RMA
Risk Management & Rating Association e.V.

**Geschäftsstelle**
RMA Risk Management & Rating Association e.V.
Tel.: +49.(0)1801 – RMA TEL (762 835)
office@rma-ev.org, www.rma-ev.org



# Zeit der Vorsorge

**Ralf A. Huber,** Mitglied des Vorstands der RMA Risk Management & Rating Association e.V.

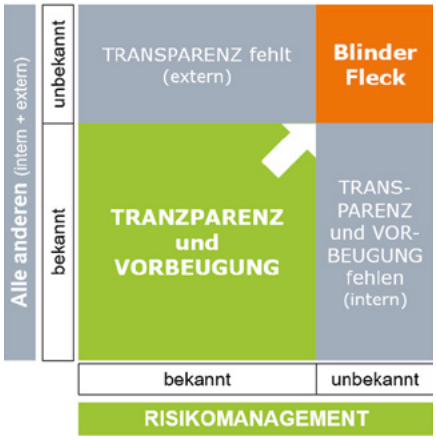
**Liebe Leserinnen und Leser,**

wenn Unternehmen Vorsorge für bestandsgefährdende Risiken treffen, wie erklärt sich dann die Abhängigkeit von einzelnen Lieferanten, die, z. B. durch Single Source, seit mind. 30 Jahren verstärkt wurde? Der Fokus wurde ausschließlich auf den Preis gesetzt und nicht auf die Verfügbarkeit. Der Preis, den es nun für die Verfügbarkeit zu zahlen gilt, kann für einige Unternehmen bestandsgefährdend werden.

Die Wahrscheinlichkeit für einen mehrtägigen Blackout wurde in der Schweiz bis vor Kurzem mit ca. 3%, also einmal innerhalb von 30 Jahren eingeschätzt. In der „NZZ am Sonntag" vom 18. September 2022 beschreibt der Artikel „Guet Nacht, Züri!" die möglichen Auswirkungen eines totalen Blackouts als fiktives Szenario für die Stadt Zürich anhand der Risikoanalyse „Katastrophen und Notlagen Schweiz". Das Szenario versetzt die Stadt ins Mittelalter zurück! Die Vorsorge mit 41 beheizten städtischen Notfalltreffpunkten ist beruhigend und hoffentlich trifft diese gute Vorsorge auch für deutsche Großstädte im gleichen Maße zu!

Für Risiken im blinden Fleck gibt es keine Vorsorge.

Lassen Sie mich den blinden Fleck anhand der nachfolgenden Darstellung basierend auf dem 1955 in der Psychologie entwickelten Johari-Fenster erklären:




Es sollte von allen am Risikomanagementprozess Beteiligten angestrebt werden, den blinden Fleck so klein wie möglich zu halten. Dies geschieht dadurch, dass die bekannten Risiken transparent sind, eine Vorsorge stattfindet und in regelmäßigen Abständen Workshops zu den Extremrisiken, z. B. mit einem Zeithorizont größer 100 Jahre, stattfinden. Achten Sie einmal auf die Skala bei den Eintrittswahrscheinlichkeiten in den sogenannten Heatmaps bei den Veröffentlichungen in den Risikoberichten der Geschäftsberichte börsennotierter Unternehmen. Mir fällt hier immer wieder auf, dass nur Risiken abgebildet sind, die in einem Zeithorizont von 50 Jahren oder kleiner einmal auftreten können. Dies stellt leider ein Vergrößern des blinden Flecks dar, falls es nicht mit entsprechenden Risikoworkshops abgesichert wird.

Eine kritische Vorstufe zum blinden Fleck ergibt sich, wenn ein intern unbekanntes Risiko leicht erkannt werden kann und dennoch keinerlei Vorsorge stattgefunden hat.

Risiken, die als unmöglich eingeschätzt werden, z. B. der Hurricane Katrina mit einer Eintrittswahrscheinlichkeit von ca. einmal in 400 Jahren, die Pandemie und der Krieg in der Ukraine, fallen somit direkt unter den blinden Fleck und es wird ebenfalls keine oder wenig Vorsorge betrieben.

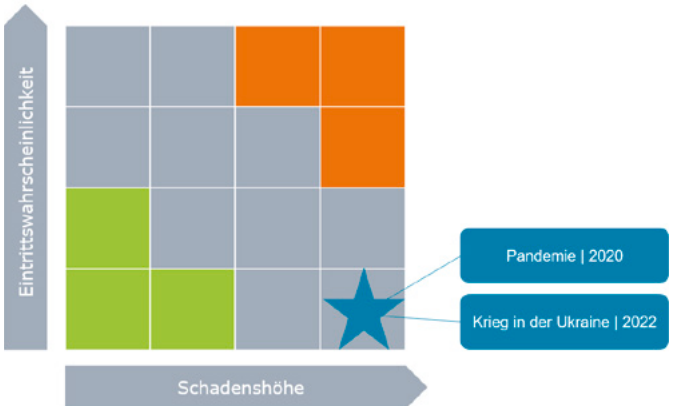
Wenn es niemanden gibt, der sich mit diesen Risiken beschäftigt oder vom Management gehört und ernst genommen wird, dann ist man beim Eintritt gänzlich unvorbereitet, also überrascht.

