert und ein Maßnahmenplan erstellt.

Die einzelnen Risikoszenarien werden dann genau bewertet, und zwar in den vier oben genannten Kategorien – akute Personengefährdung, Gesundheitsgefährdung (durch berufsbedingte Krankheiten), Umweltgefährdung und Anrainerbelästigung (Lärm, Geruch, optische Beeinträchtigung). Dafür wird eine Bewertungsmatrix verwendet.

Erstens werden die Auswirkungen betrachtet. Die Skala geht von 1 bis 100, allerdings in sechs Schritten, die im Folgenden überblicksmäßig veranschaulicht werden:

- Gering – 1: leichte gesundheitliche Beschwerden, kurzfristiger Eingriff in Umwelt (ökologisch oder Anrainer)
- Wichtig – 3: leichte Verletzung oder Erkrankung, ökologischer Schaden innerhalb von sechs Monaten reversibel, länger merkbare Störung für Anrainer

- Ernst – 7: zweiwöchiger Arbeitszeitverlust, ökologischer Schaden innerhalb eines Jahres reversibel, lokale Anrainerbelästigung
- Sehr ernst – 15: vierwöchiger Arbeitszeitverlust, ökologischer Schaden innerhalb von drei Jahren reversibel, langfristige Anrainerbelästigung
- Großschaden – 40: zwei Monate Arbeitszeitverlust, Invalidität mit Arbeitsfähigkeit, ökologischer Schaden innerhalb von vier bis zehn Jahren reversibel, Nutzungsbeschränkung für Anrainer
- Katastrophe – 100: tödlicher Unfall oder Arbeitsunfähigkeit, ökologsicher Schaden reversibel nach über zehn Jahren, langfristige Nutzungsbeschränkung für Anrainer

Zweitens wird die Wahrscheinlichkeit beurteilt. Diese Skala geht von 1 bis 10, hier in fünf Schritten:

- Sehr selten – 1: weniger als 1-mal in 10 Jahren (fast unmöglich)
- Selten – 2: weniger als 1-mal in 5 Jahren (unwahrscheinlich)
- Manchmal – 3: weniger als 1-mal pro Jahr (möglich)
- Ab und zu – 5: monatlich (gut möglich)
- Regelmäßig – 10: häufiger als 1-mal pro Monat (fast sicher)

Mithilfe dieser Bewertungsmatrix werden nun sämtliche identifizierte Risikoszenarien bewertet. Dafür wird die Auswirkung mit der Wahrscheinlichkeit multipliziert. Das Ergebnis ist eine Risikokennzahl (RKZ), die einen maximalen Wert von 1.000 annehmen kann, was einer Katastrophe entspräche, die mehrmals pro Monat auftritt.

$$RKZ = Ausirkung * Eintrittswahrscheinlichkeit$$

Für die Risikokennzahl existiert ein Wertungsschema, das farblich gekennzeichnet ist und vorschreibt, bei welcher RKZ welches Gefahrenpotential herrscht und wann sofort gehandelt werden muss.

3.2.2 Gefährdungsanalyse

Auch die Gefährdungsanalyse ist ein Teil des Notfallmanagements. Jeder Arbeitsbereich wird dahingehend untersucht, welche Gefährdungen darin auftreten. Der wesentliche Unterschied

zur Risikobewertung SUE ist die Vorgehensweise der Risikoidentifikation. In der Risikobewertung SUE werden erst die Risikoszenarien identifiziert und dann den jeweiligen Prozessen zugeordnet. In der Gefährdungsanalyse jedoch werden die Prozesse betrachtet und dann überlegt, welche Risiken bzw. Gefährdungen darin auftreten können.

Diese Risiken werden kategorisiert nach der Art der Gefährdung: z.B. mechanisch, thermisch, elektrisch und auch sonstige Belastungen, wie eine Schwangerschaft. Die Auswirkungen und die Wahrscheinlichkeit werden nach dem gleichen Bewertungsschema wie bei der Risikobewertung SUE (siehe oben) evaluiert. Aus dem Produkt der beiden entsteht wieder eine Risikokennzahl.

Bei der Gefährdungsanalyse geht man jedoch noch einen Schritt weiter. Nach der Identifizierung und Bewertung sämtlicher Risiken werden sogleich auch Maßnahmen dokumentiert und umgesetzt. Auf der Basis dieser Maßnahmen erfolgt eine Neubewertung der Risiken, die üblicherweise weit unter dem anfangs ermittelten Wert liegt.
Ein Beispiel dafür ist die Rutsch- bzw. Stolpergefahr durch Verunreinigungen oder nicht gut aufgeräumte Arbeitsplätze. Das anfängliche Risiko hat eine „ernste“ Auswirkung (= 7) und eine monatliche Eintrittswahrscheinlichkeit (= 5). Daraus ergibt sich eine Risikokennzahl von 35. Durch die Maßnahmen der Unterweisung in Ordnung und Sauberkeit und eine regelmäßige Reinigung sinkt die Auswirkung von „ernst“ auf wichtig (= 3). Die Eintrittswahrscheinlichkeit bleibt zwar gleich, jedoch kann durch diese Maßnahmen die RKZ auf 15 gesenkt werden.

3.2.3 Risikobewertung und -verbesserung (Feuer- und Naturgefahren)

Dabei handelt es sich um eine von Sachverständigen einer Versicherung durchgeführte Bewertung der maximalen Schadenswerte in Bezug auf Feuer- und Naturgefahren. Dabei wurden sämtliche Betriebsanlagen begutachtet und Maßnahmen vorgeschlagen, die zu einer Verbesserung der Schutzmaßnahmen bzw. zu einer Reduzierung des maximal möglichen Schadens führen beitragen könnten.

3.3 Strategisches Risikomanagement: Diagnose des IST-Zustands

3.3.1 Stakeholder-Analyse

Die Stakeholder-Analyse beinhaltet sämtliche Interessensgruppen, die Teil der Industrie-EWF sind oder für das Unternehmen relevant sind. Diese werden analysiert und bewertet. Die wichtigsten Interessensgruppen sind Mitarbeiter, Mitbewerber, Kunden (bzw. der Markt), der Arbeitsausbildungsmarkt, Lieferanten und die Eigentümer. Weitere Interessensgruppen sind beispielsweise Behörden, Anrainer, Gewerkschaften, Banken und Zertifizierungsstellen.

Diese Stakeholder werden nach den folgenden Kriterien beurteilt:

- Bedeutung für die Industrie-EWF
- Nutzen für bzw. Anforderungen an das Unternehmen
- Entwicklungstrends der Interessensgruppe
- Was ergibt sich aus den Entwicklungstrends?
    - Chancen
    - Risiken
- Einfluss / Macht (Liegt der größere Einfluss eher auf der Seite der Industrie-EWF oder nicht?)
- Relevanz der Anforderungen bzw. der Anliegen des Stakeholders an das Unternehmen
- Form der Interaktion – derzeit und zukünftig (z.B.: Emails, Telefonate, etc.)
- Art der Dokumentation der Informationen (wo wird dokumentiert und überprüft)
- Risikobetrachtung – Methode, mit der das Risiko bewertet wird (z.B. im Notfallmanagement, aber auch andere Methoden wie SWOT-Analyse)
- Verantwortliche innerhalb der Industrie-EWF für den jeweiligen Stakeholder

Man kann hier erkennen, dass in der Stakeholder-Analyse sowohl Risiken als auch Chancen betrachtet werden. Gerade hier ist das immens wichtig, da sich (im Gegensatz zu den meisten operativen Prozessen – eine Maschine kann nicht „zufällig“ einmal mehr oder schneller produzieren) aus den zukünftigen Entwicklungen viele Chancen ergeben können. Identifiziert und dokumentiert man diese Chancen nicht, kann man sie auch nicht nutzen. Diese Methode der Risikoanalyse ist die umfangreichste der bisher genannten.

3.3.2 Führungsprozess

Der Führungsprozess wird hier erwähnt, um zu zeigen, dass sich die Geschäftsführung im Zuge regelmäßiger Meetings mit verschiedenen Risiken auseinandersetzt. Diese Risiken sind jedoch hauptsächlich strategischer Natur, die Betrachtung operativer Risiken ist auf Grund der fehlenden Integration der einzelnen Methoden in ein unternehmensweites System noch vergleichsweise unstrukturiert und deshalb optimierbar.

Der Führungsprozess an sich beinhaltet natürlich viel mehr als Risikomanagement, da es sich um die Führung der gesamten Industrie-EWF handelt. In Abbildung 10 kann man die schematisch dargestellte zeitliche Abfolge der Aktivitäten (über ein Jahr hinweg) erkennen, in denen Risiken in die Entscheidungsfindung mit einfließen.

Abbildung 10: Schematisch dargestellter Führungsprozess

3.4 Risiko-Übersicht in Form der Prozessrisiken

Die Prozessrisiken sowie die Maßnahmen zur Vermeidung der Risiken sind in der Prozesslandkarte der Industrie-EWF im internen ERP-System enthalten. In den 3 Hauptgruppen der Prozesslandkarte (Führungsprozesse, Kernprozesse, unterstützende Prozesse) finden sich wiederum Hauptprozesse, zu denen jeweils mehrere Subprozesse gehören. In jedem dieser Subprozesse ist das Ziel des Prozesses, der Prozessverantwortliche, die Prozessrisiken und mögliche Maßnahmen zur Vermeidung der Risiken angeführt. Dafür wurde mit jedem Prozessverantwortlichen der einzelnen Prozesse ein informelles Interview geführt, bei dem eine Einschätzung der Risiken des jeweiligen Prozesses durchgeführt wurde.

Diese Daten wurden im Zuge dieser Arbeit aus dem System entnommen, in MS-Excel übertragen, kategorisiert und analysiert. Dabei wurde großes Potential ersichtlich, da jeder Prozess des gesamten Unternehmens enthalten ist und beinahe überall bereits Risiken identifiziert wurden, sowie Maßnahmen zur Reduzierung bzw. Vermeidung dieser Risiken beschrieben wurden.

4 ERM-Prozess und Organisation: Theoretische Grundlagen

4.1 Risikomanagement-Prozess in der Theorie

Der Risikomanagementprozess ist laut ONR 49000:2014[7] wie folgt definiert:

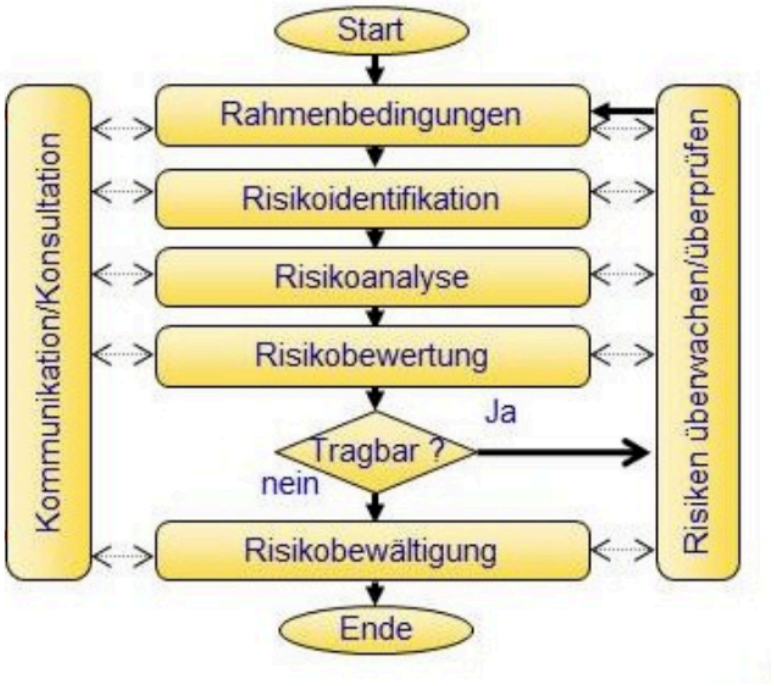


Abbildung 11: RM-Prozess, Quelle: [ONR 49000, 2014, S. 19]

4.1.1 Rahmenbedingungen

Zuerst werden *Rahmenbedingungen* bzw. *Risikokriterien* definiert. Rahmenbedingungen werden in der Risikostrategie festgelegt. Die Implementierung einer Risikostrategie wird im Kapitel *Risikostrategie* noch erläutert. Die Kriterien können beispielsweise Ausfallzeiten oder die Fehlerquote einer Maschine sein. Dies ist auf den ersten Blick sehr spezifisch, kommt aber daher, dass für die verschiedenen Bereiche langfristig auch eigene Risikostrategien entwickelt werden. Diese Beispiele würden Platz in der Risikostrategie der Produktion finden.

4.1.2 Risikoidentifikation

Das Ziel der Risikoidentifikation ist die frühzeitige Erkennung von Entwicklungen, die den Fortbestand des Unternehmens gefährden können. Dabei ist die Informationsbeschaffung die schwierigste Phase und eine Schlüsselfunktion im RM-Prozess, da alle nachfolgenden Phasen

[7] Ein Regelwerk zum Risikomanagement für Organisationen und Systeme, das die praktische Umsetzung des Internationalen Standards ISO 31000 unterstützt

auf der möglichst vollständigen Identifikation der Risiken aufbauen. Frühwarnsysteme sind ebenfalls ein wichtiges Instrument der Risikoidenfikation, in denen Frühwarnindikatoren (z.B. Auftragslage, Marktindizes) davor warnen, wenn Risiken relevant werden, die davor keine Wichtigkeit hatten [Romeike, Hager, 2013, S. 102].

Zur Risikoidentifikation können verschiedene Methoden herangezogen werden, deren Wirksamkeit sich am Einsatzgebiet orientiert. Diese Methoden können in *Kollektionsmethoden* und *Suchmethoden* eingeteilt werden. *Suchmethoden* wiederum werden in *analytische Methoden* und *Kreativitätsmethoden* unterteilt.
Während Kollektionsmethoden hauptsächlich zur Identifikation von bereits bestehenden oder bekannten Risiken geeignet sind, werden Suchmethoden zur Erfassung von noch unbekannten Risiken herangezogen [Romeike et al., 2013, S. 104].

4.1.2.1 Kollektionsmethoden

Mit Hilfe folgender Methoden werden meist bereits bekannte Risiken identifiziert [Romeike et al., 2013, S. 105-107]:

- Checklisten: Eine detaillierte Checkliste kann als Ausgangspunkt der Risikoidentifikation verwendet werden. Die Erstellung ist sehr aufwändig, außerdem können keine allgemein gültigen Checklisten verwendet werden, da sie an den jeweiligen zu überprüfenden Bereich angepasst werden müssen.
- SWOT-Analysen (strenghts, weaknesses, opportunities, threats)[8]: Eine solche Analyse liefert Informationen zu
    - dem IST-Zustand des eigenen Unternehmens (Kernkompetenzen)
    - den Zielgruppen
    - dem Wettbewerbsumfeld (Positionierung, Alleinstellungsmerkmale)
    - der Marktpräsenz
- Interviews: Auch bei der Befragung von Mitarbeitern können Risiken identifiziert werden. Interviews können sehr gute Ergebnisse liefern, wenn sowohl der Interviewführer als auch der Befragte ausreichend Kompetenz und Erfahrung mitbringt.

[8] Auf Deutsch: Stärken, Schwächen, Gelegenheiten, Bedrohungen

- Self-Assessment: Diese Methode kann mit Checklisten oder Interviews kombiniert werden und bezieht sich ausschließlich auf den internen Bereich des Unternehmens.

4.1.2.2 Analytische Suchmethoden

Diese Methoden werden genutzt, um noch unbekannte Risiken identifizieren zu können [Romeike et al., 2013, S. 107-109]:

- FMEA (Failure Mode and Effects Analysis → Fehlermöglichkeits- und Einflussanalyse): Das Unternehmen wird als störungsfreies System beschrieben. Im nächsten Schritt wird das Gesamtsystem in Funktionsbereiche zerlegt. Um Störungen finden zu können, werden potenzielle Störungszustände der Einzelbereiche untersucht. Abschließend werden die Auswirkungen auf das Gesamtsystem abgeleitet. Ein großer Vorteil der FMEA ist die formale Vorgehensweise (mit Arbeitsblättern).
- FTA (Fault Tree Analysis → Fehlerbaumanalyse): Hier wird nicht von einer Störung im Einzelbereich, sondern von einem gestörten Gesamtsystem ausgegangen. Nachdem analysiert wird, welche einzelnen Störungen zur Störung des Gesamtsystems beitragen, werden diese Störungsursachen gegliedert, bis keine weitere Differenzierung mehr möglich ist.
- Fragenkatalog: Der Fragenkatalog baut häufig auf einer anderen Identifikationsmethode auf, die die Grundlage für die Zusammenstellung der Fragen bildet.

4.1.2.3 Kreativitätsmethoden

Ebenfalls zur Identifizierung von noch unbekannten Risiken eignen sich folgende kreative Methoden [Romeike et al., 2013, S. 109-113]:

- Brainstorming: Eine ungezwungene Atmosphäre soll die Kreativität der Beteiligten fördern. Die Ergebnisqualität dieser Methode beruht darauf, dass
    - das Wissen mehrerer Personen genutzt wird,
    - Blockaden im Denken ausgeschaltet werden,
    - Restriktionen vermieden werden und so die Vielfalt der Lösungsansätze vergrößert wird und
    - die Kommunikation der Beteiligten demokratisiert wird.

- Brainwriting: Diese Methode funktioniert ähnlich wie Brainstorming, jedoch schreiben hier die Beteiligten ihre Ideen auf ein Blatt Papier, das dann an die nächste Person weitergereicht wird. Diese kann dann eine bereits hinzugefügte Idee aufgreifen und ergänzen oder neue Ideen hinzufügen.
- Delphi-Methode: Ausgangslage für diese Methode ist ein Fragebogen oder Thesenpapier mit allen zu beantwortenden Fragen. In mehreren Runden, die aufeinander aufbauen, werden Experten befragt. Diese Befragungen erfolgen meist in zwei bis vier Iterationen mit den Prozessschritten Befragung, Datenanalyse, Feedback, Diskussion und Entscheidung. Störende Einflüsse werden durch die Anonymisierung, die Schriftform und die Individualisierung eliminiert. Konzentration auf das Wesentliche, mehrstufige (teilweise rückgekoppelte) Editierprozesse und umfassende Aussagen bestimmen die Strategie der Delphi-Methode.

4.1.3 Risikoanalyse

Unter *Risikoanalyse* versteht man die systematische Ermittlung von Informationen, mit deren Hilfe die Risiken verstanden, die Wahrscheinlichkeiten des Eintretens der Risiken ermittelt und die Auswirkungen eingeschätzt werden können. Dies schafft die Grundlage für die Bewertung und Bewältigung der Risiken und kann historische Daten, Analysen oder auch persönliche Meinungen eines Experten beinhalten. Dabei werden also die Risiken, die im ersten Schritt identifiziert wurden, quantifiziert. Dafür gibt es verschiedene Methoden [Romeike et al., 2013, S. 113-115].

4.1.3.1 Risikoprioritätszahl

Eine Methode der Risikoquantifizierung ist die Risikoprioritätszahl (RPZ) aus der FMEA (Failure Mode and Effects Analysis bzw. Fehlermöglichkeits- und Einflussanalyse). Sie setzt sich aus drei Faktoren zusammen, die jeweils einen maximalen Wert von 10 erreichen können [Thies, 2008, S. 50-51]:

- Bedeutung (B) – von 10 (sehr hohe Bedeutung, extremes Sicherheitsrisiko, Lebensgefahr) bis 1 (sehr gering, keine Funktionalitätseinschränkung)
- Auftrittswahrscheinlichkeit (A) – von 10 (sehr häufiges Auftreten, die Funktionalität ist demnach gänzlich unbrauchbar) bis 1 (Auftreten der Fehlerursache ist unwahrscheinlich)
- Entdeckungswahrscheinlichkeit (E) – von 10 (Entdecken der Fehlerursache ist unwahrscheinlich, sie kann nicht geprüft werden) bis 1 (Entdecken der Ursache ist absolut sicher)

Diese drei Faktoren werden multipliziert, um daraus die RPZ zu erhalten.

$$RPZ = B * A * E$$

So kann die Risikoprioritätszahl einen Wert von 1 bis 1000 annehmen, wobei 1000 ein extremes Risiko mit sehr hoher Auftrittswahrscheinlichkeit und sehr geringer Entdeckungswahrscheinlichkeit darstellt [Thies, 2008, S. 42].

Bei der Verwendung der RPZ wird weiters ein Grenzwert definiert, ab dem ein Risiko innerhalb eines Unternehmens als nicht akzeptabel eingestuft wird. Dieser Wert variiert, befindet sich jedoch üblicherweise in einem Bereich von 80 bis 125. Die Problematik der RPZ ist jedoch, dass es schwierig ist, vor allem die Entdeckungswahrscheinlichkeit akkurat abzuschätzen, wenn man keine genauen statistischen Daten zur Verfügung hat [Thies, 2008, S.52].

