



# StaRUG fordert mehr als KonTraG vom Risikomanagement

## Mit „geeigneten Gegenmaßnahmen“ der Krisenprävention zu mehr Resilienz und Robustheit



**Prof. Dr. Werner Gleißner,**  
FutureValue Group AG (Vorstand),  
TU Dresden (BWL, insb. Risikomanagement)  
kontakt@FutureValue.de,  
www.FutureValue.de,  
www.werner-gleissner.de

### Liebe Leserinnen und Leser,

die jüngsten – und in Zukunft drohenden – Krisen haben dazu geführt, dass das Ziel der Verbesserung von Resilienz und Robustheit der Unternehmen stärker als bisher deren Strategieentwicklung prägt. Klar ist, dass hier die Früherkennung und präventive Bewältigung volkswirtschaftlicher und strategischer Risiken eine große Bedeutung hat. Das strategische Risikomanagement ist an der Schnittstelle zwischen strategischem Management und Risikomanagement verortet und befasst sich genau mit der Verbesserung der Robustheit der Unternehmen. Passend ist nun, dass seit 2021 durch § 1 StaRUG auch der Gesetzgeber vom Risikomanagement erwartet, bei einer erkannten Bedrohungslage „geeignete Gegenmaßnahmen“ zu initiieren – Transparenz über den Risikoumfang reicht nicht aus. Leider ist der gebotene Ausbau der Fähigkeiten im Umgang mit Risiken oft noch nicht begonnen worden.

Ursächlich dafür ist auch, dass die durch § 1 StaRUG für alle Kapitalgesellschaften erhöhten Anforderungen an das Krisen- und Risikofrüherkennungssystem in der Jahresabschlussprüfung und dem IDW Prüfungsstandard 340 nicht berücksichtigt werden.

Das KonTraG (§ 91 Abs. 2 AktG) verlangt nur ein Risikofrüherkennungssystem. Nun fordert der Gesetzgeber mit § 1 StaRUG, dass bei Bedarf „geeignete Gegenmaßnahmen“ zu initiieren sind (z. B. zur Risikobewältigung). Entscheidungen über solche Maßnahmen sind „unternehmerische Entscheidungen“ im Sinne § 93 AktG und entsprechend vorzubereiten.

Es ergibt sich aus den Anforderungen auch, dass ergänzend zur Risikoanalyse und Risikoaggregation ein Risikotragfähigkeitskonzept zu implementieren ist. Dieses misst durch geeignete Kennzahlen, wie speziell der „Gefährdungswahrscheinlichkeit“, den „Grad der Bestandsgefährdung“. Das Überwachungsgremium hat festzulegen, ab welchem Grad der Bestandsgefährdung die im Gesetz gebotenen „geeigneten Gegenmaßnahmen“ und die Informationen des Überwachungsgremiums selbst erfolgen sollen. Mit dem § 1 StaRUG wird somit nun auch das Überwachungsgremium, z. B. der Aufsichtsrat, explizit gefordert.

Auch der Hinweis auf die Notwendigkeit der „fortlaufenden“ Überwachung in § 1 StaRUG findet sich so im älteren KonTraG nicht.

Zwischenfazit: Eine Prüfung des Risikomanagements nach IDW PS 340 greift deutlich zu kurz. Eine „bestandene“ Prüfung durch den Abschlussprüfer sagt keinesfalls, dass alle gesetzlichen Anforderungen an das

Risikomanagement erfüllt sind. Bedauerlicherweise berücksichtigen auch viele Unternehmen die Anforderungen aus § 1 StaRUG nur unzureichend.

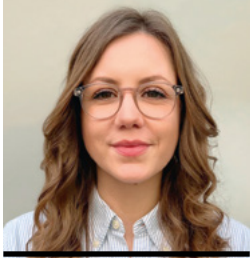
Dies ist nicht nur potenziell ein Haftungsrisiko für die Geschäftsleitung, sondern auch eine Beeinträchtigung der Zukunftsfähigkeit und der Überlebenswahrscheinlichkeit des Unternehmens. Wissenschaftliche Studien zeigen klar, was für die Zukunftsfähigkeit wichtig ist und wie man sie konkret messen kann.