Hätte die kritische Gasabhängigkeit früher wahrgenommen werden können? Wären dann nicht Maßnahmen wie LNG als Alternative und ggf. mehr und vor allem ▶

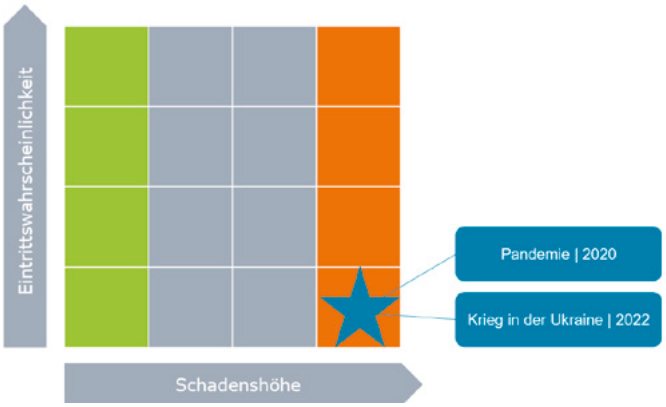
gefüllte Speicher möglich gewesen? In der Wirtschaftswoche wurde kürzlich berichtet, dass der frühere Vorstandschef 2017 gefragt wurde, ob Russland eine Abhängigkeit vom russischen Gas erzeugen könnte, um dann den Gashahn abzudrehen. Seine Antwort war: Das ist doch ABSURD! Ein treffendes Beispiel für eine Einschätzung als unmöglich (= blinder Fleck), aber leider kein Einzelfall. BASF ist mit 4 % des Gesamtgasverbrauches in Deutschland der größte Abnehmer. Die zweite Branche mit einem ähnlich hohen Gasbedarf wie die Chemie ist die Metallverarbeitung.

Die Bundesnetzagentur hat sieben Szenarien für das Gas-Mengengerüst von Juni 2022 bis Juni 2023 berechnet und Ende Juni auf der eigenen Homepage veröffentlicht. Vier Szenarien führen nicht zum Ausfall. Bei den anderen Szenarien ist ein mehrwöchiger Lieferausfall, beginnend im Januar oder Februar 2023, nicht auszuschließen. Um diesen Szenarien entgehen zu können, muss Nordstream 1 ohne Einschränkung weiter laufen und die eigenen Gasexporte reduziert werden. Da die privaten Haushalte vor der Industrie mit Gas versorgt werden, könnte eine Maßnahme der Industrie das bereits erprobte Homeoffice für die Verwaltung sein. In den Szenarien ist durch die Herabsenkung der Zimmertemperaturen, usw. schon eine Einsparung von 20 % berücksichtigt. Die mittlerweile stattgefundenen Einschränkungen bei der Belieferung von Nordstream 1 wirken nun verschärfend und es wird darauf ankommen, ob die LNG-Versorgung ab Januar 2023 in vollem Umfang stattfindet.

In den aktuellen Risikoberichten der börsennotierten Unternehmen wird leider sehr oft eine Heatmap veröffentlicht, die den Erwartungswert als Priorität hat:




Risiken im höchsten Schadensbereich werden so in zwei Bereiche aufgeteilt, die wirklich hohen Risiken (= orange) und die durch die geringere Eintrittswahrscheinlichkeit verniedlichten genauso hohen Risiken (= grau). Es ist wohl davon auszugehen, dass diese zwei dargestellten Risikoklassen auch zu Unterschieden in der Risikovorsorge führen. Gerade in der heutigen Zeit mit allen Verschärfungen des Gesetzgebers (z. B. §1 StaRUG, §91 Abs. 3 AktG) kann ich mich über solche Darstellungen nur wundern. Ich könnte z. B. nicht erklären, warum ich unter der Vorgabe des frühzeitigen Erkennens von Bestandsgefährdungen in der Schadenshöhe gleiche Risiken anders behandle. Deshalb hatte ich mich als damals noch operativer Risikomanager ab 2017 entschlossen, eine nur nach der Schadenshöhe priorisierte Heatmap im Geschäftsbericht zu veröffentlichen:




So wird jedem Betrachter sofort klar, es gibt hier kein Zwei-Klassen-Risiko im höchsten Schadensbereich (= orange) und dies trifft vor allem auch für die üblicherweise mit geringen Eintrittswahrscheinlichkeiten eingeschätzten Extremrisiken, wie hier die Pandemie und den Krieg in der Ukraine zu. Wenn für die im Unternehmen bekannten Risiken eine Vorsorge umgesetzt wird, dann haben wir ein wirklich wirksames Risikomanagementsystem erreicht.