4.1.3.2 Risikolandkarte

Eine zweite Methode ist die Erstellung einer Risikolandkarte (Risk Map). In der folgenden Abbildung wird eine solche Risikomatrix exemplarisch dargestellt.

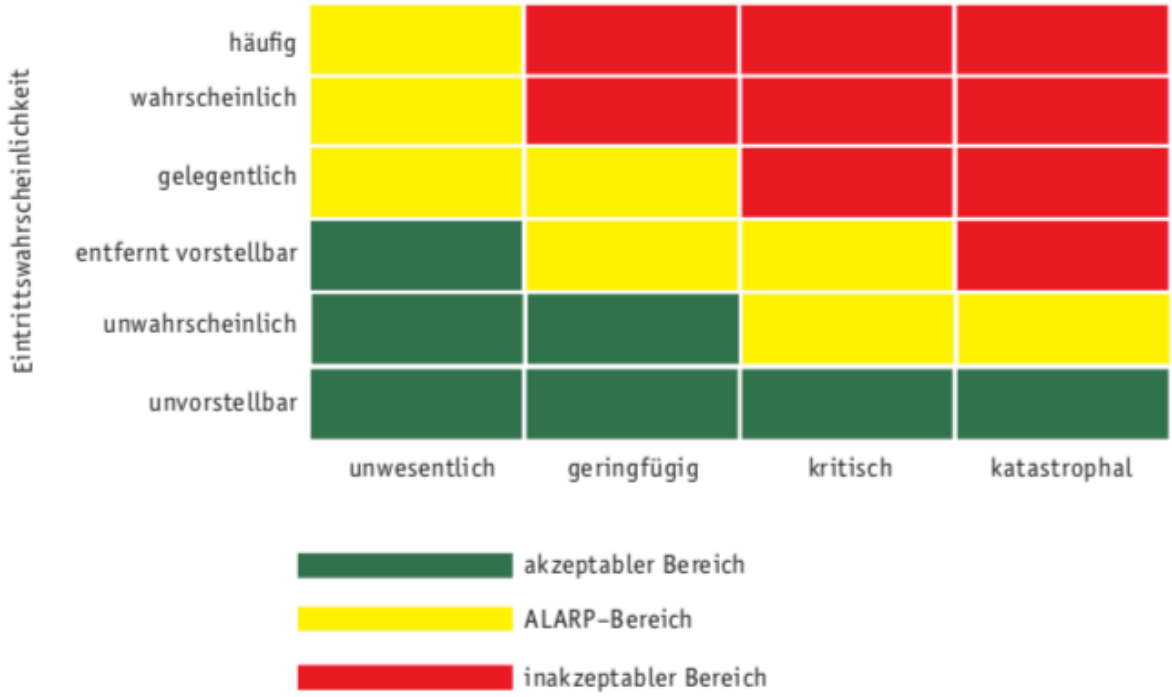


Abbildung 12: Beispiel für eine Risikolandkarte, Quelle: [Rechnungshof, 2016, S. 11]

Die Risk Map ist eine zweidimensionale Matrix, die einen Gesamtüberblick über das Risikoportfolio eines Unternehmens, einer Abteilung oder eines einzelnen Prozesses gibt. Ihr Vorteil ist, dass man auf einen Blick erkennt, welche Risiken besonders relevant sind und möglichst zeitnah bewältigt werden müssen. Ihre beiden Dimensionen setzen sich aus der Eintrittswahrscheinlichkeit und der Auswirkung (bzw. dem Schadenspotential) zusammen. In der Praxis werden diese beiden Faktoren mit Hilfe einiger Stufen klassifiziert – in der Regel basierend auf Experteneinschätzungen [Romeike et al., 2013, S. 124].

Befindet sich ein Risiko im roten Bereich, muss es sofort behandelt werden, da es sich dabei mindestens um ein Risiko mit häufigem Eintreten und geringer Auswirkung oder um ein katastrophales Risiko mit vorstellbarem Eintreten handelt. Der Worst Case ist ein katastrophales Risiko mit häufiger Eintrittswahrscheinlichkeit, zu finden im rechten oberen Bereich der Risk Map [Rechnungshof, 2016, S. 11].

Der gelbe Bereich ist der sogenannte ALARP-Bereich. ALARP bedeutet „as low as reasonably practible", also ein höchster Grad an Sicherheit, der vernünftigerweise praktikabel ist [Rechnungshof, 2016, S. 11]. Der ALARP-Bereich kann auch als Akzeptanzlinie bezeichnet werden. Es ist also jener Bereich, in dem Risiken zwar regelmäßig überwacht werden sollen, sie jedoch akzeptiert werden können [Romeike et al., 2013, S. 124].

Der grüne Bereich ist der unkritische Bereich, in dem ein Risiko entweder schwerwiegende Auswirkungen hat, der Eintritt aber unvorstellbar ist, oder ein vorstellbares Risiko nur geringe Auswirkungen mit sich zieht [Romeike et al., 2013, S. 124].

In einer Risikolandkarte kann abgelesen werden, mit welcher Priorität man sich den einzelnen Risiken widmen soll. Zuerst werden immer jene Risiken betrachtet, die sich im roten Bereich befinden. Haben mehrere Risiken das gleiche Schadensausmaß, beginnt man mit der höchsten Eintrittswahrscheinlichkeit [Romeike et al., 2013, S. 124].

Hat man für einzelne Bereiche oder Abteilungen im Unternehmen Risk Maps erstellt, können deren wichtigste Ergebnisse in einer unternehmensweiten Risikolandkarte kumuliert werden, sodass sich auf einen Blick ein Gesamtbild des Risikos im Unternehmen ergibt, welches dann gesteuert werden kann.

4.1.4 Risikobewertung

Im Zuge der *Risikobewertung* werden die Ergebnisse der Risikoanalyse mit den festgelegten Risikokriterien aus den Rahmenbedingungen verglichen. So wird ermittelt, ob das Risiko eingegangen werden kann/soll oder nicht.

4.1.5 Überwachung und Überprüfung

Wird entschieden, dass das Risiko tragbar ist, muss es *überwacht* und *überprüft* werden. Dieser Schritt fließt wieder in die Rahmenbedingungen mit ein.

Die Überprüfung ist nicht als einzelner Schritt zu einem bestimmten Zeitpunkt zu sehen, sondern sie findet ständig statt. Als Risikoverantwortlicher ist es wichtig, stets einen Überblick darüber zu haben, wie gut der RM-Prozess funktioniert. Auch kann es jederzeit zu einer

Veränderung in der Ausgangssituation kommen, was oft eine Anpassung in der Risikoanalyse zur Folge hat.

Die Überwachung wird einerseits vom Internen Kontrollsystem (IKS), andererseits von der Internen Revision (IR) durchgeführt. Auf diese beiden Funktionen bzw. Organe wird im Folgenden detailliert eingegangen.

4.1.5.1 Das Interne Kontrollsystem

Ein internes Kontrollsystem ist nicht als definierte Funktion zu sehen, sondern als eine Vorgehensweise, die in allen Unternehmensbereichen implementiert ist.
§ 82 Aktiengesetz schreibt vor: „Der Vorstand hat dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen." [RIS, 2015]
Dieser Gesetzestext lässt sehr viel Spielraum zu, da er eigentlich nur vorschreibt, dass es ein IKS geben soll, jedoch in keiner Weise das Ausmaß und die Umsetzung definiert.

Auf internationaler Ebene rückten Interne Kontrollsysteme bereits im Jahr 2002 in den Fokus, nachdem Unternehmen wie Enron und Worldcom wegen massiver Bilanzmanipulationen zusammenbrachen. Der „Sarbanes-Oxley Act"[9] wurde in den USA eingeführt, die Europäische Union zog mit der 4., 7. und 8. EU-Richtlinie[10] zur Verbesserung der Corporate Governance nach. In Österreich erfolgte die Umsetzung in nationales Recht im Unternehmensrechtsänderungsgesetz (URÄG) 2008 [Detecon, 2010, S. 6].

[9] Der „Sarbanes-Oxley Act" stellt die systematische Aufdeckung und Überwachung von Risiken in den Prozessen des Rechnungswesens in den Vordergrund [Detecon, 2010].
[10] Diese Richtlinien sollen eine verstärkte Überwachung und Wirksamkeit interner Kontroll-, Revision- und Risikomanagementsysteme ermöglichen [Detecon 2010].

Wie ist ein internes Kontrollsystem definiert?

Der österreichische Rechnungshof [Rechnungshof, 2016, Vorwort] definiert ein IKS als einen in die Arbeits- und Betriebsabläufe einer Organisation eingebetteten Prozess, der von den Führungskräften und Mitarbeitern durchgeführt wird, um

- bestehende Risiken zu erfassen,
- zu steuern und
- mit ausreichender Gewähr[11] sicherstellen zu können, dass die betreffende Organisation im Rahmen der Erfüllung ihrer Aufgabenstellung ihre Ziele erreicht.

Diese Ziele sind:

- Sicherung der Vermögenswerte vor Verlust, Missbrauch und Schaden
- Erreichung der Organisationsziele
- Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer Abläufe
- Einhaltung von Gesetzen und Vorschriften sowie Erfüllung der Rechenschaftspflicht
- Zuverlässigkeit der betrieblichen Informationen (insbesondere des Rechnungswesens)

Das *COSO Internal Control Framework* von 2013 (siehe folgende Abbildung) definiert drei zentrale Zielsetzungen für das IKS: Operations (Abläufe, Arbeitsgänge), Reporting (Berichterstattung), Compliance (Einhaltung von Vorschriften). Diese drei Zielsetzungen werden auf alle fünf Komponenten des IKS bezogen [McNally, 2013, S. 4]:

- Steuerungs- und Kontrollumfeld
- Risikobeurteilung
- Steuerungs- und Kontrollaktivitäten
- Information und Kommunikation
- Monitoring

Weiters erstrecken sich diese Komponenten und Zielsetzungen auf alle Teile des Unternehmens, im COSO Cube als Gesamtunternehmen, Einheiten und Aktivitäten

[11] Eine absolute Gewähr wird auch bei einem sehr gut durchdachten IKS nicht geboten, da niemand mit Sicherheit die Zukunft vorhersagen kann.

dargestellt. Es sollen also alle Unternehmensbereiche in Bezug auf die fünf oben genannten Komponenten überwacht und geprüft werden [McNally, 2013, S. 4].

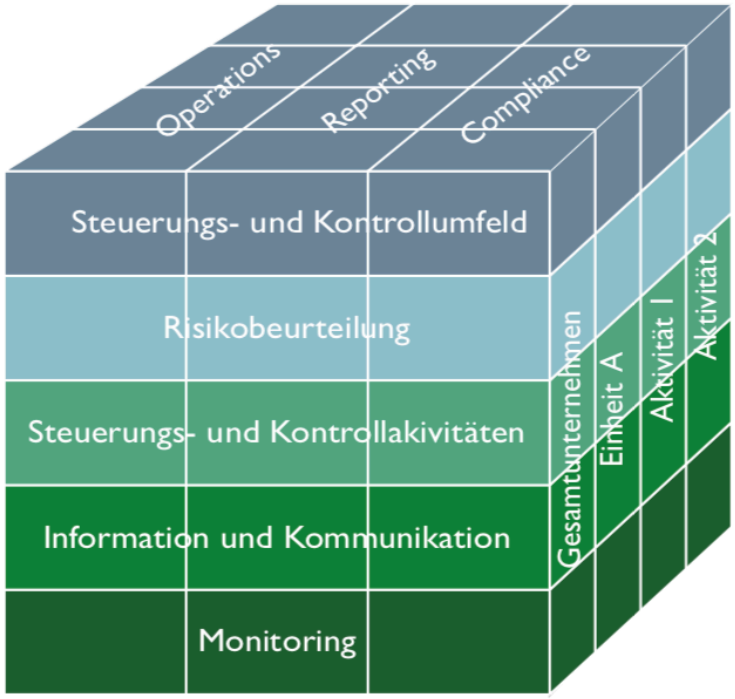


Abbildung 13: COSO Internal Control Framework 2013, Quelle: [McNally, 2013, S. 4]

Diesen Komponenten wurden 17 Prinzipien zugeordnet, die eine effektive Kontrolle widerspiegeln sollen. Diese Prinzipien werden in Abbildung 14 dargestellt.

Tabelle 6: COSO–Prinzipien effektiver Kontrolle (Stand 2013)	
Kontrollumfeld (Control Environment)	1. Bekennt sich zu Integrität und ethischen Werten 2. Nimmt Aufsichtspflichten wahr 3. Schafft Strukturen und legt Verantwortung und Zuständigkeiten fest 4. Bekennt sich zu Kompetenz 5. Fordert Verantwortung und Rechenschaftspflicht ein
Risikobeurteilung (Risk Assessment)	6. Legt angemessene Ziele fest 7. Identifiziert und analysiert bestehende Risiken 8. Bewertet Betrugsrisiken 9. Identifiziert und analysiert wesentliche Veränderungen
Kontrollaktivitäten (Control Activities)	10. Legt fest und entwickelt Kontrollaktivitäten 11. Legt fest und Entwicklung allgemeiner IT–Kontrollen 12. Setzt Richtlinien und Verfahren ein
Information & Kommunikation (Information & Communication)	13. Verwendet relevante Informationen 14. Kommuniziert intern 15. Kommuniziert extern
Überwachung (Monitoring Activities)	16. Führt laufende (prozessintegrierte) und/oder getrennte Überprüfungen durch 17. Beurteilt und kommuniziert Mängel

Abbildung 14: COSO-Prinzipien effektiver Kontrolle, Quelle: [Rechnungshof, 2016, S. 16]

Die fünf Hauptfelder sind wieder die fünf Komponenten aus dem Würfel in Abbildung 13. Mit diesen Prinzipien werden die Komponenten besser verständlich gemacht.

Doch ist nun die Risikobeurteilung Teil des IKS oder Teil des Risikomanagements?

In Tabelle 4 wird dies veranschaulicht:

Risikomanagement	**Internes Kontrollsystem**
Identifikation, Analyse und Bewertung von Risiken (Schadensausmaß und Eintrittswahrscheinlichkeit)	Festlegung von Prozessen und Verantwortlichen
IKS und RM sind untrennbar verbunden → Unternehmensrisiken sollen minimiert werden und die Unternehmensziele erreicht werden	

Tabelle 4: Abgrenzung RM – IKS, eigene Darstellung nach Quelle: [Rechnungshof, 2016, S. 12]

Das IKS soll sicherstellen, dass das Erreichen der Ziele eines Unternehmens nicht durch interne und externe Risiken verhindert wird. Diese Risiken werden im Risikomanagement evaluiert.

Welche Prinzipien beinhaltet das interne Kontrollsystem? [Rechnungshof, 2016, S. 22-24]

- *Transparenz-Prinzip*: Die Arbeitsabläufe sind klar, detailliert und transparent in schriftlicher Form geregelt und dokumentiert.
- *Kontrollautomatik / Vier-Augen-Prinzip*[12]: Kontrollen werden systematisch im Arbeitsablauf eingebaut (Kontrollautomatik), z.B. IT-gestützt oder durch Implementierung des Vier-Augen-Prinzips.
- *Prinzip der Funktionstrennung*: Es gibt keine Allein-Verantwortung für einen gesamten Prozess. Die entscheidende, ausführende und kontrollierende Funktion ist klar getrennt. (Bsp.: Produktionsplanung – Produktion – Qualitätsmanagement)
- *Prinzip der Mindestinformation*: Es wird genau die Information bereitgestellt, welche zur Erfüllung einer Aufgabe bzw. einer Verantwortung benötigt wird.
- *Prinzip der minimalen Rechte*: Zugangs- und Zugriffsberechtigungen (z.B. zu IT-Systemen, Räumlichkeiten) werden so vergeben, dass nur auf jene Daten zugegriffen werden kann, die zur Erfüllung der Aufgaben erforderlich sind.
- *IKS als rollierender Prozess*: Das IKS wird regelmäßig und systematisch auf Funktionsfähigkeit, Wirksamkeit und Aktualität überprüft. Damit wird sichergestellt, dass die internen Kontrollen nachhaltig wirksam sind und entsprechend angepasst werden, wenn sich die Rahmenbedingungen ändern.
- *Kosten-Nutzen-Abwägung*: Der Ressourceneinsatz für die Kontrollen muss in einem angemessenen Verhältnis zu den zu vermeidenden Risiken stehen.

[12] Das Vier-Augen-Prinzip ist eine Sonderform des Mehr-Augen-Prinzips. Das Ziel ist die Minimierung des Risikos von Fehlern und Missbrauch. Wichtige Entscheidungen dürfen nicht von einer einzelnen Person getroffen werden [Deutsches Vergabeportal, 2019].

4.1.5.2 Die Interne Revision

Die IR kann als eine Art Versicherung und unabhängige Prüfstelle betrachtet werden, die die folgenden Bereiche überwachen und über deren Durchführung berichten soll [IIA, 2013, S. 5]:

- alle Elemente des Risikomanagements und des IKS → von der Risikoidentifizierung, Risikoanalyse, Risikobewertung und -bewältigung über den Informationsfluss und die Kommunikation bis hin zu der Überwachung dieser Prozesse im Sinne des IKS
- die Einhaltung von Regeln, Gesetzen, Normen und Verträgen
- die Überprüfung der Effizienz und Effektivität des operativen Managements
- das Unternehmen als Ganzes – sowie Abteilungen bzw. Bereiche wie Verkauf, Marketing, Produktion, etc. – jedoch nicht im Detail, sondern die einzelnen Führungs- und Überwachungsprozesse

Für die Interne Revision wurden ebenfalls Grundsätze festgelegt, die von Internen Revisoren eingehalten und angewandt werden sollen [DIIR, 2018, S. 17]:

- Integrität: Durch Integrität entsteht Vertrauen und damit die Grundlage für die Zuverlässigkeit des Urteils der IR.
- Objektivität: Beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Prozesse ist ein Höchstmaß an Objektivität essentiell. Interne Revisoren lassen sich nicht beeinflussen und arbeiten unabhängig.
- Vertraulichkeit: Der Wert und das Eigentum der erhaltenen Informationen werden beachtet.
- Fachkompetenz: Für die Durchführung ihrer Arbeit besitzen Interne Revisoren das nötige Wissen und die nötige Kompetenz und Erfahrung.

Die Implementierung einer Internen Revision ist sehr wichtig und kann einem Unternehmen helfen, vor allem das Risikomanagement nachhaltig zu verbessern. Der positive Effekt der Implementierung einer IR in einem Unternehmen wird in einer Studie von Prof. Walter Schwaiger [Schwaiger et al., 2018] belegt. In der folgenden Abbildung ist ersichtlich, dass Unternehmen, die seit mindestens fünf Jahren (IR > 5 Jahre) eine Interne Revision als Prüforgan installiert haben, im ERMMA-Gesamt-Score deutlich besser als der Durchschnitt abschneiden.

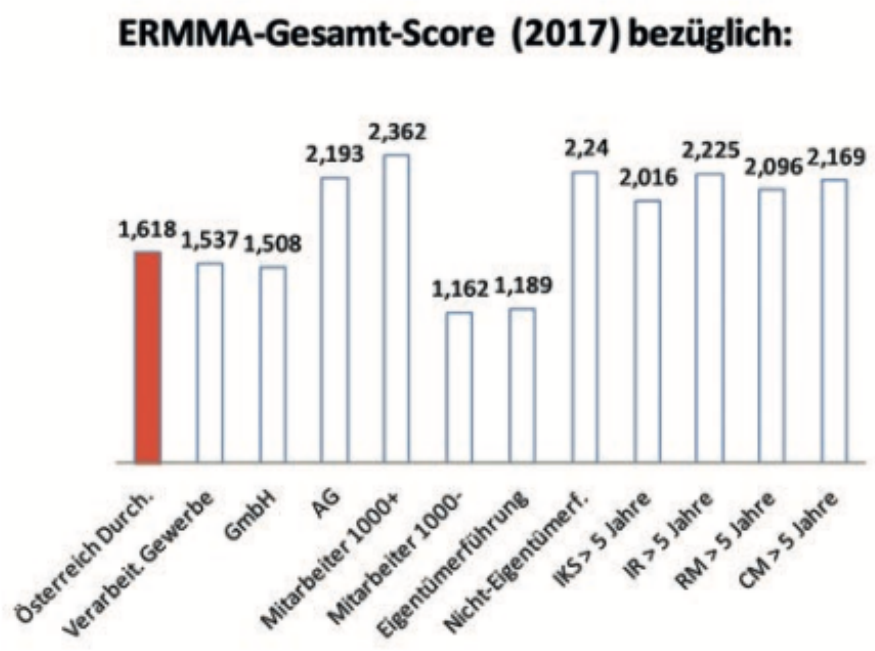


Abbildung 15: Einfluss der IR auf ERMMA-Gesamt-Score, Quelle: [Schwaiger et al., 2018, S. 9]

Der österreichische Durchschnitt dieser Studie liegt bei einem ERMMA-Score von 1,618, während Unternehmen mit einer IR, die älter als fünf Jahre ist (37 von 71 teilnehmenden Unternehmen), auf einen Wert von 2,225 kommen. Auch Interne Kontrollsysteme haben einen großen positiven Einfluss auf das Ergebnis des Tests.