Hohe Zukunftsfähigkeit bedeutet, dass das Unternehmen als ein „robustes Unternehmen“ angesehen werden kann (und einen hohen „QScore“ als Maß der Zukunftsfähigkeit aufweist). Ein solches robustes Unternehmen ist charakterisiert durch finanzielle Nachhaltigkeit, eine robuste Strategie mit resilienter Leistungserstellung und gute Fähigkeiten im Umgang mit Unsicherheit. Und genau diese Fähigkeiten sollen durch ein leistungsfähiges Risikomanagement erreicht werden. Notwendig ist es, neue Risiken rechtzeitig zu erkennen, um darauf reagieren zu können, und bei anstehenden unternehmerischen Entscheidungen die mit diesen verbundenen Risiken zu berücksichtigen (z. B. bei Investitionsentscheidungen).

Fazit: Ein robustes Unternehmen setzt ein leistungsfähiges Risikomanagement voraus. Die neuen gesetzlichen Mindestanforderungen durch § 1 StaRUG bieten einen zusätzlichen Anlass, sich mit dem Ausbau des Risikomanagements zu beschäftigen. ■

*Ihr Prof. Dr. Werner Gleißner*

## Inside RMA



Theresa  
Gutmann

Wir haben zu Beginn des Jahres 2023 einige organisatorische Änderungen in unserem Backoffice der RMA vorgenommen: Seit dem 1.1.2023 unterstützt uns Theresa Gutmann als Office Managerin und Assistenz von Vorstand und Geschäftsführung bei der RMA. Theresa Gutmann absolvierte eine Ausbildung zur Verwaltungsfachangestellten bei der Senatsverwaltung für Inneres und Sport Berlin. Im Anschluss arbeitete sie als Sachbearbeiterin beim Landesamt für Bürger- und Ordnungsangelegenheiten in Berlin. Seit Januar 2023 ist sie nun also bei der RMA – hier ist sie unter anderem für die Mitgliederbetreuung, das Rechnungswesen sowie die Veranstaltungsorganisation verantwortlich.

Noch mehr in unsere RMA-Tätigkeiten eingebunden ist seit Jahresbeginn auch Simone Meister. Bereits seit Januar 2021 ist sie Assistentin der Geschäftsführung der RMA Rating & Risk Academy GmbH. Neben den damit verbundenen Tätigkeiten rund um die Betreuung von Semi-

naren und Webinaren ist sie für die RMA vorwiegend in folgenden Bereichen tätig: Organisation unseres RMC und weiterer Konferenzen, Ansprechpartnerin für das Controller Magazin und für die RMA-Schriftenreihe sowie für die Pflege der RMA-Webseite. Theresa Gutmann und Simone Meister freuen sich auf den Kontakt mit Ihnen und möchten durch ihre Arbeit einen Mehrwert für die RMA schaffen!

Apropos Kontakt: Wir haben ein neues RMA-LinkedIn-Profil. Wenn Sie also keine Neuerungen mehr verpassen und immer auf dem Laufenden sein möchten, vernetzen Sie sich am besten gleich mit uns auf LinkedIn: RMA Risk Management & Rating Association e.V. – und treten Sie am besten auch gleich unserer gleichlautenden RMA-LinkedIn-Gruppe bei. Da Xing die Gruppenfunktion auslaufen lässt, möchten wir News und Interessantes künftig mit Ihnen auf LinkedIn teilen und diskutieren. Wir freuen uns auf den Austausch mit Ihnen! ■