Sorgen Sie dafür, dass in Ihrem Unternehmen der blinde Fleck verkleinert und die Vorsorge vergrößert wird!

*Ihr Ralf A. Huber*

# Trusted Governance – vom Risikomanagement zur vertrauenswürdigen Unternehmenssteuerung

In einer Welt übersät von Krisen sowie plötzlich aufkeimender und vernetzter Risiken, ist ein holistischer Blick unverzichtbar, um Komplexität zu reduzieren, Vertrauen zu schützen und Unternehmensziele zuverlässiger zu erreichen.

Ein integrierter Risikomanagementansatz bietet diesen Blick, indem er nicht nur das wachsende Unternehmensökosystem ganzheitlich überblickt, sondern auch verschiedene bereits bestehende Risikomanagementaktivitäten verzahnt und technologisch verknüpft.

Die Herausforderung besteht für den heutigen Risikomanager darin, nicht nur zeitnah alle relevanten Informationen zu erhalten, sondern auch deren Interdependenzen zu überblicken, um frühzeitig kritische Kausalverflechtungen zu erkennen.

Tatsächlich werden Risiken häufig bereits dezentral an vielen Stellen im Unternehmen isoliert identifiziert und gesteuert, teilweise ohne dies explizit „Risikomanagement" zu nennen. Dabei werden heterogene Ansätze verwendet, um der Natur des Risikos gerecht zu werden. So denkt beispielsweise eine Personalabteilung an Risiken mit Auswirkung auf die Fluktuation, Compliance an Verstöße gegen Verpflichtungen und der Vertrieb an Auswirkungen auf den Absatz. Alle jedoch verstehen hierunter potentielle Zielabweichungen und damit implizit Risiken, die sie schon heute aktiv steuern.

Umso wichtiger ist es für den Risikomanager, ein Grundverständnis darüber zu haben, wie aus der Unternehmensvision, den Werten und Leitplanken tatsächlich Ziele abgeleitet und entlang der Governance-Struktur operationalisiert werden.

Die Kunst der Integration liegt darin, im Sinne der Subsidiarität, einen „kleinsten gemeinsamen Nenner" zu finden. Mit einem integrativen Rahmenwerk müssen klare Mindestanforderungen für Konsistenz geschaffen werden, beispielsweise für Bewertungsschemata und Berichtsprozesse. Auf diesen aufbauend können Spezifika entlang der Governance-Struktur eines Unternehmens ergänzt werden. Beispielsweise könnten Personalrisiken zusätzlich zu klassischen Risikobewertungsdimensionen, wie Eintrittswahrscheinlichkeit und finanzielle Auswirkung auch hinsichtlich ihrer Auswirkung auf die Fluktuation bewertet werden.

Auch aus technologischer Sicht gilt es, diese gemeinsame Basis im Sinne einer Plattform zu verstehen, um verschiedene risikorelevante Informationen zu integrieren. Die Integration von Informationen sollte dabei aber nicht mit einer Konsolidierung verwechselt werden. Es gilt vielmehr die dahinterstehenden Informationen sinnvoll zu verzahnen, um Kausalverflechtungen zu erkennen und sie in den Kontext der Geschäftsziele zu stellen.


**Abbildung 1: Trusted Governance Framework**

Gelingt es Unternehmen, ihre Risikomanagementaktivitäten klar an ihren Zielen auszurichten und diese methodisch, organisatorisch und technologisch zu integrieren, so werden Ziele zuverlässiger und binnen festgelegter Leitplanken erreicht. Das Risikomanagement fördert somit das Vertrauen in die Unternehmenssteuerung und schafft damit eine „Trusted Governance". ■

*Daniel E. Cassel & Nicolai A. I. Butsch*
HORVÁTH
*Horváth und Partner GmbH*

# Personalrisiken im Fokus: erste Erkenntnisse aus einem Projekt der Hans-Böckler-Stiftung

Ein aktuelles Forschungsprojekt der Dualen Hochschule Baden-Württemberg hat u. a. das Ziel, Personalrisiken aus Sicht der Arbeitnehmervertretung in Aufsichtsräten herauszuarbeiten. Gefördert von der Hans-Böckler-Stiftung wurden im Rahmen einer schriftlichen Befragung von Arbeitnehmervertretungen im Aufsichtsrat (Schwerpunkt Großunternehmen > 10.000 MA) zwischen April - Juni 2021 (n=329) nun erste Erkenntnisse gesammelt und ausgewertet. Neben Fragen zur generellen Strategiefähigkeit des Personalmanagements und der Güte des Risikomanagements wurde auch nach konkreten und akut relevanten Personalrisiken gefragt. Die so zusammengetragenen Erkenntnisse sind deshalb von so großer Bedeutung, da die Mehrzahl der Arbeitnehmervertretungen im Aufsichtsrat selbst im Unternehmen beschäftigt sind. Sie haben entsprechende Einblicke in die operativen Prozesse und können eine recht belastbare Momentaufnahme abgeben.