Weiters kann ein eine positive Auswirkung der IR auf die Zufriedenheit der Eigentümer bzw. des Aufsichtsrats mit dem Risikomanagement-System nachgewiesen werden:

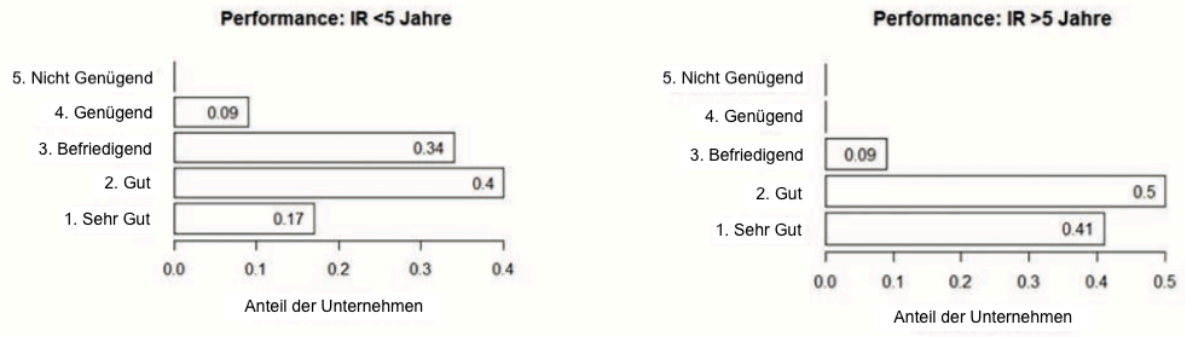


Abbildung 16: Zufriedenheit der Eigentümer mit RM-System, Quelle: [Schwaiger et al., 2018, S. 10]

In der Abbildung ist die Zufriedenheit der Eigentümer bzw. des Aufsichtsrats mit dem Risikomanagement-System dargestellt. In der linken Grafik sind jene Unternehmen abgebildet, deren IR kürzer als 5 Jahre existiert, während in den Unternehmen rechts die IR

bereits seit mehr als 5 Jahren implementiert ist. Es ist eine deutliche Verbesserung zu erkennen, die Zufriedenheit steigt mit der Dauer der IR-Tätigkeit deutlich.

4.1.6 Risikobewältigung

In der Risikobewertung wird eruiert, ob ein Risiko tragbar ist oder nicht. Kommt dabei heraus, dass es das nicht ist, müssen Maßnahmen zur Vermeidung oder Verminderung des Risikos entwickelt und umgesetzt werden.

Um Risiken zu bewältigen, gibt es verschiedene Möglichkeiten. Schon 2002 wurde durch Hölscher eine Einteilung der verschiedenen Maßnahmen vorgenommen. In der folgenden Abbildung werden diese Möglichkeiten dargestellt.

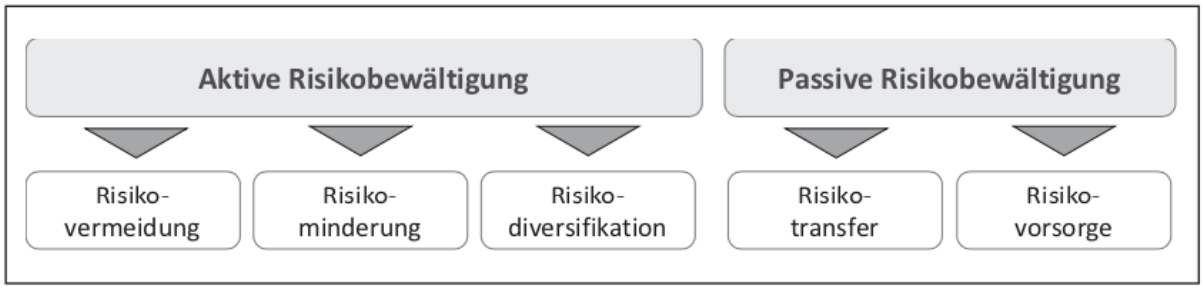


Abbildung 17: Maßnahmen der Risikobewältigung, Quelle: [Hölscher, 2002, S. 14]

In der aktiven Risikobewältigung findet man also die Vermeidung, Minderung und Diversifikation von Risiken, während die passive Risikobewältigung den Risikotransfer sowie die Risikovorsorge beinhaltet.

Diese Einteilung wurde 2013 weiterentwickelt. Diese Einteilung sieht folgendermaßen aus [Romeike et al., 2013, S. 139]:

Präventive Risikopolitik	**Korrektive Risikopolitik**	**Keine aktive Risikopolitik**
Aktive Risikobewältigung durch • Risikovermeidung • Risikominderung • Risikodiversifikation	Passive Risikobewältigung durch • Risikotransfer • Risikofinanzierung • Risikovorsorge	Risiko wird selbst übernommen
Risikostrukturen werden gestaltet! Keine oder verminderte Risikofolgen durch Verringerung der Eintrittswahrscheinlichkeit und/oder des Schadenausmaßes	Risikostrukturen bleiben unverändert! Keine oder verminderte Risikofolgen durch Vorsorge oder Abwälzen der Konsequenzen	Risikostrukturen bleiben unverändert! Eventuell „intelligentes“ Selbsttragen

Tabelle 5: Maßnahmen der Risikobewältigung, eigene Darstellung nach Quelle: [Romeike et al., 2013, S. 139]

In dieser Einteilung wird aktive Risikobewältigung als präventiv beschrieben. Das bedeutet, dass die Risikostrukturen selbst gestaltet werden, indem Maßnahmen zur Verringerung der Eintrittswahrscheinlichkeit bzw. des Schadensausmaßes getroffen werden.

Korrektive Risikopolitik hingegen beinhaltet die passive Risikobewältigung. Dabei bleiben die Risikostrukturen unverändert, durch einen Risikotransfer (beispielsweise zu einer Versicherung oder einem Vertragspartner) oder die vorsorgliche Finanzierung werden die Risikofolgen ebenfalls vermindert.

Aktive Risikobewältigung wird also durch „ursachenbezogene Maßnahmen“ geprägt, während passive Risikobewältigung „wirkungsbezogene Maßnahmen“ beinhaltet [Weißensteiner, 2014, S. 21].

Ein gewisses Restrisiko bleibt jedoch immer übrig, wenn man unternehmerische Chancen nutzen und erfolgreich realisieren will. Wenn jedoch das Risikomanagement-System gut funktioniert, ist die Risikosituation transparent und jedes identifizierte Risiko wird mithilfe adäquater Maßnahmen zu einem vertretbaren Restrisiko vermindert. Diese Vorgehensweise wird durch den Risikoappetit des Unternehmens bestimmt und sollte auch in der Risikostrategie klar formuliert und dokumentiert sein.

In der folgenden Abbildung ist ersichtlich, dass das Restrisiko auch nicht identifizierte Risiken enthält, die aufgrund des Mangels von Informationen, Wissen oder einer Fehleinschätzung nicht erfasst wurden [Weißensteiner, 2014, S. 21].

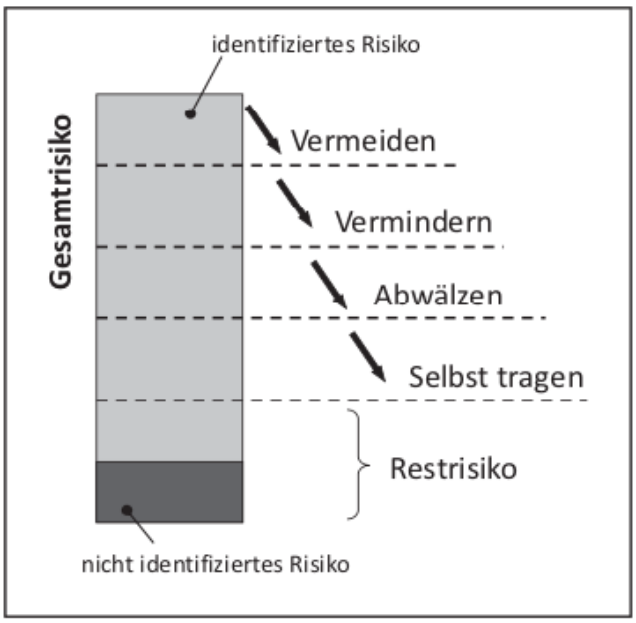


Abbildung 18: Risikoreduktion mittels Bewältigungsmaßnahmen, Quelle: [Weißensteiner, 2014, S. 21]

4.2 Unternehmensweites RM-System in der Theorie

4.2.1 COSO-Prinzipien

Die beschriebenen einzelnen Schritte sind Teil jedes Risikomanagement-Prozesses, für eine ganzheitliche Betrachtung über ein ganzes Unternehmen hinweg müssen jedoch übergeordnete Ziele definiert werden und ein Rahmen für das ERM-System geschaffen werden.

Für ein ERM-System wurden vom Committee of Sponsoring Organizations vier Zielkategorien entwickelt [COSO, 2004, S. 3]:

- Strategische Ziele – übergeordnete Ziele, die die Mission unterstützen und darauf abgestimmt sind
- Betriebliche Ziele – wirtschaftlicher und wirksamer Ressourceneinsatz
- Berichterstattung – Zuverlässigkeit
- Regeleinhaltung – Einhaltung von Gesetzen und Vorschriften

Doch die Darstellung des unternehmensweiten Risikomanagements hat sich seit COSO 2004 verändert. Im zweiten[13] COSO-Entwurf war es noch ein Würfel, der in Abbildung 19 zu sehen ist. Dabei standen die Beziehungen zwischen den Unternehmensbereichen und den Schritten zur Risikobeurteilung bzw. -steuerung im Vordergrund.

[13] Anmerkung: Der erste COSO-Entwurf wurde im Jahr 1992 herausgegeben.

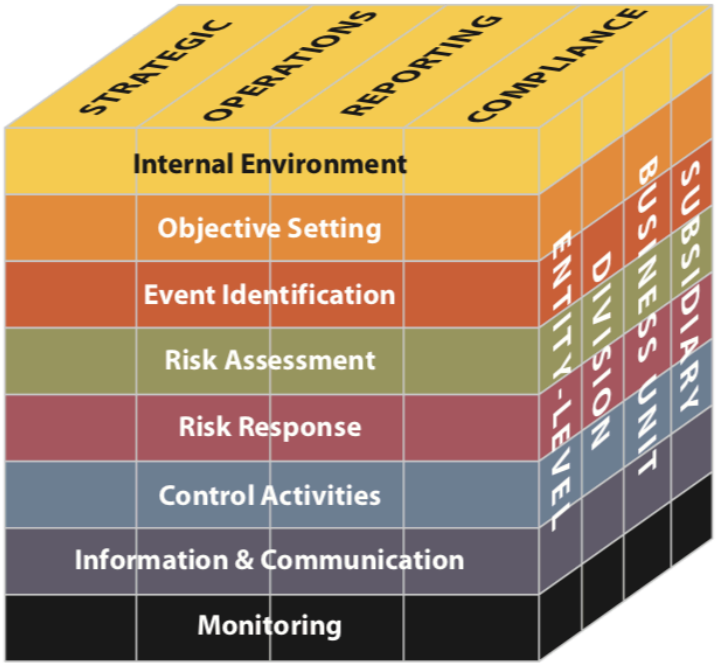


Abbildung 19: COSO Cube 2004, Quelle: [COSO, 2004, S. 5]

In der neuesten Ausgabe von 2017 wurde aus dem Würfel aus COSO 2004 ein kontinuierlicher Prozess, der in der folgenden Abbildung dargestellt wird [COSO, 2017, S. 6].

Abbildung 20: COSO Framework - Enterprise Risk Management, Quelle: [COSO, 2017, S. 6]

Der Prozess beginnt links mit „Mission, Vision & Core Values“. Das bedeutet, dass die Mission und Vision des Unternehmens sowie dessen Kernwerte vorab definiert werden. Im nächsten Schritt steht „Strategy Development“ im Vordergrund, also die Strategieentwicklung. Es folgen „Business Objective Formulation“, also die Formulierung der Unternehmensziele, und

„Implementation & Performance“, die Implementierung und Durchführung. Am Ende wird das Ziel des Prozesses, der „Enhanced Value“, also die gesteigerte Wertschöpfung erreicht.

Das COSO Framework besteht aus 20 Prinzipien, die in fünf Komponenten kategorisiert sind [COSO, 2017, S. 6]:

1. „Governance and Culture“ – Unternehmensführung und Kultur: Die Unternehmensführung bestärkt die Bedeutung des Risikomanagements und legt die Aufsichtsverantwortung desselben fest. Kultur bezieht sich auf ethische Werte, gewünschte Verhaltensweisen und ein Verständnis von Risiko im gesamten Unternehmen.
2. „Strategy and Objective-Setting“ – Strategie und Zielsetzung: ERM, Strategie und Zielsetzung arbeiten im strategischen Planungsprozess zusammen. Der Risikoappetit[14] wird festgelegt und mit der Strategie abgestimmt. Unternehmensziele setzen die Strategie in die Praxis um und dienen als Grundlage für die Identifizierung, Bewertung und Reaktion auf Risiken. Die Risikostrategie und deren Inhalt bzw. Funktion wird im Kapitel *Risikostrategie: Theorie und praktische Umsetzung* erläutert.
3. „Performance“ – Durchführung: Risiken, die das Erreichen der Unternehmensziele beeinflussen könnten, werden identifiziert und bewertet. Sie werden nach Dringlichkeit im Rahmen des Risikoappetits priorisiert. Maßnahmen zur Risikobewältigung werden ausgewählt und die Höhe des eingegangenen Risikos wird in einem Portfolio dokumentiert. Die Ergebnisse dieses Prozesses werden an die wichtigsten Risikoverantwortlichen berichtet. Das Kapitel *ERM-Prozess und Organisation: Praktische Umsetzung in Industrie-EWF* beinhaltet die Durchführung.
4. „Review and Revision“ – Überprüfung und Revision: Durch die Überprüfung der Leistung des Unternehmens kann beurteilt werden, wie gut die ERM-Komponenten im Laufe der Zeit und während wesentlicher Veränderungen funktionieren und welche Anpassungen nötig sind. Das vierte Prinzip ist ebenfalls im Kapitel *ERM-Prozess und Organisation: Praktische Umsetzung in Industrie-EWF* zu finden.
5. „Information, Communication and Reporting“ – Information, Kommunikation und Berichterstattung: ERM benötigt einen kontinuierlichen Informationsfluss bzw. -

[14] Absicht, bewusst bestimmte Risiken einzugehen; spiegelt den Ausglich von Leistung, Wachstum, Ertrag und Risiko einer Organisation wider (Im Gegensatz dazu – Risikoaversion) [ONR 49000, 2014, S. 11]

austausch aus internen und externen Quellen, und zwar nach oben und unten in der Unternehmenshierarchie. Der kontinuierliche Informationsfluss ist wie die Überprüfung und Revision Teil des Kapitels *ERM-Prozess und Organisation: Praktische Umsetzung in Industrie-EWF*.

Diese Zielkategorien und Prinzipien spiegeln Werte wider, die bei der Umsetzung eines unternehmensweiten Risikomanagement-Systems beachtet werden sollen. Jedoch bergen sie keine organisationalen Umsetzungsvorschläge.

4.2.2 3-Lines-Of-Defense – die organisationale Umsetzung der COSO-Prinzipien

Das „3-LOD – 3-Lines-Of-Defense"-Modell (3-LOD-Modell) geht einen Schritt weiter und bietet ein Rahmenwerk für ein unternehmensweites RM-System. Dieses Referenzmodell grenzt die verschiedenen Funktionen des Risikomanagements voneinander ab. In der folgenden Abbildung wird dieses Modell schematisch dargestellt:

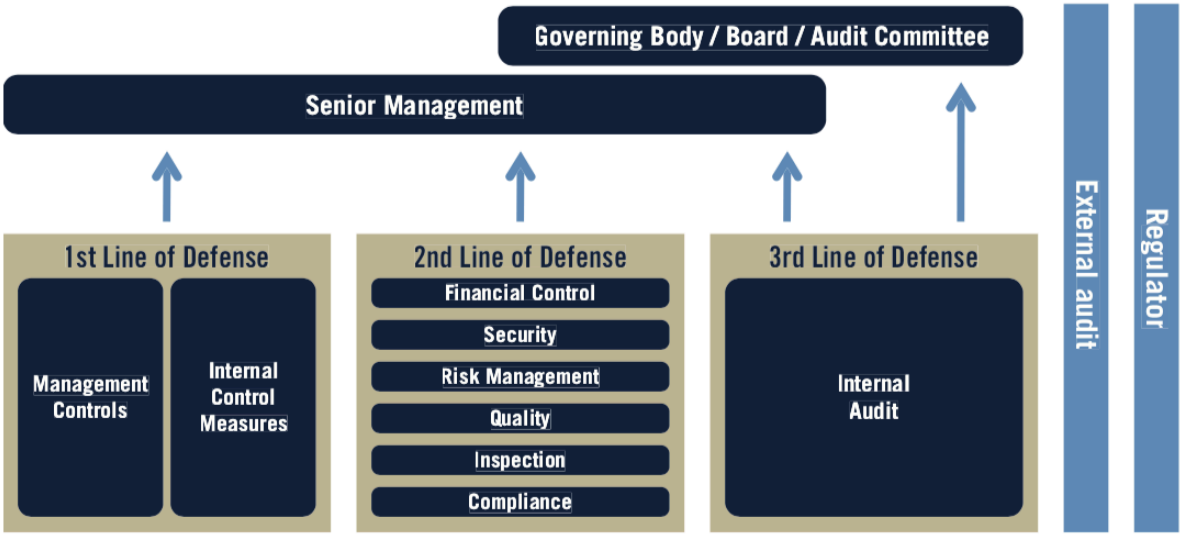


Abbildung 21: Three Lines of Defense Modell, Quelle: [IIA, 2013, S. 2]

Das 3 LOD Modell wurde in dieser Form vom internationalen Verband der Auditoren entwickelt und beinhaltet drei Verteidigungslinien, die dazu dienen, eine Struktur in den RM-Prozess eines ganzen Unternehmens bringen zu können. Weder die Geschäftsführung (Senior Management) noch der Aufsichtsrat (oder vergleichbare Prüfungsausschüsse –Governing Body / Board / Audit Commitee) sind Teil der drei Verteidigungslinien, sie spielen jedoch eine große Rolle und sind die Stellen im Unternehmen, an die berichtet wird. Außerdem sind sie

essentiell in ihrer Unterstützerrolle, um ein unternehmensweites RM-System implementieren zu können [IIA, 2013, S. 2-3].

Auf der rechten des Schemas werden auch externe Prüfer (External Audits) und Regulierungsbehörden (Regulators) erwähnt, um zu zeigen, dass diese in den Prozess integriert werden sollen.

4.2.2.1 Die 1. Line of Defense

Abbildung 22: First Line of Defense, Quelle: [IIA, 2013,. S. 2]

Die erste Verteidigungslinie beinhaltet sämtliche Funktionen, die Risiken im Tagesgeschäft managen. Das inkludiert die Identifizierung, Analyse, Beurteilung und Bewältigung von Risiken, Kontrollaktivitäten im Sinne des IKS und Informationsbereitstellung bzw. Kommunikation [Anderson, Eubanks, 2015, S. 5].

Man kann also die 1. LOD dem operativen Management[15] zuordnen, da dort die meisten Risiken auftreten und auch zuallererst damit umgegangen werden muss. Das operative Management ist auch dafür verantwortlich, erste interne Kontrollen durchzuführen und den RM-Prozess durchzuführen [IIA, 2013, S. 3].

[15] Unter operativem Management versteht man das Managen des Betriebsalltags. Teil davon sind sämtliche Prozesse, die den kurzfristigen Ablauf in einem Unternehmen betreffen. Dazu gehören die Produktionsplanung, Sicherstellung der Kommunikation, die Bereitstellung von Material, Personal und Betriebsmitteln → also der vom strategischen Management vorgegebene laufende Betrieb. Der Planungshorizont beträgt meist maximal ein Jahr.