Simone  
Meister

# Arbeitskreis „Human Risk Factors“ – Arbeitskräftemangel ein Personalrisiko?

Mittlerweile spricht man in der Wirtschaft nicht mehr von Fachkräftemangel, sondern von einem generellen Arbeitskräftemangel. Die Zahl der offenen Stellen steigt, wohingegen die Arbeitslosigkeit stetig sinkt. Die Gründe dafür sind vielfältig: Aufgrund des demografischen Wandels gehen mehr geburtenstarke Jahrgänge der Babyboomer jetzt in Rente, als junge Menschen in den Arbeitsmarkt eintreten. Durch die Digitalisierung entstehen neue Arbeitsplätze, wofür neue Kompetenzen und Fähigkeiten benötigt werden, die in der Ausbildung noch zu wenig angeboten werden. Die Branchen sind unterschiedlich betroffen: So konnten beispielsweise weite Teile des Dienstleistungssektors die pandemiebedingten Abwanderungen von Arbeitskräften noch immer nicht kompensieren und gesellschaftliche Herausforderungen wie der Kampf gegen den Klimawandel bescheren vielen Gewerbetreibenden einen konjunkturellen Aufschwung.

Neben diesen gesamtgesellschaftlichen Veränderungen ist jedoch auch bei den Mitar-

beitenden ein tiefgreifender Einstellungswandel zu beobachten: Die Pandemie hat die digitalisierte Kommunikation und das flexible Arbeiten im Homeoffice vorangetrieben, wodurch das Gefühl der Zugehörigkeit und die Bindung zum Unternehmen bei manchen geschwächt wurde. Die Lebensmodelle der Generation Y und Z führen zu einer Neubewertung der Arbeit, wo Sinn, Anerkennung, Selbstbestimmung und flexible Arbeitszeiten wichtige Faktoren sind und auch entsprechend eingefordert werden.

Die oben genannten Faktoren sind jedoch nur einige der oberflächlich erkennbaren Symptome des Arbeitskräftemangels. Die eigentlichen Gründe liegen viel tiefer und sind differenzierter zu betrachten, um wirkungsvolle Maßnahmen zu finden und um das Problem in den Griff zu bekommen.

Mitarbeitende sind die wichtigste Ressource für Innovationen, für den technologischen Fortschritt, für eine Nachhaltigkeitsstrategie und schließlich für den Unternehmenserfolg. Risiken im HR-Bereich entfalten einen gra-

vierenden und unmittelbaren Einfluss auf diesen Erfolg und können letztlich den Fortbestand des Unternehmens gefährden.

Vor diesem Hintergrund hat der Arbeitskreis Human Risk Factors das Thema „Personalrisiko“ abermals aufgegriffen. Bernhard Kessler von der kd Unternehmensberatung zeigte auf, dass viele Personalabteilungen vorwiegend mit operativen Tätigkeiten beschäftigt sind. Nach wie vor zählt es zu deren Hauptaufgaben, „... die richtigen Mitarbeiter, zum richtigen Zeitpunkt, mit den richtigen Qualifikationen, am richtigen Ort zu haben“. Kessler machte deutlich, dass es aber einer viel engeren Zusammenarbeit mit dem Risikomanagement bedarf, um die potenziellen Personalrisiken zu erkennen und wirksam zu steuern. Der Umgang mit Unsicherheiten, das Erkennen von Frühindikatoren und die Entwicklung unterschiedlicher Szenarien gehören ebenso dazu, um bessere Entscheidungsgrundlagen für das Management auszuarbeiten. Erst durch die Verschränkung des Fach- und Prozesswissens von Human Resources mit den Perspektiven