Zunächst wurde eine Abfrage zur Relevanz verschiedener Personalrisikofelder abgefragt. Dabei ergab sich, dass Motivationsrisiken sowie Anpassungsrisiken als relevanteste Kategorien angesehen wurden. Diese kategorienbasierte Abfrage wurde dann er- ▶

gänzt durch eine Freitextabfrage, bei der die Aufsichtsräte gebeten wurden, konkrete Personalrisiken in „ihren Worten" zu benennen. Insgesamt wurden so 789 Angaben in einem Freitextfeld gemacht, die anschließend systematisch nach Themen gruppiert wurden. Die Abbildung unten zeigt dabei die Verteilung.

Es fällt auf, dass Risiken durch das Personalmanagement die mit Abstand am häufigsten genannte Kategorie darstellt (42,8%). Konkret wurden fehlende Personalentwicklungsmöglichkeiten, eine fehlende/unpassende Personalstrategie oder eine falsche Methodik bei der Personalauswahl genannt. Diese Ergebnisse geben Hinweise auf eine möglicherweise mangelnde Strategieanbindung des Personalmanagements, die bereits in anderen Projekten genannt wurde und bestätigen auch Hinweise aus Interviews mit Aufsichtsräten in der ersten Phase dieses Projektes. Dies muss jedoch noch weiter untersucht werden.

Bei den weiteren Risiken aus dem Unternehmen wurden vor allem Risiken aus der Unternehmensstruktur mit Auswirkungen auf das Personal genannt, Führungsrisiken oder fehlende Ressourcen im Unternehmen.

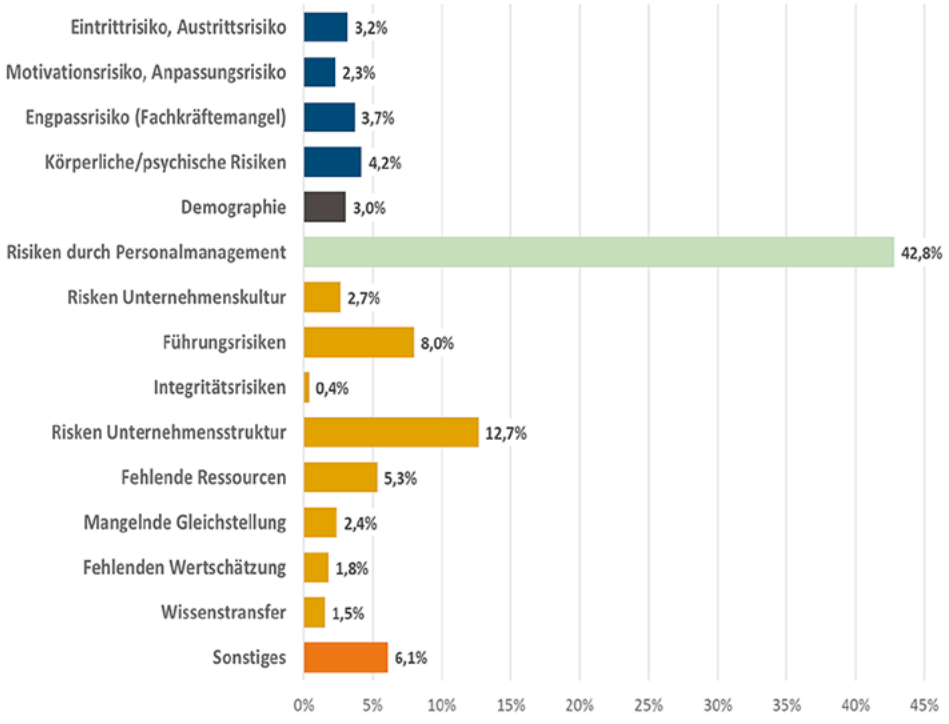
Diese Ergebnisse können zunächst einmal „nur" als Momentaufnahmen dienen. Insbesondere Personalrisiken und ihre Schwerpunkte scheinen über den Zeitverlauf (entlang der spezifischen wirtschaftlichen Entwicklung) zu variieren. Anderseits dienen die Ergebnisse vor allem der Entwicklung einer praxisgerechten Betrachtungsweise und auch Semantik, um mit geeigneten didaktischen und auch kommunikativen Mitteln zentrale Entscheidungsträger der Unternehmensführung zu erreichen und fachlich-methodisch zu stärken.

Mit den Projektergebnissen sollen Aufsichtsräten in ihrer Kontroll- UND Beratungsfunktion wichtige Argumente und Kenntnisse für eine anforderungsgerechte und zukunftsgerichtete Personalstrategie sowie zur Analyse von Personalrisiken an die Hand gegeben werden. Als nächster Schritt ist die Auswertung einer zweiten Befragung geplant, die die Ergebnisse dieser ersten Befragung verifizieren helfen soll und dazu auch eine Verknüpfung der Angaben zum Personalrisikomanagement mit dem bestehenden Risikomanagementsystem erlaubt.