4.2.2.2 Die 2. Line of Defense

Abbildung 23: Second Line of Defense, Quelle: [IIA, 2013, S. 2]

In der zweiten Verteidigungslinie stehen Kontrolle und Übersicht im Vordergrund. Wie auch die 1. LOD untersteht die zweite Verteidigungslinie der Geschäftsführung.

Die Funktionen, die der 2. LOD zugeordnet sind, arbeiten stets eng mit dem operativen Management in der 1. LOD zusammen, um es bei verschiedenen Funktionen zu unterstützen. Dazu gehören die folgenden Aufgabengebiete [IIA, 2013, S. 4-5]:

- Implementierung und Kontrolle des Risikomanagement-Systems – Dazu gibt es in der 2. LOD einen (oder mehrere) RM-Verantwortlichen, der die Implementierung überwacht und den Risiko-Verantwortlichen in den einzelnen Prozessen dabei hilft, Zielsetzungen zu definieren und risikorelevante Informationen im Unternehmen zu verbreiten (bzw. an die richtigen Stellen weiterzuleiten)
- Compliance-Funktion – Die Vereinbarkeit von Risiken mit Gesetzen und Regulatorien wird ebenfalls in der 2. LOD überprüft.
- Finanz-Controlling – Mit Hilfe des Finanz-Controllings werden finanzielle Risiken überwacht und Probleme in diesem Bereich aufgedeckt und an die GF berichtet.
- Folgende Funktionen sind ebenfalls Teil der zweiten Verteidigungslinie [Anderson et al., 2015, S. 6-7]:
    - Qualitätsmanagement und Qualitätsüberprüfung
    - Gesundheit, Umwelt und Sicherheit (auch Informationssicherheit)
    - die Rechtsabteilung
    - Supply Chain Management

Diese Funktionen werden vom Management implementiert, um sicherzustellen, dass die erste Verteidigungslinie richtig konzeptioniert wurde und auch so ausgeführt wird. In der 2. LOD werden außerdem Informationen generiert, die den unternehmensweiten Status im jeweiligen Bereich widerspiegeln und an die Geschäftsführung weitergegeben werden bzw. in Berichten dokumentiert werden. Die Vernetzung sowohl mit der Geschäftsführung als auch mit dem operativen Bereich ist essentiell für eine gute Verteidigungslinie.

4.2.2.3 Die 3. Line of Defense

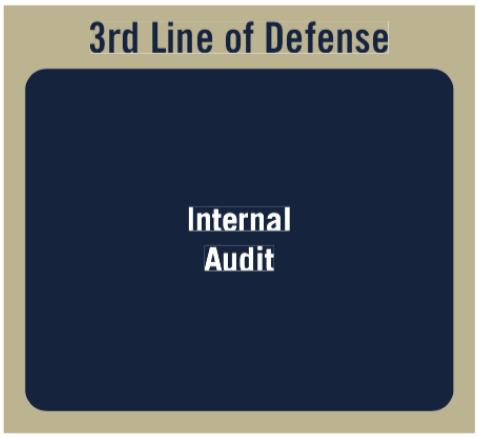


Abbildung 24: Third Line of Defense, Quelle: [IIA, 2013, S. 2]

Die 3. LOD besteht aus der Internen Revision (IR), welche verschiedene Bereiche eines Unternehmens prüft, jedoch mit Hauptaugenmerk auf das Risikomanagement-System sowie die Führungs- und Überwachungsprozesse (IKS). Um diese Prüfungen zufriedenstellend durchführen zu können, muss die IR gut über die Anforderungen der Geschäftsführung an das RM-System informiert sein, Kenntnis über die zu prüfenden Bereiche haben und fähig sein, als beratende Funktion diese Bereiche zu unterstützen. Bei der Durchführung ihrer Aufgaben muss die IR jedoch stets objektiv und unabhängig agieren [Schwaiger et al., 2018, S. 4].

Die Unabhängigkeit grenzt die dritte Verteidigungslinie auch deutlich von den ersten beiden ab → Berichte gehen von der Internen Revision nicht nur an die Geschäftsführung, sondern auch an den Aufsichtsrat [Anderson et al., 2015, S. 7-9].

Wie werden die drei Lines-of-Defense strukturiert bzw. koordiniert?

Das Modell muss aus dem Grund, dass jedes Unternehmen verschiedene Anforderungen und Ziele hat, immer individuell angepasst werden. Wichtig ist jedoch, dass die Verteidigungslinien klar definiert werden. Je besser sie voneinander abgegrenzt werden, desto besser funktionieren sie auch. Diese Abgrenzung entsteht aus der Rollenverteilung, die jeder Verteidigungslinie zugewiesen ist. In der folgenden Abbildung ist diese Rollenverteilung ersichtlich:

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	**Risk Control and Compliance**	**Risk Assurance**
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

Abbildung 25: Rollenverteilung in den Three-Lines-of-Defense, Quelle: [IIA, 2013, S. 6]

Das operative Management findet sich also in der 1. LOD. Darin inkludiert sind die Risiko-Owner bzw. die Prozessverantwortlichen. Dazu gehört auch die Implementierung eines IKS.
In der 2. LOD findet die Steuerung bzw. Kontrolle des Risikomanagements statt. Ergebnisse des RM-Prozesses aus der ersten Verteidigungslinie werden an die Geschäftsführung berichtet.
Die 3. LOD besteht aus der Internen Revision, welche als Versicherung und Beratungsfunktion fungiert. Die IR ist unabhängig von den restlichen Abteilungen und berichtet zwar an die Geschäftsführung, jedoch ebenso an den Aufsichtsrat.

5 ERM-Prozess und Organisation: Praktische Umsetzung in Industrie-EWF

Um den Risikomanagement-Prozess in der Industrie-EWF zu verbessern und ein unternehmensweites RM-System daraus zu entwickeln, werden die im vorherigen Kapitel angeführten theoretischen Rahmenbedingungen in praxisorientierte Konzepte umgewandelt, die es dann umzusetzen gilt. Dafür wurden abermals die Dimensionen RM-Prozess und Risikoorganisation gemeinsam betrachtet.

Die COSO-Komponenten, die ebenfalls im vorangegangenen Kapitel beschrieben wurden, dienen hier als Orientierungshilfe. Drei der fünf Komponenten finden sich im Risikomanagement-Prozess wieder.

Die dritte Komponente, die „Performance“, betrifft die Durchführung des Risikomanagement-Prozesses, also sämtliche Schritte von der Risikoidentifizierung bis zur Risikobewältigung.

In „Information, Communication and Reporting”, der fünften Komponente, findet sich die Kommunikation, also der Informationsfluss NEU, sowie die Berichterstattung.

„Review and Revision“, die vierte Komponente, bezieht sich auf das Interne Kontrollsystem und die Interne Revision.

5.1 Optimierung des Risikomanagement-Prozesses: Praktische Umsetzung

Der wichtigste Schritt dabei ist die Verbindung der einzelnen Methoden. Die Informationen, die aus den einzelnen RM-Prozessen generiert werden, müssen kommuniziert werden und in einer unternehmensweiten Risikolandkarte zusammenfließen. Nur so kann gewährleistet werden, dass möglichst wenige Risiken übersehen werden und ein Gesamtbild des Risikos in der Industrie-EWF erschaffen wird.

Um dieses Zusammenspiel zu verdeutlichen, wird der Informationsfluss überarbeitet:

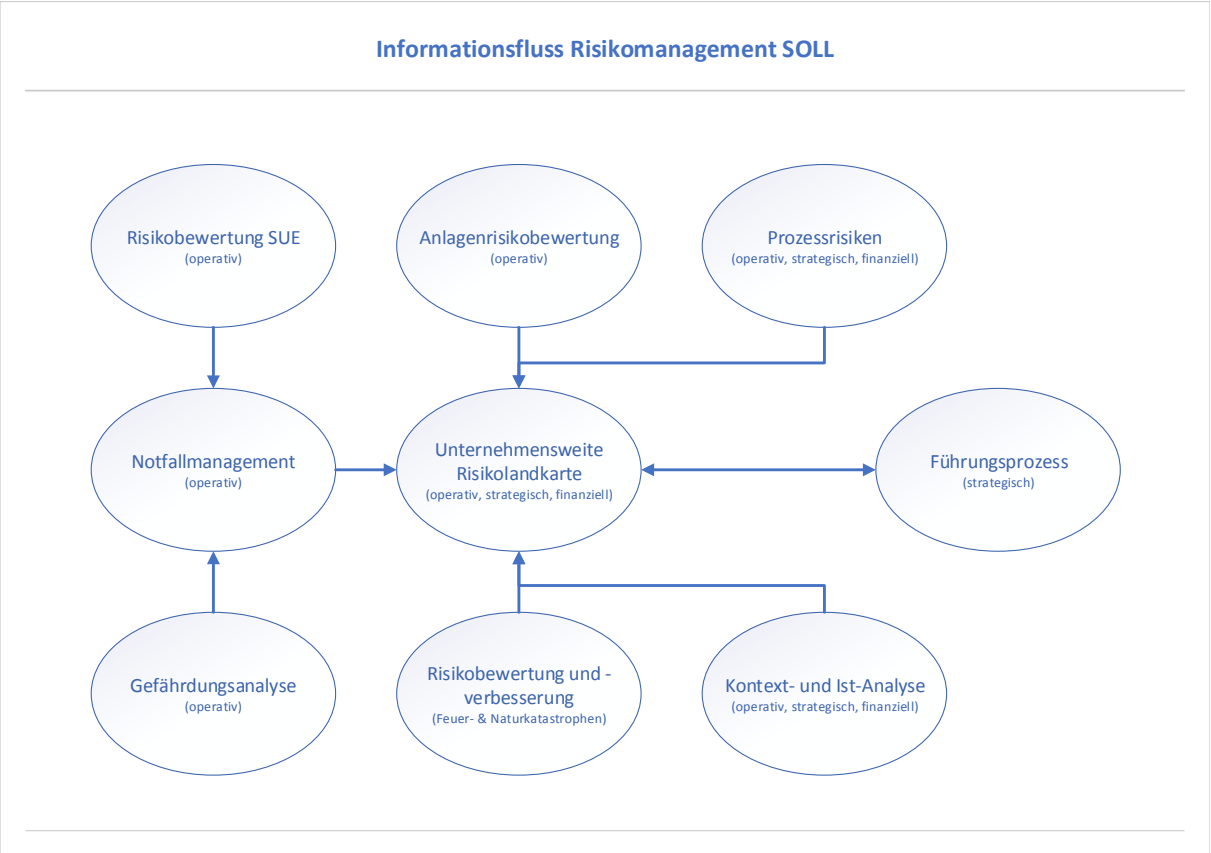


Abbildung 26: Informationsfluss Risikomanagement SOLL

Darin ist auf den ersten Blick zu erkennen, dass keine abgeschotteten Blasen mehr existieren, sondern alle einzelnen RM-Prozesse miteinander verbunden sind. Das Zentrum des Informationsflusses bildet die unternehmensweite Risikolandkarte. Darin werden die wichtigsten Informationen der einzelnen RM-Prozesse vereinigt. Um den Überblick zu wahren, werden nicht alle Details darin dargestellt.

Aus den folgenden Einzelprozessen fließen Informationen in die unternehmensweite Risikolandkarte:

- Notfallmanagement – dieses wird mit Informationen gefüttert aus
    - Risikobewertung SUE
    - Gefährdungsanalyse
    - Risikobewertung und -verbesserung für Feuer- und Naturgefahren
- Anlagenrisikobewertung
- Prozessrisiken
- Kontext- und Ist-Analyse

Mit dem Führungsprozess entsteht daraus eine Wechselwirkung. Einerseits werden die Informationen aus der unternehmensweiten Risikolandkarte verwendet, um an die Geschäftsführung, die Teil des Führungsprozesses ist, zu berichten. Andererseits wird im Führungsprozess die Richtung vorgegeben, in die sich die Risikolandkarte entwickeln soll.

Die *Prozessrisiken* dienen als Überblick für sämtliche Prozesse der Prozesslandkarte. Darin findet sich eine überblicksmäßige Risikoidentifikation und Maßnahmen zur Gegensteuerung, die vom jeweiligen Prozessverantwortlichen definiert wurden. Wichtig dabei ist jedoch, dass in den Prozessrisiken nicht alle Risiken im Detail behandelt werden sollen. Das hat den Grund, dass in der Industrie-EWF operative Risiken vorherrschend sind, welche aber mit Hilfe der anderen RM-Funktionen genau betrachtet werden. Für Prozesse, die jedoch nicht direkt mit dem operativen Bereich zusammenhängen, dienen die Prozessrisiken als Basis für eine überblicksmäßige Risikoidentifikation und -bewertung. Sehr wichtig ist, dass in den Prozessrisiken nicht nur Risiken, sondern auch Chancen angeführt werden. Diese soll ebenfalls in jedem Prozess inkludiert werden, damit man wirklich einen vollständigen Überblick erhält.

Detaillierter wird es in der *Anlagenrisikobewertung*, sowie im *Notfallmanagement*, das Informationen von der *Risikobewertung SUE* und der *Gefährdungsanalyse* erhält. Die *Risikobewertung für Feuer- und Naturgefahren* wird hier zwar noch erwähnt, ist aber kein laufender Prozess, da sich diese Vorschläge hauptsächlich auf bauliche Veränderungen beziehen und diese schon großteils umgesetzt wurden. Aus diesem Grund werden die Feuer- und Naturgefahren im laufenden Prozess nicht inkludiert.

Um ein funktionierendes unternehmensweites RM-System zu erhalten, sollen, wie im Informationsfluss dargestellt, die einzelnen Methoden des RM-Prozesses verbunden und standardisiert werden.

Im ersten Schritt soll definiert werden, wie der Teilprozess der **Risikoidentifizierung** gehandhabt werden soll. Bisher wurden Experten-Interviews durchgeführt. Das hat in der Vergangenheit sehr gut funktioniert, weswegen hier auch empfohlen wird, dass diese Methode beibehalten wird. In der Industrie-EWF werden Facharbeiter sehr gut aus- bzw. weitergebildet und gefördert, aus diesem Grund haben Prozessverantwortliche bzw. Risiko-Owner viel Know-How und Erfahrung und können sehr gut einschätzen, welche Risiken auftreten und wie sie bewertet werden sollen. Weiters kommt hinzu, dass in Zukunft mit Hilfe von Schulungen im Risikomanagement das Risikoverständnis verbessert werden soll. So können neben Risiken auch Chancen erfasst werden.

Als weitere Methode wird ein Risikokatalog in Form einer Checkliste verwendet. Diese Checkliste wird vom Risikomanager erstellt und funktioniert folgendermaßen:
Alle Bereiche der Industrie-EWF werden angeführt, inklusive der Probleme, die dort auftreten können. Im ersten Schritt wird dies überblickmäßig mit den Bereichsleitern abgearbeitet. Stellt sich heraus, dass in einem Bereich signifikante Veränderungen auftreten, die eine genauere Betrachtung durch den Risikomanager benötigen, wird im nächsten Schritt eine Ebene tiefer gegangen. Die Risiken bzw. Chancen, durch die die Veränderungen hervorgerufen werden, sollen nun genau analysiert und bewertet werden. Gemeinsam mit dem Bereichsleiter werden Maßnahmen zur Bewältigung ausgearbeitet.

Mit Hilfe dieser beiden Methoden, die einerseits Bottom-Up[16], andererseits Top-Down[17] funktionieren, können möglichst alle Risiken und Chancen erfasst werden.

[16] Unter Bottom-Up versteht man eine Methode, bei der zunächst detaillierte Teilprobleme und dann mit deren Hilfe größere, darüber liegende Probleme gelöst werden [Lackes, 2019].
[17] Im Gegensatz zum Bottom-Up-Prinzip wird bei der Top-Down-Methode von „oben“ nach „unten“ ein Gesamtproblem in mehrere Teilprobleme aufgeteilt, welche dann immer detaillierter betrachtet werden [Müller-Stewens, 2019].

Der nächste Schritt ist eine einheitliche **Risikoanalyse** und **Risikobewertung**. In der folgenden Tabelle wird dargestellt, wie bisher das Risiko in den einzelnen Bereichen bewertet wird und wie es in Zukunft durchgeführt werden soll:

RM-Prozess	Bewertungsmethode IST	Bewertungsmethode NEU
Prozessrisiken	/	Zweidimensionale Risk Map mit Eintritts-wahrscheinlichkeit und Auswirkung/Schadensausmaß
Anlagenrisikobewertung	Eigene Risikozahl	
Notfallmanagement	Risk Map	
Risikobewertung SUE	Risikokennzahl (Ausmaß*Wahrscheinlichkeit)	
Gefährdungsanalyse	Risikokennzahl	

Tabelle 6: Bewertungsmethoden der RM-Prozesse

Als Bewertungsmethode NEU soll eine zweidimensionale Risk Map mit dem Dimensionen Eintrittswahrscheinlichkeit und Auswirkung verwendet werden. Diese Methode soll in allen einzelnen operativen RM-Prozessen eingeführt werden. Dafür soll grundsätzlich auch das gleiche Schema verwendet werden, jedoch werden einzelne Anpassungen benötigt, da beispielsweise ein Maschinenausfall (finanzieller Schaden) anders bewertet wird als ein Arbeitsunfall (gesundheitlicher Schaden).

Die Risikolandkarte kann wie folgt aussehen:

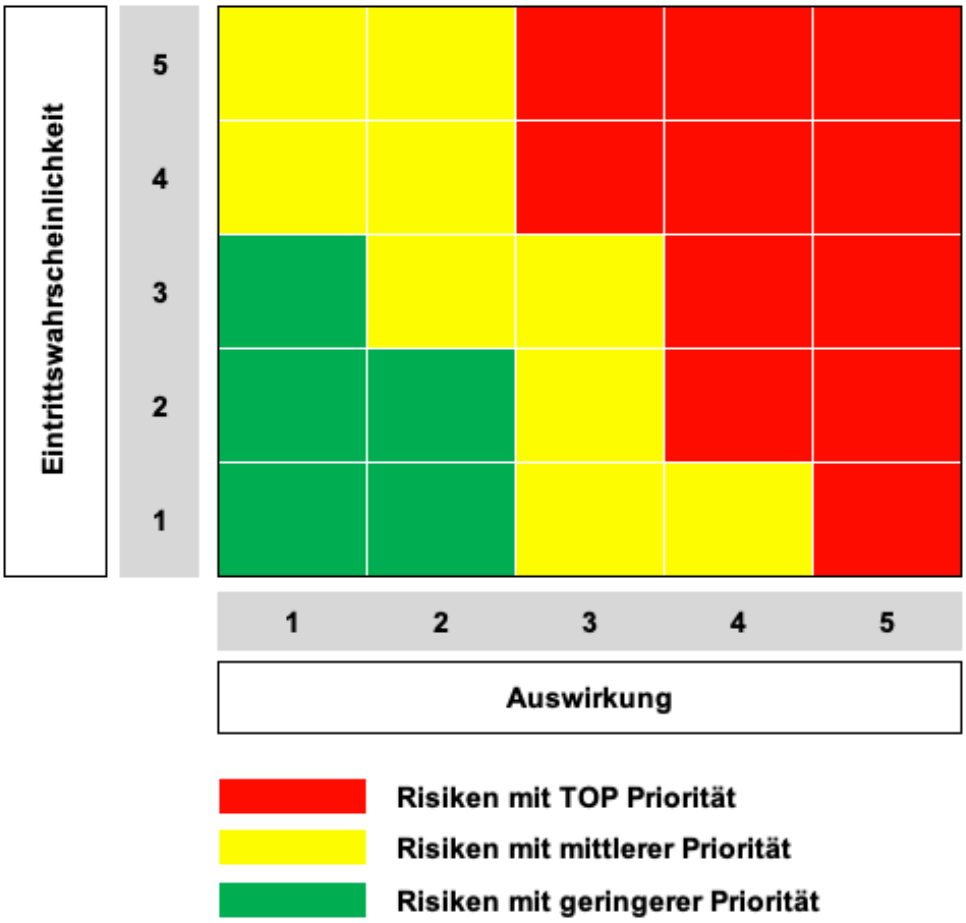


Abbildung 27: Risikolandkarte Industrie-EWF

Die Eintrittswahrscheinlichkeit und die Auswirkung bzw. das Schadenspotential werden jeweils in fünf Stufen gegliedert. Diese Gliederung sieht wie folgt aus:

Klasse	Auswirkung	Bandbreite (EUR)	Eintritts-wahrscheinlichkeit	Bandbreite (%)	entspricht
5	Katastrophal	> 3 Mio.	Sehr wahrscheinlich	> 80	< 1 Jahr
4	Kritisch	> 1 Mio.	Eher wahrscheinlich	60 – 79	1 – 3 Jahre
3	Spürbar	> 500 Tsd.	Wahrscheinlich	40 – 59	3 – 5 Jahre
2	Gering	> 100 Tsd.	Eher unwahrscheinlich	10 – 39	5 – 10 Jahre
1	Unbedeutend	< 100 Tsd.	Sehr unwahrscheinlich	< 10	> 10 Jahre

Tabelle 7: Einteilung Eintrittswahrscheinlichkeit und Auswirkung

Wurden die Risiken mit Hilfe der Eintrittswahrscheinlichkeit und des Schadensausmaßes bewertet, werden die dabei entstehenden Resultate in die jeweilige Risk Map eingetragen. Dabei muss keine Zahl von 1 bis 5 herauskommen, es kann manchmal auch eine Dezimalzahl zu einer genaueren Bewertung führen, vor allem bei Risiken mit gravierenden Konsequenzen, die man möglichst genau bewerten sollte.