## RMA Top-Events

**17. Mai 2023:** Seminar: „Aktuelle Einschätzungen zur makroökonomischen Risikolage“

**24. Mai 2023:** Seminar: „Simulationsbasierte, risikogerechte Bewertung mit Excel: Teil I Grundlagen“

**13./14. Juni 2023:** Seminar: „Krisenmanagement für Führungskräfte“

**15. Juni 2023:** AK „Human Risk Factors“ (online)

**16. Juni 2023:** AK „Information Risk Management“ (online)

**21. Juni 2023:** Seminar: „Simulationsbasierte, risikogerechte Bewertung mit Excel: Teil II Aufbaukurs A“

**18. Juli 2023:** Seminar: „Volkswirtschaftliche Krisen- Quelle möglicher bestandsgefährdender Entwicklungen“

**19. Juli 2023:** Seminar: „Simulationsbasierte, risikogerechte Bewertung mit Excel: Teil III Aufbaukurs B“

des Risikomanagements kann Transparenz geschaffen werden. Hierzu gehören die Identifikation, das Erkennen der Ursachen und Wechselwirkungen von Personalrisiken, sowie die Einschätzung von Schadenshöhe und Wahrscheinlichkeit. Gerade im Bereich der Risikoquantifizierung der oftmals „weichen“ Risiken im HR-Bereich gibt es große methodische und praktische Herausforderungen bei der Verwendung gängiger Instrumente der Risikobewertung (wie etwa der Monte-Carlo-Simulation).

Die Teilnehmer waren sich aber einig, dass das Topmanagement die Vorgehensweise unterstützen und mittragen muss. Die engagierte Diskussion im Anschluss an den Beitrag ließ naturgemäß noch einige Fragen offen – aus diesem Grund werden im Rahmen des nächsten Arbeitskreis-Meetings die bisher erlangten Erkenntnisse zusammengefasst und zur Diskussion gestellt.

Das nächste Treffen des Arbeitskreises „Human Risk Factors“ findet am 15. Juni 2023 online von 9.00 bis 11 Uhr statt. Anmeldungen richten Sie bitte an [brigitta.john@rma-ev.org](mailto:brigitta.john@rma-ev.org). ■

## Risikomanagement bei HEIDELBERG

Die Risikoaggregation kann heute sicherlich als eine Schlüsseltechnologie im Risikomanagement bezeichnet werden. Ohne eine Aggregation der Risiken mit Bezug auf die Unternehmensplanung lässt sich der Gesamtrisikoumfang nicht bestimmen und eine Beurteilung des Grads der Bestandsgefährdung eines Unternehmens unter Beachtung von Kombinationseffekten von Risiken ist so nicht möglich (zur Methodik siehe Gleißner, Grundlagen des Risikomanagements, 2022).

Herr Reichert von der Heidelberger Druckmaschinen AG (HEIDELBERG) beantwortet in diesem Interview einige Fragen zur Risikoaggregation in seinem Unternehmen, die von Ralf Huber, Vorstand der RMA Risk Management & Rating Association e.V., gestellt werden.

**Huber:** Was waren die größten Herausforderungen im Bereich Risikomanagement seitdem Sie verantwortlich sind?

**Reichert:** Gerade nach Wirecard sind im Dezember 2021 die Anforderungen aus FISG und StaRUG vom Gesetzgeber relativ kurzfristig Ende Dezember 2021 erlassen und nahezu in Kraft gesetzt worden. Wie aus unseren Geschäftsberichten ersichtlich, haben wir bei HEIDELBERG daraufhin entsprechende Maßnahmen ergriffen, vor allem die Umstellung von quantitativen und qualitativen Risikobeschreibungen hin zu rein quantitativen. Es galt sämtliche vorhandene Risk Records des Risikoinventars zu überprüfen und die qualitativ beschriebenen Risiken

in rein quantitative zu transformieren. Da die Dokumentation dazu einen recht hohen Verwaltungsaufwand nach sich zog, favorisierten wir eine IT-gestützte GRC-Lösung, die uns nun digitalisierte Prozesse ermöglicht. Auch dieses Projekt ist erfolgreich abgeschlossen und unterstützt uns, ein angemessenes und wirksames Risk-Management-System (RMS) zu haben. Aus meiner Sicht ist gerade die Nachvollziehbarkeit von Chancen und Risiken und deren Entwicklung im Zeitablauf, insbesondere aus Dokumentationsgesichtspunkten, von wesentlicher Bedeutung.

**Huber:** Bei der Heidelberger Druckmaschinen AG aggregieren Sie die Risiken mittels Monte-Carlo-Simulation. Grundlage ist dabei die Unternehmensplanung. Wer in Ihrem Unternehmen ist für die Risikoaggregation verantwortlich und wer erhält die Ergebnisse der Risikoaggregation?