Mehr Informationen zum Projekt können unter folgender Adresse bezogen werden:

https://www.mitbestimmung.de/html/personalrisiken-ein-unterschatzter-16316.html

*Autoren: Prof. Dr. Thomas Berger (DHBW Stuttgart), Jan-Paul Giertz (Hans-Böckler-Stiftung)*





# Impressum

**Ralf Kimpel**
Vorsitzender des Vorstands
der RMA Risk Management
& Rating Association e.V.
ralf.kimpel@rma-ev.org
V.i.S.d.P.

**RMA-Geschäftsstelle**
RMA Risk Management
& Rating Association e.V.
Zeppelinstr. 73
D-81669 München

Tel.: +49.(0)1801 - RMA TEL (762 835)
Fax: +49.(0)1801 - RMA FAX (762 329)
office@rma-ev.org | www.rma-ev.org

**Prof. Dr. Werner Gleißner**
fachartikel@futurevalue.de
Tel.: 0711 79735830


## RMA Top-Events

**15. November 2022:** Stammtisch Baden Risikomanagement & Revision

**16. November 2022:** RMA-Konferenz Rating & Krisenmanagement

**17. November 2022:** Seminar „Volkswirtschaftliche Krisen - Quelle möglicher bestandsgefährdender Entwicklungen"

**25. November 2022:**
Online-Seminar „Einführung in die Identifikation und Analyse von Nachhaltigkeits- bzw. Klimarisiken"

**30. November 2022:**
AK „Interne Revision und Risikomanagement"

**01. Dezember 2022:**
AK „Supply Chain Risk Management"

**01. Dezember 2022:**
Webinar „Das Lieferkettensorgfaltspflichtengesetz - Umsetzung mit R2C_GRC"

**01. Dezember 2022:**
Online-Seminar „Planung in unsicheren Zeiten: Erfolgsfaktoren für einen effektiven Planungsprozess"

**19. Januar 2023:**
AK „Supply Chain Risk Management"

**08. & 09.05.2023:**
Risk Management Congress

# Was ist Informationsrisikomanagement?

„Was würden wir beim Ausfall des zentralen E-Mail-Servers tun?“, „Welche Geschäftsprozesse könnten dann nicht durchgeführt werden?“, „Wie groß wäre der monetäre Schaden?“, „Wie stark würde das Image des Unternehmens darunter leiden?“

Auch wenn wir die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen schätzen und schützen, können Informationsrisiken in einer Welt mit zunehmender Digitalisierung, unternehmensübergreifender Vernetzung und verstärkter Auslagerung von IT-Dienstleistungen kaum ausgeschlossen werden. Daher ist es wichtig, ein transparentes und proaktives Informationsrisikomanagement (IRM) zu implementieren, welches sich flexibel nach dem Bedarf und der aktuellen Situation des Unternehmens richtet. Vor allem für Institute und Unternehmen, die regulatorische Anforderungen erfüllen und über durchgeführte Risikoanalysen und definierte Schutzmaßnahmen regelmäßig berichten müssen, ist ein effektives und effizientes Informationsrisikomanagement unverzichtbar.

Jegliche Informationen im Unternehmen sind den Fachbereichen als Eigentümern zugeordnet und bedienen die Geschäftsprozesse - die wesentlichen Bestandteile des Businessmodells. Pro Geschäftsprozess wird ein Informationsverbund definiert, zu dem die für den Geschäftsprozess relevanten Informationen und Unternehmensbereiche, IT-Systeme, aber auch die Netz- und Gebäudeinfrastruktur gehören. Das IRM bezieht sich daher nicht nur auf die IT, sondern auch auf alle Fachbereiche und relevante Schnittstellen und Funktionen. Da immer mehr Dienstleistungen, z. B. bei der Nutzung von Cloudservices, an externe Dienstleister ausgelagert werden, müssen auch diese zwingend in das IRM miteinbezogen werden.

Aufgrund der Komplexität der Informationsverbunde und der Datenlandschaft bestehen immerwährende Bedrohungen für das Unternehmen. Dabei kann es sich um technische Defekte und höhere Gewalt handeln, aber auch die eigenen Mitarbeiter*innen können die Schutzziele der Informationen gefährden. Oft passiert dies unbewusst durch menschliches Versagen. Da Unternehmen immer wieder neuen Bedrohungen gegenüberstehen - wie seit einigen Jahren vermehrt den Hackerangriffen aus dem Cyberraum – sollten sich die Beauftragten des IRM fortlaufend über neue Entwicklungen informieren. Die sich ständig verändernden Angriffsmöglichkeiten können über Szenarien in die Betrachtungen des IRM einfließen. So werden Risiken, die durch einen unzulänglichen Schutz der Informationsverbunde entstehen können, proaktiv vermindert.