Für die *Prozessrisiken* kann das genauso umgesetzt werden.

In der *Anlagenrisikobewertung* wird bisher ein dreistufiges Bewertungsschema verwendet, diese soll auf 5 Stufen erweitert werden. Außerdem soll in Zukunft die Eintrittswahrscheinlichkeit für einen Schaden dazukommen. In diese Wahrscheinlichkeit kann die bisher genutzte Wartungszahl einfließen, da anhand von statistischen Daten und/oder Erfahrungen meist eingeschätzt werden kann, wie sehr der Abstand zur letzten Wartung die Wahrscheinlichkeit für einen Schadenseintritt beeinflusst.

Die einzelnen Kriterien, also Risiko Produkt, Risiko Planung, der Anlagenzustand und die Antriebstechnik können weiterhin verwendet werden (mit 5 Stufen), sollen jedoch für eine

Darstellung in der Risk Map aggregiert werden. Da die Anlagenrisikobewertung nicht nur dem Risikomanagement dient, sondern auch der Instandhaltung, ist es nicht sinnvoll, die Verwendung dieser Einzelkriterien einzustellen. Um eine Zahl aus den vier Kriterien zu erhalten, kann der Durchschnitt gebildet werden, oder auch eine Einschätzung des Gesamtzustands einer Anlage durch den Experten erfolgen.

Im *Notfallmanagement* wird bereits eine Risk Map verwendet, die auch für die zuvor dargestellte Risikolandkarte inklusive der Bewertungskriterien herangezogen wurde. Aus diesem Grund muss hier nichts verändert werden, die Risikoanalyse und -bewertung funktioniert hier schon sehr gut.

In der *Risikobewertung SUE* wird die Bewertung ebenfalls noch anders durchgeführt. Es wird eine Risikokennzahl verwendet, die aus der Auswirkung und der Eintrittswahrscheinlichkeit zusammengesetzt ist. Für die Auswirkung geht die Skala in sechs Stufen von 1-100, diese soll an die empfohlene Gliederung (1-5) angepasst werden. Die Einteilung der Auswirkungen muss hier jedoch anhand anderer Kriterien erfolgen, da ein Personen- oder Umweltschaden nicht mit einem finanziellen Schadenswert beschrieben werden kann. Die Skala der Eintrittswahrscheinlichkeit geht von 1-10, dies erfolgt bereits in fünf Stufen, weshalb eine Anpassung an die standardisierte Gliederung kein Problem darstellt.

Die Bewertungsmethode der *Gefährdungsanalyse* erfolgt ähnlich wie in der Risikobewertung SUE. Der Unterschied ist jedoch, dass weder die Auswirkung noch die Eintrittswahrscheinlichkeit in Stufen eingeteilt sind. Auch hier soll in Zukunft eine Bewertung von 1-5 erfolgen.

Der Nachteil der Risikolandkarten ist, dass Chancen darin keinen Platz finden. Diese sollen jedoch ebenfalls identifiziert und mit Hilfe einer Eintrittswahrscheinlichkeit und eines Ausmaßes bewertet werden. Dieses Ausmaß ist kein Schaden, sondern beispielsweise eine potentielle Einsparung oder ein möglicher Gewinn.

Wurde die Bewertung der Risiken in den einzelnen RM-Prozessen angepasst, sollen durch den Prozessverantwortlichen die wichtigsten und relevantesten Risiken und Chancen

herausgehoben und für den Risikomanager zusammengefasst werden, um neben der Integration der Risiken in die Risikolandkarten auch für die Aufarbeitung der Checkliste vorbereitet zu sein.

Für den Schritt der **Risikobewältigung** werden großteils Maßnahmen herangezogen, die bereits bei der Risikoidentifizierung definiert wurden. Im Zuge der Experten-Interviews begibt man sich nicht nur auf die Suche nach den Risiken selbst, sondern stellt sich ebenfalls gleich die Frage, welche Maßnahmen diesen Risiken entgegenwirken können.

Dafür soll (wie es beispielsweise in der Gefährdungsanalyse im Notfallmanagement bereits durchgeführt wird) nach der Erforschung der Maßnahmen eine Neubewertung der Risiken erfolgen. Mit Hilfe einer zweiten Risk Map, die bereits die neu bewerteten Risiken enthält, erkennt man sogleich, wie sich die Maßnahmen auswirken und welchen positiven Veränderungen sie mit sich bringen (können). Weiters soll eruiert werden, ob die Verbesserung in einem wirtschaftlichen Verhältnis zu den damit verbundenen Kosten steht.

Ein weiterer wichtiger Punkt der Risikobewältigung ist ein gut durchdachtes Krisenmanagement. In der Industrie-EWF wird bereits ein sogenannter Krisenmonitor eingesetzt, der mit Hilfe bestimmter Indikatoren (z.B. Umsatzentwicklung, Marktverhalten, DAX-Entwicklung, etc.) erste Anzeichen einer potentiellen Krise wiedergibt. Auch wenn diese Indikatoren nur einen Überblick über das wirtschaftliche Geschehen darstellen, sind sie trotzdem eine gute Warnung, um sich bestimmte Entwicklungen genau anzusehen.

Der Großteil der operativen Risiken lässt sich durch aktive Risikobewältigung steuern, da man auf historische Daten sowie auf qualifizierte Experten zurückgreifen kann. So können die identifizierten Risiken vermieden und vermindert werden, die Risikostrukturen werden somit selbst gestaltet.

Naturgefahren lassen sich aktiv nicht beeinflussen, sie werden passiv bewältigt, beispielsweise durch einen Risikotransfer zu einer Versicherung. Dabei bleiben die Risikostrukturen zwar unverändert, die Konsequenzen treffen jedoch nicht überraschend ein. Der Risikotransfer kann jedoch nicht zu 100% erfolgen, da im Falle einer Naturkatastrophe die Produktion so

gravierend darunter leiden könnte, dass sie eingestellt werden muss, was sehr schwerwiegende Konsequenzen zur Folge hätte.

So bleibt stets ein gewisses Restrisiko, einerseits durch Gefahren, die nicht beeinflusst werden können, andererseits durch Risiken, die nicht erkannt oder falsch eingeschätzt wurden.

Der letzte Schritt im RM-Prozess ist das **Risikoreporting**. Die aus der Identifikations-, Bewertungs- und Bewältigungsphase gewonnenen Daten und Informationen sollen aggregiert werden, um eine Basis für unternehmerische Steuerungsentscheidungen zu schaffen [Weißensteiner, 2014, S. 22].

Die Informationen aus den einzelnen RM-Prozessen werden hauptsächlich für das zentrale Risikomanagement zusammengestellt. Vom Risikomanager werden diese Ergebnisse dann für die Geschäftsführung aufbereitet und präsentiert bzw. besprochen.

5.2 Überwachung und Überprüfung: Praktische Umsetzung

5.2.1 Optimierung des Internen Kontrollsystems

Die in der Theorie beschriebenen Maßnahmen eines IKS [Rechnungshof, 2016, S. 22-24] wurden in der Industrie-EWF schon großteils implementiert. In einigen Bereichen fand dies allerdings ohne das Bewusstsein, dass es sich dabei um IKS-Maßnahmen handelt, statt.

Folgende Maßnahmen sind bereits Teil der Unternehmenskultur der Industrie-EWF:

- *Transparenz*: Die Prozessabläufe sind durchgängig im Unternehmen in schriftlicher Form dokumentiert.
- *Vier-Augen-Prinzip*: Dieses Kontrollprinzip ist Standard in der Industrie-EWF und findet in allen Unternehmensbereichen Anwendung.
- *Prinzip der minimalen Rechte*: Für alle IT-Bereiche und Räumlichkeiten werden Zugriffsberechtigungen vergeben. In dieser Hinsicht ist man in der Industrie-EWF sehr streng, damit keine Daten für Personen, die sie weder benötigen noch Zugriff darauf haben sollten, zugänglich werden.

Die anderen angeführten Maßnahmen werden bis dato teilweise oder gar nicht umgesetzt:

- *Prinzip der Funktionstrennung*: Die kontrollierende Funktion ist in der Industrie-EWF in manchen Arbeitsbereichen identisch mit der planenden oder ausführenden Funktion. Damit findet nicht überall eine klare Trennung der Funktionen statt. Die Interne Revision kann als kontrollierendes Organ eingesetzt werden, jedoch nicht in jedem Bereich, da dies schlicht zu umfangreich wäre. Deswegen wird empfohlen, das Prinzip der Funktionstrennung stärker zu forcieren. Um die Umsetzung dieses Prinzips und dessen Einhaltung zu überprüfen, eignet sich die IR sehr gut.
- *Prinzip der Mindestinformation*: Manche Mitarbeiter erhalten Informationen, die sie zur Erfüllung ihrer Aufgabe nicht benötigen. Die Überprüfung dessen ist naturgemäß sehr schwierig. Deswegen soll durch vertrauensbildende Maßnahmen die Sensibilisierung verbessert und das „Streben“ nach nicht benötigten Informationen verringert werden. Ein Hauptgrund dafür, warum ein Mitarbeiter Informationen besitzen möchte, die er nicht benötigt, ist, dass er sich aus einem Vertrauenskreis ausgeschlossen fühlt. Da dies nicht die Intention ist, kann durch ein besseres Vertrauen ebendiese Sorge minimiert werden.

- *Überprüfung des IKS*: Das Interne Kontrollsystem wird noch gar nicht überprüft. Diese Überprüfung soll in Zukunft zum Aufgabenbereich der Internen Revision gehören. Sie soll einerseits regelmäßig und systematisch zu festgelegten Zeitpunkten, andererseits auch stichprobenartig zu unregelmäßigen Zeitpunkten erfolgen.
- *Kosten-Nutzen-Abwägung*: Die Effizienz und Effektivität der Kontrollmaßnahmen werden bereits überprüft, jedoch nur für jene, die schon implementiert sind. Bei der Ausweitung der Kontrollmaßnahmen wird auch eine Kosten-Nutzen-Abwägung eine Rolle spielen.

Die Umsetzung der noch ausstehenden und die Weiterführung der bereits implementierten Maßnahmen soll zu einem umfassenden Internen Kontrollsystem führen, das einen großen Teil dazu beiträgt, Risiken zu minimieren und im Zuge dessen die Wirtschaftlichkeit und Effizienz der Industrie-EWF nachhaltig zu verbessern.

5.2.2 Implementierung der Internen Revision

Die Interne Revision überprüft und berät den Risikomanager und die Verantwortlichen der Führungs- und Überwachungsprozesse aus dem operativen Risikomanagement und dem Internen Kontrollsystem. Sie arbeitet unabhängig und objektiv und berichtet nicht nur der Geschäftsführung, sondern auch dem Aufsichtsrat und der Eigentümervertretung. Durch diese Art der Berichterstattung wird die Unabhängigkeit und Objektivität zusätzlich gefördert.

5.2.2.1 Einführung einer Internen Revision

Bei der Einführung einer IR ist es wichtig, deren Aufgabenstellung, Befugnisse und Verantwortung in einer Geschäftsordnung festzuhalten. Dabei gilt es, die in der Theorie genannten Grundsätze einzuhalten – Integrität, Objektivität, Vertraulichkeit, Fachkompetenz. Die Geschäftsordnung muss der Geschäftsführung bzw. dem Aufsichtsrat zur Genehmigung vom Leiter der IR vorgelegt werden. Sie beinhaltet die Stellung der IR innerhalb der Industrie-EWF, gestattet den Zugriff auf Personal, Vermögensgegenstände und Aufzeichnungen (soweit erforderlich) und bestimmt den Umfang der Tätigkeit [DIIR, 2018, S. 67].

Folgende Abschnitte sind üblicherweise Teil dieser Geschäftsordnung [DIIR, 2018, S. 68-69]:

1. Einführung – Erklärung der Rolle der Internen Revision.
2. Befugnisse – der Zugriff auf Aufzeichnungen, Personal und physische Objekte durch die IR wird definiert und die Verantwortung für den Schutz der Vertraulichkeit geklärt.
3. Organisation und Berichtslinien – die Berichtslinie der IR wird dokumentiert. Der Leiter der IR berichtet an die Geschäftsleitung, den Aufsichtsrat und die Eigentümervertretung. So kann gewährleistet werden, dass die IR ihrer Verantwortung gerecht wird.
4. Unabhängigkeit und Objektivität – die Wichtigkeit der Unabhängigkeit und Objektivität der IR wird beschrieben. Außerdem wird definiert, wie diese gewahrt wird.
5. Verantwortlichkeiten – darin beinhaltet ist beispielsweise der Prüfungsumfang, die Dokumentation des Prüfungsplans, die Genehmigung, die Durchführung der Prüfungen, die Dokumentation und Kommunikation der Ergebnisse und die Überwachung von korrigierenden Maßnahmen durch das Management.
6. Qualitätssicherung und -verbesserung – die Erwartungen an die Ergebnisse.

7. Unterschriften – die Vereinbarung zwischen dem Überwachungsorgan (Aufsichtsrat, Eigentümervertretung), der Geschäftsführung und dem Leiter der IR.

Die Geschäftsordnung bildet also die Basis für die gesamte Arbeit der Internen Revision. Eine der wichtigsten Fragen in der Geschäftsordnung ist, wie Unabhängigkeit, speziell organisatorisch, erreicht werden kann. Üblicherweise treffen der Leiter der IR, die GF, der Aufsichtsrat und die EV sowie die leitenden Führungskräfte eine Vereinbarung darüber, welche dann in der Geschäftsführung dokumentiert wird. Das sollte kein Problem darstellen, da die Einführung einer Internen Revision auch im Interesse der teilnehmenden Parteien ist. Weiters ist eine direkte Berichtslinie an das Überwachungsorgan und ein direkter Zugang wichtig [DIIR, 2018, S. 26-27].

Innerhalb der Industrie-EWF kann die Interne Revision in der Nähe der Legal Compliance situiert sein, da auch die Überprüfung der Einhaltung von Gesetzen und Normen ein Teil der IR ist und sie so abgegrenzt vom Risikomanagement agiert.

5.2.2.2 Ablauf einer Internen Revision

In der folgenden Abbildung wird der übliche Ablauf einer Internen Revision dargestellt:

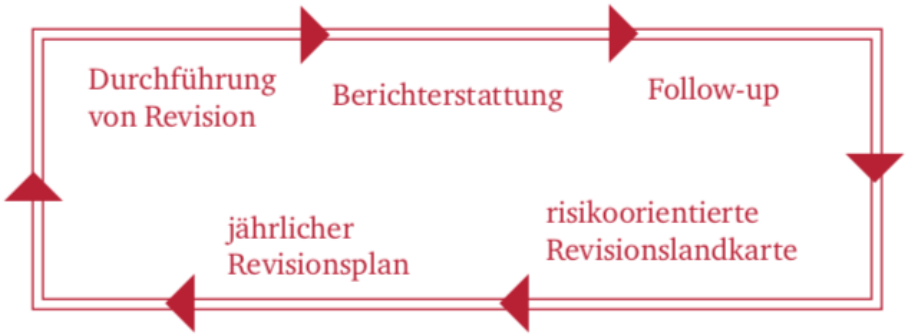


Abbildung 28: Ablauf einer Internen Revision, Quelle: [PwC, 2014, S. 12]

Der Prozess beginnt mit einer risikoorientierten Revisionslandkarte, welche für drei bis vier Jahre erstellt wird. Aus dieser Landkarte wird ein jährlicher Revisionsplan abgeleitet, der das Ziel, den Umfang und einen Zeit- und Ressourcenplan für die Revision beinhaltet.
Im nächsten Schritt wird die IR durchgeführt. Die Ergebnisse werden mit den geprüften Bereichen abgestimmt und Maßnahmen entwickelt und vereinbart.

Im Zuge der Berichterstattung wird ein Revisionsbericht verfasst, der das Prüfziel, die Prüfungshandlungen, Empfehlungen und vereinbarte Maßnahmen zum Inhalt hat. Außerdem werden die Ergebnisse vor der Geschäftsführung, dem Aufsichtsrat und gegebenenfalls der Eigentümervertretung (EV) präsentiert.
Im letzten Schritt werden die mit den geprüften Bereichen vereinbarten Maßnahmen im Zuge des Follow-Ups verfolgt und deren Umsetzung überwacht.

Bei der Durchführung der Internen Revision gilt es, die richtigen Fragen zu stellen. Im Folgenden werden exemplarisch einige Fragen angeführt, die präzisiert werden sollen bzw. für die einzelnen zu prüfenden Stellen angepasst werden sollen. Weiters werden Instrumente/Methoden angegeben, mit deren Hilfe diese Fragen beantwortet werden können [Rechnungshof, 2016, S. 20-22]:

1. Kennt die geprüfte Stelle die dort auftretenden Risiken? Wurden die für den Prozess relevanten Risiken analysiert?
   → schriftliche Ergebnisse einer Risikoanalyse der geprüften Stelle
   a. Wurden die möglichen Risiken inklusive einer Einschätzung des Schadensausmaßes und der Eintrittswahrscheinlichkeit dokumentiert und eine Risk Map erstellt?
   b. Wurden Schlüsselfunktionen/Hauptprozesse identifiziert, die im Falle eines Fehlers oder eines Ausfalls besonders gravierende Konsequenzen nach sich ziehen würden?
2. Gibt es bezüglich der Hauptprozesse klar definierte Abläufe und Verantwortungen?
   → Organigramme, Prozesshandbücher, Geschäftsordnungen
   a. Wurden die Abläufe der Prozesse analysiert, standardisiert und dokumentiert?
   b. Gibt es klar festgelegte Zuständigkeiten für wichtige Entscheidungen? Gibt es Stellvertreterregelungen, Wertgrenzen, etc. für Entscheidungen?
3. Sind die Definitionen aus Punkt 2 geeignet, um Risiken zu minimieren und das Erreichen der Unternehmensziele zu gewährleisten?
   → Soll-Ist-Vergleich Risikoanalyse – Sollvorgaben, Analyse von Worst-Case-Szenarien
   a. Sind unvereinbare Funktionen getrennt? (beispielsweise Zahlungsanordnung und Zahlungsvollzug)

   b. Werden automatisierte Prüfroutinen als Kontroll- und Steuerungsmaßnahmen nach Möglichkeit genutzt?
   c. Werden bei risikobehafteten Prozessschritten systematische Kontrollen durchgeführt?

4. Werden die Maßnahmen des IKS eingehalten?
   → Stichproben, eigene Kontrollberichte
   a. Gibt es eine Berichterstattung über den IKS-Status?
   b. Wird die Funktionsfähigkeit des IKS kontrolliert?
   c. Werden die Prozessabläufe, Entscheidungen und Kontrollen dokumentiert?
5. Findet regelmäßig eine Überprüfung des IKS auf Wirksamkeit/Funktionsfähigkeit statt?
   → Eigene Kontrollberichte, Anpassungen des IKS der geprüften Stelle
   a. Werden Fehler entdeckt?
   b. Wird das IKS bei gefundenen Fehlern angepasst?

Diese Fragen dienen als Orientierungshilfe für die IR. Sie sind ein guter Anhaltspunkt bei der erstmaligen Implementierung der Internen Revision. Im Laufe der Zeit bzw. auch bei der Implementierung selbst werden sich noch weitere Fragen ergeben, die relevant sind und mit deren Hilfe das Risikomanagement und die Hauptprozesse noch weiter verbessert werden können.