**Reichert:** Der deutsche Gesetzgeber fordert ein, dass der Vorstand als Organ im Rahmen des Aktiengesetzes verantwortlich ist, ein angemessenes und wirksames IKS und RMS zu betreiben. Dies ist von unserem Vorstand so entsprechend vollumfänglich umgesetzt. Gemäß unserem Business Mandat für das RMS hat der Vorstand die operative Umsetzung an uns delegiert. Das Controlling bei HEIDELBERG ist für die mehrjährige Unternehmensplanung operativ zuständig. Diese mehrjährige Unternehmensplanung ist das Fundament für das Modell der Monte-Carlo Simulation. Im letzten Jahr haben wir die



Ralf  
Huber

Mitglied des Vorstands der  
RMA Risk Management &  
Rating Association e.V.

Workflows unseres Risikomanagements durch die Einführung der SAP GRC Software digitalisiert und haben nun eine revisionssichere Datenbasis – jederzeit in Echtzeit verfügbar – für die Risikoaggregation. Wir als RMS-Team nehmen die Mehrjahresplanung als Fundament, geben die Chancen und Risiken, die in aller Regel als 3-Punkt-Schätzung vorliegen dazu und legen fest, ob die Planungs- und/oder Ereignisrisiken sich auf EBIT, Liquidität etc. auswirken. Als Ergebnis errechnen wir neben den reinen Planwerten über drei Planjahre (gemäß der GoP 3.0) auch Simulationen zu EBIT, Eigenkapital und Liquidität. Dazu wird auch ein simuliertes, synthetisches Rating berechnet.

**Huber:** Wie viele Risiken werden in Ihrem Unternehmen bei der Risikoaggregation berücksichtigt und wie werden diese quantitativ beschrieben?

**Reichert:** Hier möchte ich auf unseren Geschäftsbericht verweisen, in dem wir über alle hohen Risiken ausführlich berichten. Die reine Anzahl der Risk Records ist an dieser Stelle aus meiner Sicht wenig aussagekräftig, da wir sie auch in Gruppen zusammenfassen und nur das Ergebnis des Erwartungswertes dieser Gruppen in die Simulation eingehen lassen. Ein Beispiel aus der Praxis ist unser Informationssicherheitsmanagementsystem (ISMS), bei dem sehr viele Kleinst Risiken in der Betrachtung sind, die teilweise auch unterhalb unserer Aufnahmegrenze ansonsten liegen würden. Hinsichtlich der quantitativen Risikobeschreibung versuchen wir stets, keine Punktschätzungen mehr allein zu verwenden. Dies liegt daran, dass Punktschätzungen in aller Regel sehr schwer vorzunehmen sind. Einfacher ist es, wenn man den Best Case und den Worst Case als Ausgangsbeschreibung für die Bruttowerte verwendet und dann einen „most likely“ Case jeweils daraus ableitet und die Maßnahmen entsprechend abzieht – also Nettobetrachtung. Wir bei HEIDELBERG speichern alles in der GRC-Software, auch die Einschätzungen für die jeweiligen 3 Jahre und aktualisieren diese entsprechend, wenn sich neue Erkenntnisse auftun. Gleiches gilt auch für Gegenmaßnahmen, um schlussendlich das Nettorisiko zu bestimmen.

**Huber:** In einer Reihe wissenschaftlicher Stellungnahmen wurde immer wieder darauf hingewiesen, dass es keine geeignete Alternative zur von Ihnen genutzten Monte-Carlo-Simulation für die Risikoaggregation gibt. Haben Sie z. B. von Kollegen in anderen Unternehmen von einer alternativen Methode gehört oder wurde bei Ihnen darüber nachgedacht ein anderes Verfahren für die Risikoaggregation zu nutzen?