Um sich aktiv gegen die Gefährdungen vorzubereiten, sollte der Schutzbedarf der Daten nachvollziehbar und in angemessenem Umfang anhand der Schutzziele „Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität“ reproduzierbar definiert werden. Gezielte Fragen zur Einstufung in Schutzniveaus helfen dabei: „In welchen Bereichen werden vertrauliche oder personenbezogene Daten verarbeitet?“, „Welche Geschäftsprozesse müssen sich auf Aktualität und Korrektheit der Informationen verlassen können?“, „Wie stark eingeschränkt wäre dann die Aufgabenerfüllung im Falle einer Kompromittierung der Daten?“ und „Welcher Schaden kann für das Unternehmen entstehen?“

Ist der Schutzbedarf bekannt, werden die Maßnahmen eines vordefinierten Sollmaßnahmenkataloges angewandt, um das Unternehmen entsprechend abzusichern. Dieser orientiert sich an den aktuellen betrieblichen Erfordernissen und der individuellen branchenbezogenen Risikosituation. So kann im Vergleich zu den anderen Schutzzielen beispielsweise für Unternehmen im Finanzwesen die Integrität, im Bereich „Forschung und Entwicklung“ die Vertraulichkeit und im Transportsektor unter Umständen die Verfügbarkeit der Informationen wichtiger sein.

Schließlich sollte im Rahmen einer Risikoanalyse regelmäßig ein Abgleich der Ist- und Sollmaßnahmen durchgeführt werden, um Restrisiken anhand von Schadenspotenzial und Schadenshäufigkeit zu identifizieren. Restrisiken, die gemäß des Risikoappetits des Unternehmens genehmigt werden, werden dann in das Management der operationellen Risiken überführt. Dabei gilt es primär, eine Balance zwischen der zur Risikomitigierung notwendigen Investition und dem noch vorhandenen Restrisiko zu finden. Mit der Kenntnis, welcher Schutzbedarf besteht und welche konkreten Maßnahmen bei bewusst akzeptiertem Restrisiko durchzuführen sind, helfen differenzierte Richtlinien, Verfahren und Technologien beim Management der Schwachstellen. Eine so geschaffene Transparenz schärft das Informationsrisikobewusstsein bei der Geschäftsleitung und sensibilisiert Mitarbeiter auf Risiken und Risikominimierung durch vorgelebte Praktizierung der definierten Maßnahmen.

Der gemeinsame Arbeitskreis „Information Risk Management“ der Risk Management & Rating Association e.V. (RMA) und des ISACA Germany Chapter e.V. befasst sich mit Themen rund um das Informationsrisikomanagement und erarbeitet Handlungsempfehlungen für Praktiker des Risikomanagements. Die Mitglieder betrachten konkrete Fragestellungen zur Identifikation von Bedrohungen der Informations- und IT-Landschaft, zu deren Auswirkungen auf Unternehmen und zu praktischen, proaktiven und reaktiven Maßnahmen. Die praktischen Handlungsempfehlungen bieten eine Möglichkeit, sich schrittweise dieser herausfordernden Thematik zu nähern und so Informationsrisiken – auf wirtschaftlich sinnvolle Art und Weise – frühzeitig zu identifizieren und zu minimieren. ■

*Zu den Autoren: Dr. Anne Hamnett ist Senior Consultant in Frankfurt bei der globalen, auf Risikomanagement spezialisierten Unternehmensberatung, Control Risks.*

*Andreas J. Henke ist Senior Manager Information Security and Business Risk Management in Frankfurt bei der Deutschen Lufthansa AG.*

# 32. Treffen des RMA-Arbeitskreises „integriertes Risikomanagement“ (AK iRM)

## Erste Ergebnisse der Klein-Arbeitsgruppe: „Interdisziplinäres iRM-Projektmanagement“ und Impulsvortrag zur „integrierten Risikobewertung und -aggregation“

„Was heißt integriertes Risikomanagement bei mir im Unternehmen?“ – „Was macht die Zusammenarbeit schwierig und was sind nachweisbare Erfolge der Integration des Enterprise Risk Managements?“ – mit diesen Fragen setzten sich die Mitglieder der seit Juni 2022 gegründeten Klein-Arbeitsgruppe (KAG) „interdisziplinäres iRM-Projektmanagement“ auseinander. Ziel ist ein systematischer Erkenntnisgewinn zu Umsetzungserfolgen, wie auch -schwierigkeiten bei der Integration des Risikomanagements (iRM) in bestehende Managementsysteme, die in einem Zusammenhang mit der jeweils genutzten Methodik bei den meistens als Projekt umgesetzten Analyse-, Abstimmungs- und Implementierungsschritten stehen.