5.3 3-Lines-Of-Defense als organisationale ERM-Struktur in der Praxis

Um ein Rahmenwerk für ein unternehmensweites Risikomanagement-System zu erhalten, wird das Three-Lines-of-Defense-Modell herangezogen. In der folgenden Abbildung werden die drei Verteidigungslinien nochmals angeführt – allerdings angepasst an die Industrie-EWF:

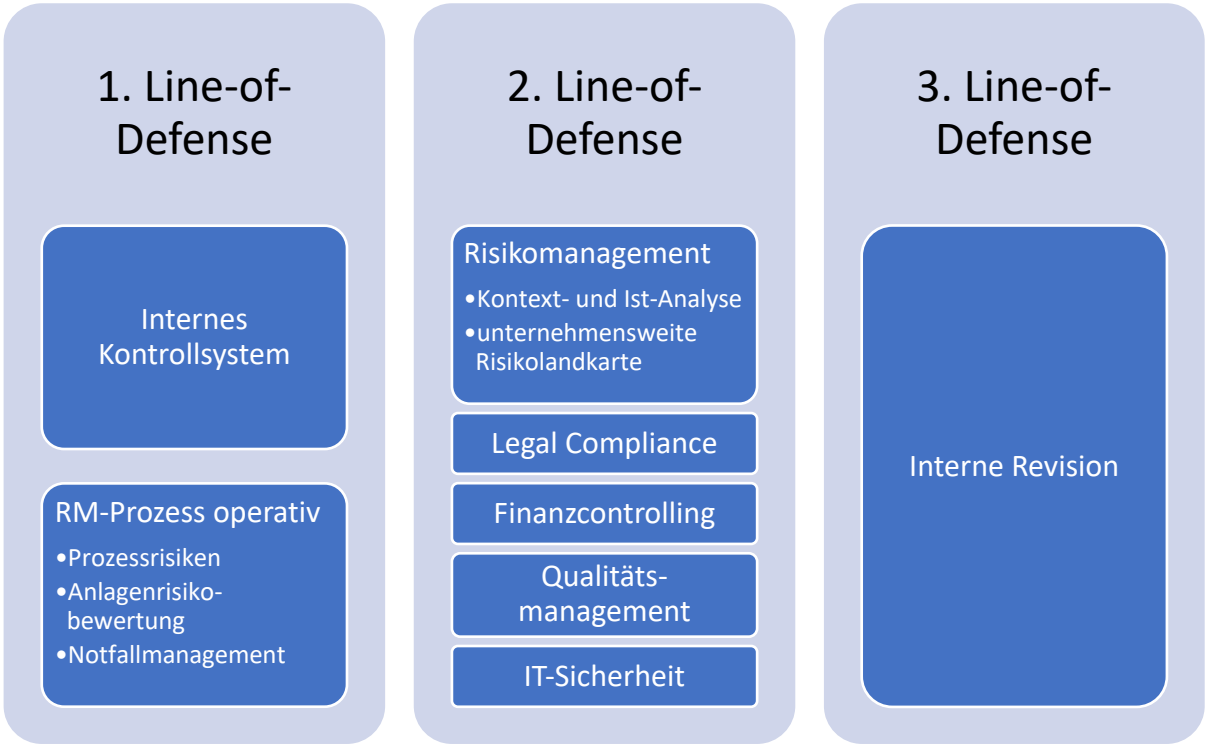


Abbildung 29: 3 Lines-of-Defense Industrie-EWF

5.3.1 Die 1. Line-Of-Defense

Die erste Line-of-Defense beinhaltet das IKS sowie den operativen Risikomanagement-Prozess. Der operative RM-Prozess setzt sich aus den verschiedenen Teil-Prozessen zusammen. Berichte aus der ersten Verteidigungslinie gehen an die Geschäftsführung oder an die zweite Verteidigungslinie, während die Risikoinformationen aus den RM-Prozessen großteils an das Risikomanagement in der 2. LOD weitergegeben werden, da sie dort zusammengeführt, für die Geschäftsführung aufbereitet und dann präsentiert bzw. besprochen werden.

Das Interne Kontrollsystem soll in der ersten Verteidigungslinie überall präsent sein und von den einzelnen Bereichen bzw. Prozessverantwortlichen auch jederzeit im Arbeitsalltag gelebt werden.

5.3.2 Die 2. Line-Of-Defense

Die zweite Line-of-Defense beinhaltet zuallererst das Risikomanagement. Ausgehend davon werden die einzelnen RM-Prozesse in der ersten Verteidigungslinie gesteuert und die Informationen in der *unternehmensweiten Risikolandkarte* zusammengeführt. Für diese Risikoaggregation werden die durch den RM-Prozessverantwortlichen zusammengefassten relevantesten Risiken und Chancen der einzelnen RM-Prozesse an den Risikomanager weitergegeben. Um die Wichtigkeit der einzelnen RM-Funktionen in die unternehmensweite Risikolandkarte zu integrieren, kann eine unterschiedliche Gewichtung der Methoden stattfinden.

Diese Risikolandkarte dient als Überblick über die wichtigsten Prozesse im Unternehmen, außerdem als Ausgangspunkt für die gesamte Risikosteuerung. Die daraus gewonnenen Informationen berichtet der Risikomanager direkt an die Geschäftsführung.

Als weiterer Überblick dient die *Stakeholder-Analyse*. Sie beinhaltet die vom Risikomanager angelegte Checkliste, die sämtliche Bereiche des Unternehmens mit ihren Hauptprozessen umfasst. Mit den einzelnen Bereichsleitern wird diese Checkliste Punkt für Punkt durchgegangen. Ist in einem Bereich alles in Ordnung, kann dieser Punkt einfach abgehakt werden. Kommen jedoch Probleme ans Licht, wird mit dem einzelnen Bereichsleiter detailliert darauf eingegangen.

Mit der unternehmensweiten Risikolandkarte und der Stakeholder-Analyse hat der Risikomanager also zwei Tools zur Verfügung, die einmal Bottom-Up (Risikolandkarte) und einmal Top-Down (Stakeholder-Analyse) funktionieren. Dadurch entsteht eine Wechselwirkung, in der zwei Sicht- bzw. Herangehensweisen aufeinandertreffen und sich gegenseitig überprüfen.

Weitere Elemente in der zweiten Verteidigungslinie sind:

- *Legal Compliance* – Rechtliche Fragen bzgl. Verträgen etc. werden von der Legal Compliance Abteilung geklärt und bearbeitet. Diese Abteilung ist deswegen Teil der zweiten Verteidigungslinie, da sie abgesehen von der Erstellung bzw. Überprüfung von Verträgen auch eine Überwachungsfunktion über die 1. LOD innehat und die Vereinbarkeit von Risiken mit Gesetzen und Regulatorien überprüft.
- *Finanzcontrolling* – Hier verhält es sich ähnlich wie bei der Legal Compliance. Finanzielle Risiken werden überwacht und Probleme aufgedeckt. Berichtet wird an die Geschäftsführung.
- *Qualitätsmanagement* – Das Qualitätsmanagement ist ein eigenständiger Teil der 2. LOD, weil der langjährige Erfolg der Industrie-EWF darauf aufbaut, dass die Qualität der erzeugten Produkte die der Konkurrenz übersteigt. Diese Abhängigkeit von der Qualität macht das Qualitätsmanagement zu einem sehr wichtigen Bestandteil des Unternehmens.
- *IT-Security* – Im Zeitalter der Digitalisierung spielt die Sicherheit im IT-Bereich eine immer größere Rolle. Dies umfasst nicht nur die Absicherung gegen ein Eindringen von außen, sondern auch die Integrität und Sicherung sämtlicher Daten, die unter anderem auch für das Risikomanagement essentiell sind.

Prozesse wie die Steuerung von Risiken, Finanzcontrolling oder IT-Security bedürfen ebenfalls einer internen Kontrolle, da in diesen Bereichen große Gefahren lauern. Das Interne Kontrollsystem beschränkt sich also nicht nur auf die erste Verteidigungslinie, sondern soll ebenso in der 2. LOD umgesetzt werden.

5.3.3 Die 3. Line-Of-Defense

In der dritten Verteidigungslinie befindet sich die *Interne Revision*. Sie ist für die Überprüfung und Beratung des Risikomanagements und der Führungs- und Überwachungsprozesse, die sich in den anderen beiden Verteidigungslinien befinden, zuständig und arbeitet unabhängig und objektiv. Weiters überprüft die IR die Organisation des Risikos und des Risikomanagements der Industrie-EWF. Berichtet wird nicht nur an die Geschäftsführung, sondern auch an den Aufsichtsrat (und die Eigentümervertretung). Diese Art der Berichterstattung fördert die Unabhängigkeit der IR zusätzlich.

5.4 Auswirkung auf den ERMMA-Reifegrad

Nach Umsetzung dieser Maßnahmen können Risiken unternehmensweit identifiziert, bewertet, dokumentiert und schließlich bewältigt werden. Außerdem können Chancen erkannt werden und in Zukunft auch besser genutzt werden.

Mit Hilfe einer unternehmensweiten Risikolandkarte werden die Risiken im Risikomanagement aggregiert und bilden die Basis für ein RM-System für das gesamte Unternehmen. Das Interne Kontrollsystem kann die Fehlerrate in diesen Prozessen stark reduzieren. Als Überwachungs- und Beratungsorgan, das unabhängig agiert und direkt an den Aufsichtsrat (bzw. die Eigentümervertretung) berichtet, unterstützt die Interne Revision das RM-System.

Der ERMMA-Reifegrad der RM-Prozesses kann mit Hilfe dieser Maßnahmen von 2 auf 4 deutlich verbessert werden.

Die größte Herausforderung in der Risikoorganisation liegt in Unterstützung des RM-Prozesses bei der Aggregation der Risiken in einer unternehmensweiten Risikolandkarte. Die einzelnen RM-Funktionen müssen explizit als solche definiert werden, um nicht nur einen Überblick über die Prozesse und Methoden, sondern auch über die die einzelnen Funktionen zu erhalten. Weiters ist eine Prüfung der Organisationsstruktur durch die Interne Revision vonnöten, damit die Wirksamkeit der Organisation des Risikos bzw. des Risikomanagements auch in Zukunft weiter verbessert werden kann.

Mit Hilfe dieser Maßnahmen kann der ERMMA-Reifegrad der Risikoorganisation von 1 auf 3 erhöht werden, wobei auch schon Vorgaben für Reifegrad 4 erfüllt werden, nämlich die unternehmensweite Risikoaggregation.

6 Risikoverständnis und RM-Schulungen: Theorie und praktische Umsetzung

6.1 Risikoverständnis und RM-Schulungen: Diagnose des IST-Zustands

6.1.1 Risikoverständnis: Diagnose des IST-Zustands

Das Risikoverständnis beinhaltet das allgemeine Verständnis, was Risiko und Risikomanagement an sich ist. Durch ein gutes Risikoverständnis entsteht ein Bewusstsein für Risiko und den Umgang damit.

Der Risikomanager hat sich dieses Verständnis großteils schon selbst angeeignet. Auch die Geschäftsführung (vor allem der CFO) ist sehr erfahren mit Risikomanagement. Das ist sehr wichtig, da ohne ein grundlegendes Wissen über Risiko und dessen Management auch wenig Verständnis für Berichte bezüglich der Risiken bzw. des Risikomanagement-Prozesses aufgebracht werden kann.

Die Prozessverantwortlichen (vor allem im operativen Bereich) sowie Mitarbeiter in der mittleren Führungsebene müssen dahingehend jedoch noch geschult werden, da sie zwar im Zuge von KVP (kontinuierlicher Verbesserungsprozess) schon versuchen, wenige Risiken einzugehen, für das Risikomanagement aber noch kein bzw. wenig Bewusstsein vorhanden ist. Das Risikoverständnis steht demnach in direktem Zusammenhang mit einer Risikoschulung.

Weiters müssen vor der Implementierung einer Internen Revision die künftigen Revisoren ein sehr gutes Risikoverständnis aufweisen können. Dies ist essentiell für die Durchführung ihrer Überwachungs- und Beratungstätigkeiten.

In der Industrie-EWF werden generell neue Wege oder Innovationen gründlich dokumentiert. So verhält es sich auch mit Wissenszuwachs im Risikomanagement. Jedes Wissen, das bisher gewonnen wurde, wurde auch dokumentiert.

6.1.2 RM-Schulungssystem: Diagnose des IST-Zustands

Eine durchdachte und konsequente Risikoschulung bildet die Basis für ein gutes Risikoverständnis im ganzen Unternehmen. Wie bereits erwähnt wurde, müssen vor allem die Risiko-Owner (im Falle der Industrie-EWF also die Prozess-Verantwortlichen) dahingehend geschult werden.

Wie man aus dem Reifegrad von 0 schließen kann, gibt es in der Industrie-EWF noch kein Risikomanagement-Schulungssystem.

Generell ist das Schulungssystem innerhalb der Industrie-EWF jedoch sehr umfassend und bietet viele Möglichkeiten. Als Industrieunternehmen ist man sich der Tatsache bewusst, dass gute Facharbeiter schwierig zu finden sind. Aus diesem Grund haben Mitarbeiter in der Industrie-EWF die Möglichkeit, sich in viele Richtungen weiterzubilden. Dafür gibt es einen firmeneigenen Schulungskatalog, der viele Schulungsmaßnahmen sowohl mit internen Trainern als auch in externen Bildungseinrichtungen umfasst. Darin werden nicht nur fachliche, sondern auch persönlichkeitsbildende und gesundheitsfördernde Weiterbildungen angeboten. Im Rahmen der jährlichen Mitarbeitergespräche können Programme, die zu den individuellen Aufgabenbeschreibungen passen, ausgewählt werden.

Gerade in der Lehrlingsausbildung ist man sehr weit fortgeschritten und innovativ. Auszubildende verbringen den Anfang ihrer Lehrzeit nicht damit, zusammenzukehren, zu putzen oder die einfachen Arbeitsschritte für die Facharbeiter zu erledigen, sondern lernen von Beginn an jene Tätigkeiten, die sie nach der Ausbildung durchführen werden.
Um dies umzusetzen, gibt es ein eigenes Lehrlingsausbildungszentrum, in dem sämtliche Lehrlinge arbeiten. Sie werden dort von Fachkräften in den verschiedenen Kompetenzen ihres Lehrberufs ausgebildet. Dabei arbeiten sie genauso an Maschinen und stellen Produkte her wie die Arbeiter in der Produktion.

6.2 Risikoverständnis und RM-Schulungen in der Theorie

Um das Risikoverständnis zu erhöhen bzw. das Bewusstsein für Risikomanagement überhaupt erst zu schaffen, muss ein grundlegendes Basiswissen durch Selbststudium oder Schulungen erlangt werden. Diese theoretischen Aspekte werden im Folgenden angeführt.

6.2.1 Risikoverständnis in der Theorie

Wie ist Risiko definiert? Dafür gibt es verschiedene Charakterisierungen, die stark vom Anwendungsgebiet abhängen. Es kann als mögliche zweiseitige Abweichung, also positiv oder negativ, betrachtet werden, manchmal ist es jedoch sinnvoll, sich auf die negativen Aspekte zu beschränken [Muschick, Müller, 1987, S. 108-132].

Eine Beschränkung auf negative Aspekte ist hauptsächlich im operativen Bereich gegeben. Beispielsweise kann eine Maschine ausfallen – also ein negativer Aspekt, da sie dann nicht ihr Potential entfalten kann. Die Chance, dass sie plötzlich mehr produziert als ihre technischen Möglichkeiten zulassen, besteht jedoch nicht. Hier kann also keine positive Abweichung, keine Chance, entstehen.

In der ISO 31000:2009, einer internationalen Norm, wird Risiko wie folgt definiert:
„*Risiko = Auswirkung von Unsicherheit auf Ziele*“ [ISO 31000, 2009, S. 6].

Darin lässt sich auch ein sehr wichtiger Aspekt des Risikomanagements erkennen – die Zielorientierung. Ein gutes Risikoverständnis beinhaltet immer eine Orientierung an den Unternehmenszielen.
Dazu werden noch einige Anmerkungen gemacht, um diese kurze Erklärung etwas detaillierter zu beschreiben [ISO 31000, 2009, S. 6]:

1. Eine Auswirkung stellt eine Abweichung von Erwartungen dar. Und zwar in positiver und/oder negativer Hinsicht.
2. Ziele können verschiedene Aspekte beinhalten (z.B. Finanzen, Sicherheit, Umwelt, Gesundheit, etc.) und sich auf verschiedene Unternehmensebenen beziehen (z.B. strategisch, projekt-, produkt- oder prozessbezogen).
3. Ein Risiko wird oft in Bezug auf eventuell eintretende Ereignisse und Auswirkungen (oder eine Kombination daraus) charakterisiert.

4. Ein Risiko wird oft mit Hilfe der Auswirkungen eines Ereignisses in Verbindung mit der Wahrscheinlichkeit seines Eintretens charakterisiert.
5. Unsicherheit ergibt sich aus dem Fehlen von Informationen (gänzlich oder teilweise), Verständnis oder Wissen über ein Ereignis, dessen Auswirkung oder Wahrscheinlichkeit.

Als Beispiele für unterschiedliche Definitionen werden hier die Mathematik und die Rechtswissenschaft angeführt.
In der Mathematik wird Risiko (R) als das Produkt des Ausmaßes eines negativen Ereignisses (A) mit der Eintrittswahrscheinlichkeit (E) beschrieben [Muschik, Müller, 1987, S. 108-132]:

$$R = A * E$$

Im Rechtswesen[18] hingegen wird der Begriff Risiko durch die Trias Gefahr, Risiko und Restrisiko bestimmt. Er kann nur durch eine Abgrenzung zu den Begriffen Gefahr und Restrisiko betrachtet werden. Eine Gefahr ist gegeben, wenn es bei ungehindertem Ablauf eines objektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit zu einem Schaden kommen kann. Ausschlaggebend hierbei ist die hinreichende Schadenswahrscheinlichkeit, die eine Bedingung für Gefahr ist. Beim Risiko hingegen reicht die reine Möglichkeit eines Schadens aus, es geht also um die Nichtausschließbarkeit eines Schadens. Gefahr ist somit ein qualifiziertes Risiko. Ein Restrisiko ist dadurch definiert, dass die Möglichkeit eines künftigen Schadens praktisch ausgeschlossen werden kann [Jung, 2003, S. 545-546].

Die Definition für Risiko kann also ziemlich unterschiedlich ausfallen, je nachdem in welchem Anwendungsgebiet man sich befindet. Für diese Arbeit, bzw. das Risikomanagement in einem Unternehmen, sind die Definition der ISO 31000:2009 und die mathematische Formulierung wichtig. Die Norm bezieht sich auf das Anwendungsgebiet Wirtschaft (bzw. auf Unternehmen), während die mathematische Formulierung praxisnahe ist und verwendet wird, um Risiken zu quantifizieren. Um Risiken bewerten und vergleichen zu können, benötigt ein Risikomanager eine Zahl oder eine Bandbreite.

Weiters werden Risiken in Typen eingeteilt – reine Risiken und spekulative Risiken.

[18] Beispiel aus deutschem Recht

Diese verschiedenen Risikotypen werden in der folgenden Abbildung dargestellt:

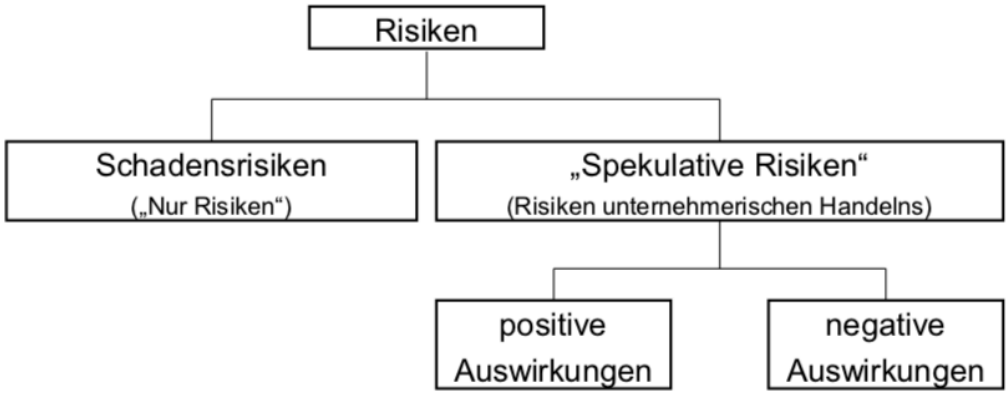


Abbildung 30: Spekulative vs. reine Risiken, Quelle: [Koubek, 2015, S. 5]

Man erkennt, dass reine Risiken (hier Schadensrisiken genannt), nur negative Konsequenzen haben können. Reine Risiken treten am Häufigsten in operativen Bereichen auf (z.B. Maschinenausfälle).
Spekulative Risiken hingegen können entweder positive oder negative Auswirkungen haben. Das bedeutet in beiden Fällen eine Zielverfehlung, bei einer positiven Zielverfehlung spricht man allerdings von einer Chance, nicht von einem Risiko. Diese Risikotypen finden sich hauptsächlich im strategischen und finanziellen Management (z.B. eine positive Entwicklung bei volatilen Rohstoffpreisen = Chance).

In einer weiteren Einteilung differenziert man zwischen beeinflussbaren und nicht beeinflussbaren Risiken. Dies ist ein wichtiger Punkt und erhöht das Verständnis deswegen, weil man diese Risikotypen den jeweiligen Risiken zuteilen kann und auf einen Blick weiß, ob man ein bestimmtes Risiko vermeiden und bewältigen kann (beeinflussbar) oder ob man sich nur möglichst gut darauf vorbereiten kann (nicht beeinflussbar) [Saßen, 2019, S. 42].

In der Industrie-EWF wird eine Einteilung nach Beeinflussbarkeit bereits durchgeführt, und zwar in der Stakeholder-Analyse. Darin werden verschiedene Informationen zu sämtlichen Interessensgruppen (Stakeholder) betrachtet. Dabei wird vor allem ausgearbeitet, welchen Risiken und Chancen mit diesen Interessensgruppen in Verbindung gebracht werden. Weiters wird definiert, wo der Einfluss für diese Ereignisse hauptsächlich liegt. Beispielsweise hat die Industrie-EWF großen Einfluss darauf, welche Versicherung gewählt wird (der Rahmen bzw.

das Risiko wird selbst festgelegt), jedoch hat das Unternehmen gar keinen Einfluss auf Regeln, die von Behörden vorgegeben werden.

Weiters ist die Theorie über den Risikomanagement-Prozess mit den einzelnen Schritten (Identifikation, Analyse, Bewertung, Bewältigung), die Überprüfung durch das Interne Kontrollsystem sowie die Aggregation von Risiken in der unternehmensweiten Risikolandkarte sehr wichtig für ein gutes Risikomanagement-Verständnis. Diese Punkte werden jedoch hier nicht nochmals angeführt, da sie in der Theorie zum RM-Prozess bereits ausführlich beschrieben wurden.

6.2.2 Risikomanagement-Schulungen in der Theorie

Da die Bedürfnisse bezüglich eines RM-Schulungssystems von Unternehmen zu Unternehmen stark variieren, ist es sehr schwierig, einen theoretischen Bauplan dafür zu erstellen. Es gibt jedoch einige Institutionen in Österreich, die Weiterbildungen im Risikomanagement anbieten.

Orientiert man sich am Inhalt der Kurse bei den großen Anbietern[19], kann man den Inhalt für eine Schulung ungefähr wie folgt gliedern:

- Grundlegendes Risikomanagement
    - Definitionen, Begriffe, Prinzipien
    - Phasen des RM-Prozesses – identifizieren, analysieren, bewerten, bewältigen und überwachen
    - Normen, rechtliche Aspekte
    - Risikopolitik und -strategie
- Risikomanagement-Tools
    - Monte-Carlo-Analyse, Simulationen
    - Integration in IT-Systeme
    - RM-Organisation
- Kommunikation und Berichtswesen
    - IKS, IR
    - Krisenmanagement
    - Berichtswesen

[19] [WIFI, 2019], [Qualityaustria, 2019]

Diese Gliederung als Anhaltspunkt dienen, wie eine solche Schulung aufgebaut werden kann, für die Durchführung muss man jedenfalls erwägen, welche Themengebiete interessant und relevant für die Bedürfnisse des jeweiligen Unternehmens sind.

6.3 Risikoverständnis und RM-Schulungen: Praktische Umsetzung in Industrie-EWF

Wie bereits erwähnt wurde, verfügt der Risikomanager bereits über ein fundiertes Wissen. Zusätzliche Kompetenz kann er sich selbst unter anderem durch das Studium der theoretischen Aspekte dieser Arbeit aneignen. Eine externe Schulung wäre für den Risikomanager nur wichtig, wenn ein Zertifikat[20] erlangt werden soll.

Folgende Aspekte sollten in jedem Fall Teil der Weiterbildung des Risikomanagers sein (nicht inkludiert ist bereits erlangtes Wissen):

- RM-Framework → 3 Lines-of-Defense als organisationaler Rahmen für das unternehmensweite RM-System
- Internes Kontrollsystem
- Interne Revision → Arbeitsweise, Aufgaben, Ziele, Implementierung
- Zusammenführung der Risikobewertungen der einzelnen RM-Prozesse in einer unternehmensweiten Risikolandkarte

Dank der bereits sehr umfassenden Kompetenz des Risikomanagers ist die Integration der RM-Schulungen in das bereits bestehende und sehr umfangreiche Schulungssystem der Industrie-EWF ein sehr guter Ansatz. Dabei gibt der Risikomanager sein Wissen an die Mitarbeiter weiter. Im Zuge dessen soll ein eigenes Modul „Risikomanagement“ geschaffen werden, das nicht nur Facharbeiter und Manager belegen können, sondern das auch Lehrlinge während ihrer Ausbildungszeit auswählen und sich so schon während der Lehrzeit ein Verständnis für Risiko und Risikomanagement aneignen können.

Für dieses Modul wurde im Zuge dieser Arbeit ein Informationsblatt (siehe Ende des Kapitels) entworfen, das einen ersten Überblick über Risiko und dessen Management bieten soll. Es kann zu Beginn der Risikoschulungen integriert werden.

[20] Dies kann durch das Absolvieren eines Kurses bei einem der genannten externen Anbieter erreicht werden. Nach einer Prüfung erhielte er ein Diplom als zertifizierter Risikomanager.

Das größte Verbesserungspotential liegt bei den Prozessverantwortlichen und der mittleren Managementebene der Industrie-EWF, da sie die vorhandenen Risiken identifizieren, bewerten und teilweise steuern sollen.

In der RM-Schulung sollen jedoch nicht alle Themengebiete, die in der Theorie angegeben wurden, gelehrt werden, da schlichtweg bei weitem nicht alle benötigt werden, um ein gutes Risikomanagement auf Prozessebene zu betreiben. Die grundlegenden Aspekte, die jeder Risk Owner kennen sollte, sind:

- Grundlegendes Risikomanagement
    - Definitionen rund um das Risikomanagement
        - Risiko/Chance
        - Risikotypen (rein, spekulativ, beeinflussbar, nicht beeinflussbar)
        - Schadensausmaß, Eintrittswahrscheinlichkeit
    - Vorteile durch Risikomanagement
    - Grundlagen zum RM-Prozess
        - Identifikation, Analyse, Bewertung, Bewältigung von Risiken
- Reporting (wer berichtet was an wen)
- Normen und rechtliche Aspekte
- Internes Kontrollsystem (Grundzüge, bzw. relevante Informationen für Risk Owner)
- Interne Revision (wozu dient die IR, was darf sie)

Diese Inhalte können jeden Mitarbeiter darauf vorbereiten, aktiv im Risikomanagement-Prozess mitzuarbeiten und die für ihn relevanten Aufgaben durchführen zu können.

Das Wissen der Mitarbeiter der mittleren Managementebene muss weitergehen – die verschiedenen Methoden und Schritte des RM-Prozesses sollten genau bekannt sein (inklusive der Risikoaggregation mit Hilfe der unternehmensweiten Risikolandkarte sowie die organisationale Struktur des Risikomanagements im Sinne des 3-LOD-Modells). Weiters soll das Interne Kontrollsystem genauer behandelt werden, sowie die Gründe für die Installation einer Internen Revision und deren Aufgabengebiete.

Risiko – eine kurze Information

Was ist Risiko?

Risiko ist eine Abweichung vom definierten Ziel (mit einer bestimmten Wahrscheinlichkeit):

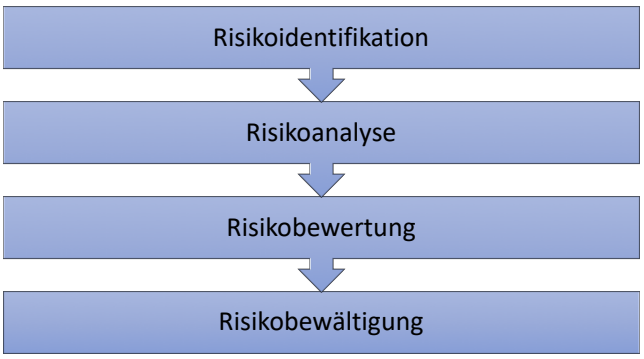
- Positive Abweichung = Chance
- Negative Abweichung = Risiko

Warum betrachtet man Risiko?

Chancen/Risiken im Vorhinein zu kennen, bedeutet:

- Genauere Planung
- Weniger Überraschungen
- Bessere Vorbereitung auf Abweichungen vom Plan
- Kontinuierliche Verbesserung
- Weniger Fehler

Was bedeutet Risikomanagement?



Risikoidentifikation: Welche unvorhergesehenen Ereignisse können eintreten? Was kann in meinem Prozess der Grund für eine Abweichung vom Plan sein? Welche Risiken und/oder welche Chancen beinhaltet mein Prozess?

Risikoanalyse: Was ist die Ursache für ein Risiko? Woraus entsteht eine Chance? Wie hoch ist die Wahrscheinlichkeit für das Eintreten eines Risikos / einer Chance? Was sind die Auswirkungen? (Basis dafür sind Daten aus Vergangenheit, persönliche Einschätzungen, etc.)

Risikobewertung: Was bedeutet das Eintreten von zuvor identifizierten Ereignissen? (Kosten/Einsparung, Zeitverlust/-gewinn, etc.)

Risikobewältigung: Wie können Risiken vermieden und Chancen genutzt werden? Wenn die Vermeidung eines Risikos nicht möglich ist: Wie kann das Risiko minimiert werden? Wie kann man sich am besten auf die Auswirkungen vorbereiten?

Abbildung 31: Informationsblatt Risiko

6.4 Auswirkung auf den ERMMA-Reifegrad

Wird das genannte Wissen über Risiko und Risikomanagement (mit Hilfe des Schulungssystems) an die am RM-Prozess beteiligten Mitarbeiter weitergegeben, wird sich deren Risikoverständnis stark verbessern und dazu führen, dass Aufgaben wie die Identifizierung, Analyse, Bewertung und Bewältigung von Risiken und Nutzung von Chancen viel effizienter und vor allem bewusster durchgeführt werden können.

Diese Umstellung wird kurzfristig keine sehr großen Auswirkungen haben, da auch die Schulungsmaßnahmen erst umgesetzt und genutzt werden müssen, mittel- bis langfristig jedoch wird sich das Bewusstsein über Risiko in der Industrie-EWF verankern und merkbar dazu beitragen, negative Auswirkungen zu vermindern oder gänzlich zu vermeiden.
Nicht jeder Mitarbeiter muss dabei das vollständige Wissen erhalten, sondern prioritär das für ihn relevante Verständnis erlangen.

So kann sich der aktuelle ERMMA-Reifegrad des Risikoverständnisses von 1 auf 4 erhöhen.

Die Implementierung der Schulungen wird für die Industrie-EWF keine großen Schwierigkeiten mit sich bringen, da das Schulungssystem innerhalb des Unternehmens (sowohl intern als auch extern) bereits sehr gut funktioniert und den Mitarbeitern sehr viele interessante Möglichkeiten bietet, sich weiterzubilden. Diese Erfahrung, die über die Jahre gesammelt wurde, macht es möglich, sowohl Lehrlingen als auch langjährigen Mitarbeitern die Vorteile und Methoden eines Risikomanagement-Systems nahezubringen.

Die Integration des Risikomanagements in das Schulungssystem erhöht den ERMMA-Reifegrad des RM-Schulungssystems von bisher 0 auf 3.

7 Risikostrategie: Theorie und praktische Umsetzung

7.1 Risikostrategie: Diagnose des IST-Zustands

Bisher existiert eine Risikostrategie bzw. Risikopolitik (Risikoappetit, Risikotoleranz[21]) in der Industrie-EWF nur in recht grundlegenden Zügen. Das bedeutet, der Risikoappetit ist definiert, jedoch nur wenig dokumentiert. Eine deklarierte Risikostrategie gibt es nicht.

Im Zuge eines Interviews mit dem Chief Financial Officer der Industrie-EWF stellte sich heraus, dass sich die Eigentümer sehr risikoavers verhalten. Aus diesem Grund ist die Risikopolitik generell als risikoavers einzustufen, da letzten Endes die Eigentümervertretung die großen und wichtigen Entscheidungen trifft.
Das äußert sich bei Investitionen und Strategien. Einerseits werden zwar große Investitionen getätigt (wie z.B. der Zukauf von neuen Werken in anderen Ländern oder der Zukauf von Land rund um bestehende Werke, um in der Zukunft Platz für neue Hallen und andere nutzbare Gebäude zu haben), jedoch nur, wenn diese mit einem geringen und vor allem nachvollziehbaren Risiko behaftet sind. Diese Investitionen haben sich in der Vergangenheit auch sehr schnell amortisiert und als gute Entscheidungen erwiesen, weswegen für die Eigentümer auch kein Grund besteht, ihre Risikoaversion abzulegen.

Auch die „Kriegskasse“, also das überschüssige Kapital des Unternehmens, das nicht reinvestiert, sondern gespart wird, wird möglichst risikolos veranlagt. Dafür hat man sich als Partner eine Investmentfirma ausgesucht, die genau auf die eigenen Wünsche eingeht. Dabei wird in einen breit gestreuten Fonds investiert, für die Volatilität und die Rentabilität gibt es klare Vorgaben. Um die Veranlagung zu überprüfen, werden quartalsweise „Reviews“ abgehalten.

Diese Einstellung zu Risiko hat jedoch auch andere Gründe. In einem Unternehmen dieser Größe, das darauf abzielt, dass Mitarbeiter lange bleiben und sogar über Generationen hinweg dort arbeiten, will man auch für jene Personen kein übermäßiges Risiko eingehen. Die meisten Mitarbeiter verlassen sich auf ihren Arbeitsplatz und wollen durch die Verbundenheit und den annähernd familiären Umgang in kein anderes Unternehmen wechseln. Dieses

[21] Die Annahme eines Risikos im Rahmen der gesetzlichen bzw. regulatorischen Vorgaben [ONR 49000, 2014, S. 14]

Vertrauen ist unter anderem darin begründet, dass die Eigentümervertretung in der Vergangenheit ebenfalls risikoavers agiert hat und auch während diverser Krisen keine Arbeitsplätze abbauen musste.

Ein weiterer Grund ist, dass Mitglieder der Eigentümerfamilie in der Geschäftsführung tätig sind. Naturgemäß gehen Manager, die auch Eigentümer sind, weniger Risiko ein, da es sich bei einem potentiellen Verlust auch um ihr eigenes Geld handelt.

7.2 Risikostrategie in der Theorie

Die grundlegenden Werte, Normen und Verhaltensweisen von Unternehmensmitgliedern bilden die Basis für alle Unternehmensaktivitäten. Daraus entsteht eine Unternehmenskultur, die als gewachsenes, gelebtes und gestaltbares Denk-, Entscheidungs- und Verhaltensmuster verstanden wird. Das Unternehmensgeschehen und die Führungsentscheidungen (wie beispielsweise die Einführung und Umsetzung des Risikomanagements) werden daher von der Unternehmenskultur maßgeblich beeinflusst. Diese Werte und Verhaltensweisen werden ebenfalls in der Risikokultur manifestiert. Darunter versteht man das die risikobezogenen Handlungen und das risikobezogene Verhalten beeinflussende Werte- und Normengerüst der Unternehmensmitglieder. Aus diesen Definitionen entstehen risikopolitische Grundsätze, die ihrerseits die Basis für eine unternehmensweit konsistente Risikostrategie bilden [Hoitsch, Winter, Bächle, 2005, S. 126-127].

Eine Risikostrategie wird in jeder Organisation benötigt, um reproduzierbare Verhaltensnormen im täglichen Risikomanagement zu schaffen [Hoffmann, 2017, S. 20-23].

Im Zuge der Risikostrategie sollen risikopolitische Leitlinien definiert werden, die Aussagen über die Natur des Risikos, seine Bedeutung für das Unternehmen, die Einstellung der Unternehmensleitung zur Risikoübernahme (Risikoappetit, Risikotoleranz) sowie die Funktion und Notwendigkeit des Risikomanagement beinhalten. Weiters sind fundamentale risikobezogene Ziele zu formulieren [Hoitsch et al., 2005, S. 128-129].

Die Wirtschaftsprüfungsgesellschaft KPMG, die ebenfalls sehr aktiv als Unternehmens- bzw. Managementberatungsagentur tätig ist, empfiehlt, sich an den folgenden Punkten (Best Practice) zu orientieren [Stangl, 2017, S. 21]:

- Risikopolitische Grundsätze: Um den Umgang mit Geschäftstätigkeiten und deren Risiken zu regeln, werden Grundsätze definiert. (z.B.: Nur Geschäfte, deren Risiken bekannt sind, werden durchgeführt)
- Enge Verzahnung der strategischen Geschäftsplanung mit dem Risikomanagement: Die strategische Geschäftsplanung wird mehrjährig ausgelegt. Sie identifiziert, wohin sich das Unternehmen in den nächsten Jahren entwickeln soll (und wohin nicht).

- Verständnis über eigenes Risikoprofil (Art des Risikos, nicht die Steuerung der Einzelrisiken): Voraussetzung dafür ist ein unternehmensweiter Risikomanagement-Ansatz.
- Information über Risikoherkunft: Damit ist die Herkunft im eigenen Unternehmen gemeint (Geschäftsbereiche, Tochterunternehmen, etc.). Nur so können Risiken detaillierter, also auf operativer Ebene, identifiziert, bewertet und bewältigt werden.
- Risikotragfähigkeit: Der stärkste Treiber für die Risikotragfähigkeit ist die Innenfinanzierungskraft – kann sich das Unternehmen in Fall einer Krise die definierte Risikoposition leisten?
- Risikotoleranz: Definition, welches Ausmaß eines Risikos gewählt wird. Diese Definition muss sich innerhalb der gesetzlichen bzw. regulatorischen Vorgaben befinden [ONR 49000, 2014, S. 14].

Man erkennt, dass diese Vorgehensweise Ähnlichkeiten zu der zuvor beschriebenen Theorie aufweist, jedoch noch einen Schritt weiter geht, indem sie konkrete Aspekte angibt, auf die es zu achten gilt.

Dabei muss stets auf eine Abstimmung zwischen der Risiko- und der Geschäftsstrategie geachtet werden. Deswegen liegt die Verantwortung für die Risikostrategie auch bei der Geschäftsführung und nicht beim Risikomanagement. Eine mehrjährige Planung und eine starke Verzahnung mit dem restlichen Planungsprozess sind ebenso wichtig wie eine umfassende Sicht auf das Unternehmen.

Ein weiterer wichtiger Punkt ist das Monitoring der Risikostrategie. Dabei handelt es sich um die laufende Überprüfung, Aufsicht, kritische Beobachtung oder Bestimmung des Ist-Stands, um Abweichungen vom erwarteten Leistungsniveau zu erkennen [ISO 31000, 2009, S. 13]. Natürlich muss die Risikostrategie nicht laufend überprüft werden. Jedoch so regelmäßig, dass kurzfristige strategische Probleme auch rechtzeitig erkannt werden. Dieses Monitoring ist eine klassische Aufgabe der Internen Revision. Sie überprüft die Risikostrategie auf Zweckmäßigkeit und Funktionsfähigkeit.

7.3 Risikostrategie: Praktische Umsetzung in Industrie-EWF

Die Risikostrategie bezieht sich auf die zweite COSO-Komponente, „Strategy and Objective-Setting“. Im Falle der Industrie-EWF bieten sich die jährlichen Strategiemeetings zur Implementierung einer Risikostrategie an. Dafür muss einige Vorarbeit geleistet werden, sowohl von dem Risikomanager als auch von der Geschäftsführung.

Einige der in der Theorie genannten Punkte werden zwar von der Industrie-EWF bereits umgesetzt, bei anderen besteht jedoch noch großes Verbesserungspotential.

Nach risikopolitischen Grundsätzen wird bereits vorgegangen. Beispielsweise werden nur Geschäfte getätigt, deren Risiken bekannt und relativ gering sind. Die Geschäftsführung weiß auch um den Risikoappetit der Eigentümer, allerdings ist dieser nicht dokumentiert.

Eine klare Empfehlung ist also, diese Grundsätze genauer zu definieren und zu dokumentieren. Weiters kann der Risikoappetit kommuniziert werden, auch in niedrigere Ebenen der Hierarchie. So verstehen Risk Owner selbst besser, dass dies Teil der Risikopolitik des Unternehmens ist und können Führungsentscheidungen, die auf Basis des Risikoappetits gemacht wurden, besser nachvollziehen.