Im Rahmen des virtuellen 32. AK iRM-Meetings wurden am 23.09.2022 nun die ersten Erkenntnisse vorgestellt: Aus Sicht der Arbeitsgruppe spiegelt sich die Umsetzungsbesonderheit des Risikomanagements der vertretenen Unternehmen im Spannungsfeld zwischen „Compliance-fokussierten“ und „Performance-, Prozess-, Liquiditäts- bzw. Bestandsschutz-orientierten“ Systemen wider. Unter dem Motto: „Befolge Standards!“ wurde das Risikomanagement integriert, um relevante (gesetzliche, behördliche, kundenseitige oder andere Standard-) Anforderungen zu erfüllen. Neben diesem richtigen und wichtigen Ansatz gibt es auch praktische Ansätze aus den Erfahrungen der KAG-Mitglieder, nach denen aktuell die Implementierung „eines Risikomanagement-Approach für alle Bereiche“ mit dem Ziel der Steuerung und Dokumentation von unternehmensweiten Risiken in einer Softwarelösung angestrebt wird. Hierbei sollen die verschiedenen Risiko-Assessment-Methoden unter einem Dach gebündelt werden. In diesem Zusammenhang sind operationale Risiken, z. B. aus dem Datenschutz, IT & Cyber-Risiken, Tax-Compliance und strategische Risiken sowie Reputationsrisiken als grundlegende Arten zu verstehen, die jeweils eine andere Art von Bedrohung darstellen. Hier gilt es, den „richtigen Maßstab“ für die Risiko-Bewertung und für die Darstellung der Zusammenhänge zu finden. Als sehr wichtig wurde von den Vertretern dieses RM-Ansatzes die Kopplung der Risiken an das betriebswirtschaftliche Controlling und an die Unternehmenssteuerung angesehen.

Der Prozess der Integration – d.h. dem Zusammenführen und Einbinden diverser Anforderungen (aus QMS, UMS, ISMS, SGA-MS sowie Anforderungen weiterer interessierter Parteien) wurde stets auch verbunden mit einem kulturellen Wandel (Change-Prozess), der parallel zum Tagesgeschäft erfolgen wird. Daher ist die Überführung der Integrations-Aktivitäten in ein interdisziplinäres iRM-Projekt (mit Zielen, Ressourcen, Commitments und entsprechenden Beteiligungen interner und ggf. externer Art) zu empfehlen.

Die im AK-Meeting vorgestellten Erkenntnisse wurden im Rahmen der anschließenden moderierten Diskussion durch individuelle Statements ergänzt und erweitert. So wurde z. B. festgestellt, dass ESG-Risiken in das Risikoinventar zu übernehmen sind, um Anforderungen aus gesetzlicher bzw. Kundensicht frühzeitig zu erkennen und entsprechend bewältigen zu können. Ein weiterer Teilnehmer sprach über seine Erfahrung (im Konzernmaßstab), dass eine Integration über spezielle Arbeitskreise und thematische wöchentliche Treffen mit den Bereichsleitern realisiert wurde. Damit konnte die erforderliche Awareness geschaffen werden.

Um im Rahmen der KAG interdisziplinäres iRM-Projektmanagement weitere Erfahrungen zum „methodisch-didaktisch geeigneten Miteinander“ zwischen den Risikomanager/-innen und den Akteuren der verschiedenen Managementsysteme sowie den relevanten Fach- und Führungskräften unter den ständig anwachsenden Herausforderungen an ein unternehmensweites integriertes Risikosystem analysieren zu können und um Handlungsableitungen für Mittelstands- wie Konzern-Organisationen zu formulieren, sucht die AK-Leitung weitere aktive und erfahrene Umsetzerinnen bzw. Umsetzer aus dem Integrationsumfeld von Unternehmen. Interessierte können sich melden unter: www.rma-ev.org/verein/arbeitskreise/integriertes-risikomanagement; Kontakt: Dirk Rönnecke, AK-Leiter (kundenpartner.rt@mac.com)

Im Anschluss an diese erste Session stellte Dr. Uwe Wehrspohn (Wehrspohn GmbH & Co.KG) zwei professionelle Softwaretools zur Risikobewertung und -aggregation vor, die z. B. im Rahmen eines Integrationsprojektes für die Unterstützung der Risikomanager und weiterer interessierter Parteien zum Einsatz kommen können. Mit „Risk Kit“ können Risikoanalysen und -Simulationen in Excel realisiert werden. Der vorgestellte „Werkzeugkasten“ kann lt. Dr. Wehrspohn bestehende Excel-Modelle – wie etwa ein zuvor ermitteltes und einzelbewertetes Risikoinventar – zu Simulationen erweitern.

Aufgrund der Kompatibilität mit dem zweiten Softwareprodukt können die in einem Integrationsprojekt erforderlichen Stakeholder mit ihren jeweiligen Hintergrunderfahrungen zielbezogen eingebunden werden. Der „Enterprise Risk Evaluator“ (ERE) unterstützt Organisationen bei der Realisierung des Risikomanagementprozesses innerhalb der Gesamtorganisation. Dies betrifft das Management von Daten, Workflow, Analysen, Berichten, Eskalationen und die Dokumentation – von der kleinsten Einheit bis zur Geschäftsführung bzw. Aufsichtsrat.