Der wichtigste Punkt, der mit der Implementierung eines unternehmensweiten Risikomanagement-Systems angestrebt werden sollte, ist die enge Verzahnung der strategischen Geschäftsführung mit dem Risikomanagement. Das bedeutet, dass zwischen der GF und den in der 2. LOD angesiedelten Bereichen, vor allem dem Risikomanagement, risikorelevante Informationen ausgetauscht werden. Einerseits kann dadurch gewährleistet werden, dass die Risikostrategie mit den Unternehmenszielen im Einklang steht, andererseits kann durch die Integration von Informationen aus dem RM-Prozess die strategische Planung verbessert werden.

Aus dieser Verzahnung der Geschäftsführung mit dem unternehmensweiten RM-System gehen mehrere Vorteile hervor:

- Ein eigenes Risikoprofil: Darin sind keine Einzelrisiken inkludiert, sondern die Risikoarten, die in der Industrie-EWF vorherrschen. Dieses Risikoprofil kann mit Hilfe der unternehmensweiten Risikolandkarte und der Stakeholder-Analyse formuliert werden.
- Information über Risikoherkunft: Auch hier dient die unternehmensweite Risk Map als Schnittstelle, mit welcher der Risikomanager einen guten Überblick über die wichtigsten Risiken geben kann. Durch die Zusammensetzung der Risk Map aus den Risikolandkarten der einzelnen RM-Prozesse kann jedes Risiko bis zu seinem Ursprung zurückverfolgt werden.
- Definition der Risikotragfähigkeit: Auf Basis der aus dem Risikomanagement gewonnen Informationen soll die Risikotragfähigkeit definiert werden. Manche Risiken können nicht gänzlich vermieden werden, weil man ihre Ursache nicht beeinflussen kann, andere Risiken will man nicht vermeiden, weil der Aufwand bzw. die Kosten zur Vermeidung das Ausmaß des Schadens übersteigen würden. Daraus resultiert die Risikotragfähigkeit – man stellt sich die Frage, ob man mit eventuell auftretenden Konsequenzen umgehen kann bzw. ob man sie sich leisten kann.
- Risikotoleranz: Wurde in der Industrie-EWF die Tragfähigkeit von Risiken definiert, wird eine Risikotoleranz bestimmt. Diese kann allerdings nicht für das ganze Unternehmen festgeschrieben werden, da sie von den einzelnen Risiken und deren Folgen abhängt. Bei manchen Risiken ist es sinnvoller, sie nicht so weit wie möglich zu reduzieren, sondern ein gewisses Restrisiko bestehen zu lassen. Auch hier muss man sich überlegen, wie der Aufwand im Verhältnis zu den Konsequenzen steht. Unabhängig vom Aufwand muss sich das gewählte Risiko natürlich innerhalb der gesetzlichen Vorgaben bewegen. Dies Prüfung soll eine Aufgabe der Internen Revision sein.

In der Industrie-EWF kann langfristig eine Risikostrategie für mehrere Management-Bereich sinnvoll sein, jedoch sollten zuerst die bereits genannte Punkte umgesetzt werden, da sie für die Implementierung eines unternehmensweiten RM-Systems essentiell sind.

Da es sich bei der Industrie-EWF um ein Produktionsunternehmen mit hohem Personal- und Materialaufwand handelt, sind die wohl wichtigsten Bereiche das Produktions- und Produktmanagement, das Beschaffungs-, Vertriebs- und Qualitätsmanagement sowie das Personalmanagement. Dazu kommen noch das Finanz- und Risikomanagement, sowie das Facilitymanagement, das auch die Verwaltung und Instandhaltung der Werksgebäude beinhaltet. Um einzelne Risikostrategien für diese Bereiche entwickeln zu können, muss jedoch zuerst eine Risikostrategie für das gesamte Unternehmen definiert und etabliert werden.

Wird noch ein Schritt weitergegangen, soll die Risikostrategie integriert und lernend werden. Integriert bedeutet, dass sie als Teil der Strategie implementiert ist und die Strategie auch beeinflusst. Es wird jedoch empfohlen, dass die Risikostrategie (wie bereits oben erwähnt wurde) schon bei der erstmaligen Einführung so weit als möglich in die Unternehmensstrategie integriert wird.

Lernend hingegen beschreibt eine Strategie, die regelmäßig überprüft (mit dem Erreichen von Reifegrad 2 wird dies schon erfüllt) und dann angepasst wird. Natürlich will ein Manager wissen, ob die Strategie, die zuvor entwickelt wurde, auch wirklich nach Plan ausgeführt wurde und ob sie funktioniert. Dieser Prozess wird als „single-loop learning“ bezeichnet. Das bedeutet, man überprüft das System (in diesem Fall die Strategie) auf Fehler und korrigiert diese gegebenenfalls [Kantamara, Vathanophas, 2014, S. 56].

Beim „double-loop learning“ wird ebenfalls der IST-Zustand mit dem Plan verglichen. Hier jedoch wird auch der Plan an sich in Frage gestellt [Kantamara et al., 2014, S. 56] – in diesem Fall die Strategie. Es wird also nicht nur der Fehler an sich betrachtet, sondern die ganze Vorgehensweise. Das hat folgenden Vorteil: Natürlich kann bei einem Fehler das Problem daran liegen, dass die Strategie nicht befolgt wurde. Ist das jedoch nicht der Fall, wird dieser Fehler immer wieder auftreten. Sucht man die Ursache auch bei der Strategie, kann man sie gegebenenfalls an die derzeitigen Bedürfnisse anpassen und so stetig verbessern. Diese regelmäßige Überprüfung fällt in den Aufgabenbereich der IR.

Weiters sollen realisierte Risiken und nicht realisierte Chancen betrachtet werden und in die Risikostrategie einbezogen werden. Durch die Integration realisierter Risiken ist man im Umgang damit schon erfahren, wodurch sie besser bewertet bzw. bewältigt werden können. Nicht realisierte Chancen zeigen auf, welcher Gewinn möglicherweise entgangen ist bzw. kann überprüft werden, ob es wirklich Chancen waren. So kann man in Zukunft bessere Entscheidungen treffen, da man immer besser und erfahrener wird. Deswegen ist auch eine konsequente Dokumentation so wichtig.

7.4 Auswirkung auf den ERMMA-Reifegrad

Die Etablierung, Dokumentation und Prüfung (durch die IR) einer Risikostrategie in der Industrie-EWF ist für den unternehmensweiten RM-Prozess essentiell. Nur so kann gewährleistet werden, dass die Ziele und Werte der Geschäftsführung in jedem Teilprozess des Risikomanagements umgesetzt bzw. gelebt werden. Außerdem werden die Risikopolitik bzw. der Risikoappetit des Unternehmens (ausgehend von der Eigentümervertretung) für Mitarbeiter in niedrigeren Hierarchieebenen dadurch greifbarer und verständlicher, sodass sie sich auch daran anpassen können. Manche der empfohlenen Schritte können, wie bereits erwähnt, erst mittel- bzw. langfristig umgesetzt werden und haben nicht oberste Priorität.

Durch die Umsetzung der wichtigen Maßnahmen kann mittelfristig ein Reifegrad von 4 erreicht werden.

8 Zusammenfassung und Ausblick

Zusammenfassung

Der zentrale Aspekt zu Beginn dieser Arbeit war das von Herrn Prof. Schwaiger an der TU Wien entwickelte ERMMA-Messmodell, mit dessen Hilfe der IST-Zustand des Risikomanagements in der fiktiven (an ein reales Unternehmen angelehnten) Industrie-EWF evaluiert werden konnte. Dieses Messmodell baut auf dem ISO/COSO-ERM-Modell auf, das den ISO-RM-Standard mit dem COSO-ERM-Framework kombiniert. Es gliedert das Risikomanagement in drei Dimensionen, die ERM-Governance, das Risiko-Managementsystem und die risikobasierte Planung und Steuerung. Für die Bewertung der drei Dimensionen wurde von Herrn Prof. Schwaiger ein Reifegradmodell geschaffen, das die drei Hauptdimensionen in jeweils drei Subdimensionen unterteilt. Der intelligente ERMMA-Fragebogen ordnet den Antworten Indikatoren zu, die jeweils Teil einer Subdimension sind und mit fünf Reifegraden verknüpft sind.

Das Ergebnis des ERMMA-Messmodells und die Absprache mit dem Risikomanager der Industrie-EWF ergab das größte Verbesserungspotential in den folgenden RM-Funktionen:

- RM-Prozess und Risikoorganisation
- Risikoverständnis und RM-Schulungen
- Risikostrategie

Das Ziel war, durch die Verbesserung der genannten RM-Funktionen ein Konzept für die Optimierung des unternehmensweiten Risikomanagements in der Industrie-EWF zu erstellen. Verschiedene Modelle aus Normen, Büchern und Zeitschriften dienten als Hilfe, um dieses Ziel zu erreichen. Ausschlaggebend waren dabei folgende Modelle/Normen:

- Die COSO ERM-Komponenten für die Beschreibung des Enterprise Risk Managements und die Definition von Prinzipien
- Die ISO 31000:2009 für die Gestaltung des RM-Prozesses mit den Teilschritten Risikoidentifizierung, Risikoanalyse, Risikobewertung, Risikobewältigung, Reporting und Überwachung
- Das 3-Lines-Of-Defense-Modell des Institute of Internal Auditors (IIA) für die organisationale Gestaltung des Risikomanagements

Nutzungsmöglichkeiten

Diese Arbeit kann als eine Art „Leitfaden“ herangezogen werden, der der Industrie-EWF und anderen Unternehmen die Möglichkeit gibt, ihr eigenes Risikomanagement-System zu überprüfen und weiterzuentwickeln. Der ERMMA-Reifegradtest ist gebührenfrei nach einer Registrierung durchführbar[22], es kann also jedes Unternehmen den eigenen IST-Zustand im Sinne des Reifegradmodells evaluieren.

Im Zuge der Masterarbeit wurden die (für das vorliegende Ergebnis) wichtigsten RM-Funktionen basierend auf Fachliteratur theoretisch aufgearbeitet und dann praktische Umsetzungskonzepte modelliert. Diese Konzepte können auch von anderen Unternehmen genutzt werden, individuelle Anpassungen müssen natürlich vorgenommen werden.

Weiters konnte die Qualität des ERMMA-Messmodells geprüft und bestätigt werden. Es eignet sich sehr gut, um ein bestehendes RM-System zu bewerten, sowie Stärken und Schwächen aufzudecken.

Ausblick

Für die Industrie-EWF ergeben sich mannigfaltige Herausforderungen in der Umsetzung dieses Vorgehensmodells. Um das unternehmensweite Risikomanagement-System nachhaltig zu verbessern, müssen einerseits viele Mitarbeiter (auch die Geschäftsführung und die Eigentümervertretung) eingebunden werden, andererseits müssen die Konzepte auch konsequent umgesetzt werden bzw. noch weiter auf die individuelle Situation angepasst werden. Da das obere Management und der Risikomanager diese Umsetzung aktiv unterstützen, werden diese Herausforderungen jedoch bald bewältigt werden.

Eine zukünftige Forschungsherausforderung kann eine allgemeine Aufarbeitung der einzelnen RM-Funktionen, sowohl in der Theorie als auch im praktischen Ansatz bezogen auf das Reifegradmodell, darstellen, da diese Arbeit auf die Industrie-EWF zugeschnitten ist.

[22] Siehe: https://ermma.imw.tuwien.ac.at/#/

9 Referenzen

Glossar

3-Lines-Of-Defense

Modell aus drei Verteidigungslinien (gegen Risiko), das die organisationale Struktur des Risikomanagements festlegt.

Bottom-Up

Methode, mit deren Hilfe detaillierte Teilprobleme und dann größere, darüber liegende Probleme gelöst werden können.

Enterprise Risk Management

Unternehmensweites Risikomanagement-System.

ERM-Governance

Übergeordnetes Master-Mind, legt die Risikopolitik und -kultur fest.

ERMMA

Enterprise Risk Management Maturity Assessment – Bewertung des ERM anhand von Reifegraden.

Industrie-EWF

Fiktives, an eine reale Firma angelehntes Industrieunternehmen.

Interne Revision

Unabhängige Prüf- und Beratungsstelle, die für ein Unternehmen wichtige Prozessabläufe prüft und unterstützt, unter anderem das Risikomanagement und das Interne Kontrollsystem.

Internes Kontrollsystem (IKS)

In die Arbeitsabläufe eines Unternehmens integrierter Prozess, der durchgeführt wird, um die Erfassung und Steuerung von Risiken sowie die Zielerreichung des Prozesses zu unterstützen.

Reifegrad

Bewertungsmethode zur Bestimmung des Fortschritts innerhalb einer RM-Funktion bzw. deren Qualität.

Risikoanalyse

Erfasste Risiken werden analysiert, um ihre Auswirkungen und die Wahrscheinlichkeit ihres Eintretens eruieren zu können.

Risikoappetit

Absicht, bewusst bestimmte Risiken einzugehen.

Risikobewältigung

Erfasste und bewertete Risiken werden bewältigt, indem sie vermieden, vermindert oder weitergegeben werden.

Risikobewertung

Erfasste Risiken werden mit Hilfe verschiedener Methoden in Bezug auf die Konsequenzen bewertet und mit den Vorgaben zur Tragfähigkeit der Risiken verglichen.

Risikoidentifikation

Erfassung von neuen oder bereits bestehenden Risiken in einem bestimmten Bereich oder einer Organisation mit Hilfe diverser Methoden.

Risikokultur

Legt ethische Werte und Verhaltensweisen bezüglich Risiko fest.

Risikolandkarte

Zweidimensionale Matrix zur Risikoanalyse, in die Risiken eingetragen werden. Die beiden Dimensionen sind Eintrittswahrscheinlichkeit und Auswirkungen.

Risikopolitik

Legt Bedeutung und Aufsichtsverantwortung für das Risikomanagement fest.

Risikoprioritätszahl (RPZ)

Methode der Risikoanalyse, um Risiken anhand ihrer Bedeutung, Eintrittswahrscheinlichkeit und Entdeckungswahrscheinlichkeit zu quantifizieren.

Top-Down

Ein Gesamtproblem wird von oben nach unten in mehrere Teilprobleme zerlegt, die dann detailliert betrachtet werden.

9.1 Literaturverzeichnis

Ahlemann, F., El Arbi, F., Kaiser, M., Heck, A. (2013). A process framework for theoretically grounded prescriptive research in the project management field. *International Journal of Project Management* (Ausgabe 31, S. 43-56).

Anderson, D. J., Eubanks, G. (2015). Leveraging COSO across the Three Lines of Defense. Institute of Internal Auditors (IIA).

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

COSO (2004). Enterprise Risk Management – Integrated Framework: Executive Summary. Committee Of Sponsoring Organizations Of The Treadway Commission.

COSO (2017). Enterprise Risk Management – Integrating with Strategy and Performance: Executive Summary. Committee Of Sponsoring Organizations Of The Treadway Commission.

Coughlan P., Coghlan D. (2002): Action research for operations management. *International Journal of Operations & Production Management* (2/2002, S.220-240). MCB UP Limited.

Detecon (2010). IKS – Interne Kontrollsysteme nach der 8. EU-Richtlinie. Fokus: Österreich und Deutschland. *Studie der Detecon (Schweiz) AG in Zusammenarbeit mit der Handelshochschule Leibzig und der Wirtschaftsuniversität Wien.*

Deutsches Vergabeportal (2019). Vier-Augen-Prinzip. Von https://www.dtvp.de/glossar/vier-augen-prinzip, Zugriff am 13.01.2019.

DIIR (2018). Internationale Grundlagen für die berufliche Praxis der Internen Revision. Deutsches Institut für Interne Revision. Von http://www.internerevision.at/fileadmin/Standards/Standards_2017.pdf, Zugriff am 10.01.2019

Ebert, C. (2013). Risikomanagement kompakt (S. 121-122). Springer Verlag.

French, S. (2009). Action research for practicing managers. *Journal of Management Development* (28/3, S. 187-204).

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

Hoffmann, W. (2017). Risikomanagement: Kurzanleitung Heft 4 (S. 20-23). DVP-Verlag Berlin.

Hoitsch, H., Winter, P., Bächle, R. (2005). Risikokultur und risikopolitische Grundsätze. *Zeitschrift für Controlling & Management* (49. Jg. 2005, H.2, S. 125-133). Springer Verlag.

Hölscher, R., Elfgen, R. (2002). Herausforderung Risikomanagement (S. 14). Springer Verlag.

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

IIA (2013). IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control. Institute of Internal Auditors (IIA).

ISO 31000:2009 (2009). Risk Management—Principles and Guidelines. International Standards Organisation.

Jung, T. (2003). Der Risikobegriff in Wissenschaft und Gesellschaft. *Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz* (7/2003, S. 545-547). Springer Verlag.

Kantamara P., Vathanophas V. (2014). Single-loop vs. double-loop learning: an obstacle or a success factor for organizational learning. *International Journal of Education and Research* (2/7/2014, S. 56-60).

Koubek, A. (2015). Risikobetrachtung in der ISO 9001:2015 Revision. Qualityaustria.

Lackes, R. (2019). Bottom-up-Prinzip. Gabler Wirtschaftslexikon. Von https://wirtschaftslexikon.gabler.de/definition/bottom-prinzip-27383, Zugriff am 26.02.2019.

Lewin K. (1946): Action research and minority problems. *Journal of Social Issues* (2(4), S. 34-36).

McNally, S. (2013). The 2013 COSO Framework & SOX Compliance. *Strategic Finance* (06/2013)

Müller-Stewens, G. (2019). Top-Down-Prinzip. Gabler Wirtschaftslexikon. Von https://wirtschaftslexikon.gabler.de/definition/top-down-prinzip-49846, Zugriff am 26.02.2019.

Muschick, E., Müller, P. H. (1987): Entscheidungspraxis: Ziele, Verfahren, Konsequenzen (S. 108-132). Verlag Technik Berlin.

ONR 49000:2014 (2014). – Risikomanagement für Organisationen und Systeme (S. 4-23). Austrian Standards Institute.

PwC (2014). Interne Revision: Überwachung und Nutzen für Aufsichtsorgane. Von http://files.pwc.at/publications/aufsichtsrat/Interne-Revision.pdf, Zugriff am 12.01.2019

Qualityaustria (2019). Lehrgangsreihe Risikomanagement. Qualityaustria. Von https://www.qualityaustria.com/index.php?id=2426, Zugriff am 08.01.2019.

Rechnungshof (2016). Positionen: Leitfaden zur Überprüfung von Internen Kontrollsystemen (Reihe 2016/3).

Renner, J. (2014). Interne Revision: Überwachung und Nutzen für Aufsichtsorgane. *Tool-Box für Aufsichtsräte*. PwC Österreich GmbH. Von https://www.pwc.at/de/publikationen/aufsichtsrat/interne-revision.pdf, Zugriff am 12.01.2018.

RIS (2015). Bundesrecht konsolidiert. Rechtsinformationssystem des Bundes. Von https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12039576, Zugriff am 21.11.2018.

Romeike, F., Hager, P. (2013). Erfolgsfaktor Risikomanagement 3.0. Springer Gabler Verlag.

Saßen, S. (2019). Risikomanagement (S. 42). Vincentz Network.

Schwaiger, W. (2017). Wie reif ist das Enterprise Risk-Management Ihres Unternehmens? *Österreichisches Jahrbuch für Risikomanagement 2017* (S. 144-153). TÜV AUSTRIA/Goiser.

Schwaiger, W., Brandstätter, M. (2018). In welchen Bereichen beeinflusst die Interne Revision die Qualität (Reifegrad) des ERM-Systems? *Jahrbuch des Instituts für Interne Revision Österreich* (S. 3-12).

Schwaiger, W., Brandstätter, M. (2019). ERM-Maturity Assessment (ERMMA): Definition von ERM-Best-Practice-Reifegraden und deren Messung in Unternehmen.

Schwaiger, W., Hilscher, C., Brandstätter, M. (2018). Die Geschäftsführung fragt sich „Wie reif ist unser Risikomanagement?“ und macht sogleich den Test. *Jahrbuch Risikomanagement 2019* (S. 173-190). TÜV Österreich.

Stangl, H. (2017). Chefsache. *Fachzeitschrift KPMG Österreich* (12/2017, S.20-21).

Thies, K. H. W. (2009). Management operationaler IT- und Prozess-Risiken (S. 48-51). Springer Verlag.

Weißensteiner, C. (2014). Begriffserklärungen und Grundlagen des Risikomanagements. *Reputation als Risikofaktor in technologieorientierten Unternehmen*. Springer Verlag.

WIFI (2019). Kurse Risikomanagement. WIFI Österreich. Von https://www.wifi.at/kursbuch/technik/risikomanagement/risikomanagement, Zugriff am 08.01.2019.

Zojer E., Faul E., Mayer H. (2013): Aktionsforschung – "Be part of it". *Pro Care* (09/2013, S. 12-16). Springer-Verlag.

9.2 Abbildungsverzeichnis

9.3 Tabellenverzeichnis