Fazit: Die AK-Leitung dankt allen Beteiligten für deren aktive Mitwirkung und schaut mit Freude auf das nächste spannende Treffen im Frühjahr 2023 – vielleicht einmal wieder in Form eines persönlichen Vor-Ort-Treffens in einem Gastgeber-Unternehmen. Vorschläge für eine derartige Zusammenkunft und die Vorteile der Gastgeber-Rolle können gern mit der AK- iRM-Leitung erörtert werden.

*Geva Johänntgen und Dirk Rönnecke*

# RMA-Konferenz Rating & Krisenmanagement am Mittwoch, den 16. November 2022

**Veranstaltungsort: Munich Airport Marriott Hotel, Alois-Steinecker-Straße 20, 85354 Freising**

Liebe Mitglieder und Interessierte für die Themen des Ratings und des Krisenmanagements,die **RMA-Konferenz Rating & Krisenmanagement** steht im Zeichen der **aktuellen Wissensvermittlung** von Experten für Experten und Entscheider - in Theorie und Praxis.

**Themen** wie Sustainable Finance, Integration von ESG-Kriterien in Ratingprozessen, zukünftige Nachhaltigkeitsberichterstattung, mit dem Management von ESG-Faktoren zu guten Ratingbewertungen, aktuelle Krisenentwicklungen und die Bedeutung der neuen ISO für die Fortentwicklung des Krisenmanagements sowie die Qualität des Krisenmanagements für die Wertschätzung eines Unternehmens stehen im Mittepunkt der Konferenz. Durch **praktische Beispiele** werden diese Themen anschaulich erläutert.



Jetzt dürfen wir Sie gerne zur RMA-Konferenz Rating & Krisenmanagement am 16. November 2022 einladen, die als **Präsenzveranstaltung** im Munich Airport Marriott Hotel in München-Freising stattfindet. Programm der RMA-Konferenz mit den Vortragsthemen und den Referenten finden Sie auf der nächsten Seite.

**Am Vorabend, Dienstag den 15.November 2022, ab 19.00 Uhr** dürfen wir Sie herzlich zu einem **gemeinsamen Abendessen** mit Networking einladen. Die **Gebühren für die Teilnahme** an der RMA-Konferenz Rating & Krisenmanagement betragen 75 € für Mitglieder und 125 € für Nichtmitglieder zuzgl. der gesetzl. Mehrwertsteuer.

Wir freuen uns auf einen regen Erfahrungs- und Informationsaustausch und Ihre zahlreichen Anmeldungen. In diesem Sinne verbleiben wir mit freundlichen Grüßen .

*Geschäftsführung / Vorstand*

| Zeitplan | Referenten | Vortragsthemen |
|---|---|---|
| 10.00 - 10.15 Uhr | **Prof. Dr. Wolfgang Biegert,** Stellv. Vorsitzender des RMA-Vorstands | Begrüßung |
| 10.15 - 11.00 Uhr | **Dieter Pape,** Leiter RMA-Arbeitskreis „Rating & Risikomanagement“ | Sustainable Finance - Impulse anhand des Beispiels ESG Data Hub der Österreich. Kontrollbank AG (OeKB), Wien |
| 11.00 - 11.45 Uhr | **Prof. Dr. Thomas Schempf,** SRH Fernhochschule - The Mobile University | Die Integration von ESG-Kriterien in Ratingprozesse |
| 11.45 - 12.30 Uhr | **Thomas Weber,** Mitglied des Arbeitskreises „Rating & Risikomanagement“ / Weber Consulting | Die zukünftige Nachhaltigkeitsberichterstattung und ihre Auswirkungen auf das ESG-Rating |
| 12.30 - 13.45 Uhr | | Mittagspause / Essen |
| 13.45 - 14.30 Uhr | **Prof. Dr. Wolfgang Biegert,** Stellv. Vorsitzender des RMA-Vorstands | Management von ESG-Risiken - wie gelangen mittelständische Unternehmen zu guten Ratingbewertungen? |
| 14.30 - 15.15 Uhr | **Dr. Klaus Bockslaff,** Leiter des RMA-Arbeitskreises „Krisenmanagement“ / Verismo Consulting GmbH | „Es hat doch geklappt“ - Lehren aus den jüngsten Krisen und Bedeutung der ISO 22361 für die Fortentwicklung des Krisenmanagements |
| 15.15 - 15.30 Uhr | | Kaffeepause |
| 15.30 -16.15 Uhr | **Daniel Schlup,** Leiter des Krisenmanagements der Schweizer Bundesbahnen AG | Die Bedeutung der Qualität des Krisenmanagements für die Wertschätzung eines Unternehmens anhand des Beispiels der SBB (Arbeitstitel - Vorschlag Klaus Bockslaff) |
| 16.15 -16.30 Uhr | **Prof. Dr. Wolfgang Biegert / Dr. Klaus Bockslaff** | Zusammenfassung / Verabschiedung |