**Reichert:** Ein simples Addieren von Risiken ist sicherlich nicht zielführend, auch eine mögliche händische Konsolidierung, wie in der Rechnungslegung, stößt hier an ihre Grenzen. Sicherlich sind manche Risikoszenarien anfangs schwer quantifizierbar, wie beispielweise die Risiken der IT. Diese rein qualitativ bzw. nominal zu beschreiben, ist anfangs sicherlich noch mit geringem Aufwand machbar. Aber aus der Statistik wissen wir, dass mit rein nominal skalierten Merkmalsausprägungen noch nicht einmal eine natürliche Rangfolge beschrieben werden kann. Demzufolge müssten wir mindestens ein Risikoszenario so beschreiben, dass es ordinal beschrieben ist. Hier könnten wir zumindest schon einmal die diversen Risikoszenarien untereinander in eine Reihenfolge bringen. Aber damit wäre maximal ein simples Sortieren möglich – wie sollte aber so eine Ratingberechnung nur an-

satzweise möglich sein? Bleibt also nur ein metrisch/kardinal beschriebenes Risikoszenario übrig. Mit diesem kann man eine Reihenfolge beschreiben und auch Abstände untereinander berechnen. Die Antwort an dieser Stelle ist demzufolge, dass lediglich Risikoszenarien, die kardinal beschrieben sind, vorhanden sein müssen. Im Simulationsmodell wäre dann noch festzulegen, welche n Risiken sich wie zu den verbleibenden n-1 Risiken verhalten – also welche Korrelation sie untereinander haben. Wir haben bei HEIDELBERG hier bis dato in unserem Modell solche Risiken untereinander korreliert, die offensichtlich positiv (+1) oder negativ (-1) zueinanderstehen.

**Huber:** Mit der Risikoaggregation soll insbesondere der Grad der Bestandsgefährdung, also die Wahrscheinlichkeit einer „bestandsgefährdenden Entwicklung“ im Sinne § 1 StaRUG, abgeleitet werden, um bei Bedarf rechtzeitig die im Gesetz geforderten „geeigneten Gegenmaßnahmen“ zu initiieren. Wie werden in Ihrem Unternehmen die Ergebnisse der Simulation weiterverwendet?

**Reichert:** Unser Simulationsmodell basiert auf der Mittelfristplanung und wir betrachten stets die kommenden drei Jahre. Wir berechnen auf Basis der Chancen und Risiken tatsächlich für jedes der drei Jahre ein synthetisches Rating, und natürlich gehen die Ergebnisse des ersten Jahres auch als Startpunkt in das jeweils folgende Jahr ein. Planungs- und/oder Ereignisrisiken können sich unterschiedlich auswirken. Demzufolge berechnen wir stets auch Sensitivitäten auf unsere Covenants und können hier auch sehr gut beschreiben, wie hoch mögliche „Headrooms“ sein werden. Des Weiteren haben wir auch Schwellwerte festgelegt, ab denen auch formal Organe im Unternehmen zu informieren sind. Dies war u.a. eine Konsequenz aus der FISG und StaRUG Gesetzgebung – allerdings verrate ich an dieser Stelle kein Geheimnis, dass HEIDELBERG auch bereits vorher schon solche Szenarien betrachtet hat.

**Huber:** Ist bei Ihnen im Unternehmen in Abstimmung von Vorstand und Aufsichtsrat festgelegt worden, ab welcher Wahrscheinlichkeit einer „bestandsgefährdenden Entwicklung“, der Gefährdungswahrscheinlichkeit, die in § 1 StaRUG genannten „geeigneten Gegenmaßnahmen“ initiiert werden und der Aufsichtsrat informiert werden muss?

**Reichert:** Diese Frage ist relativ einfach und kurz mit einem klaren JA zu beantworten.

**Huber:** Wird die Risikoaggregation auch genutzt, um vor einer bedeutenden „unternehmerischen Entscheidung“ im Sinne von § 93 AktG aufzuzeigen, wie sich durch diese der Gesamtrisikoumfang des Unternehmens verändern würde?

**Reichert:** Als ich seinerzeit zu HEIDELBERG gekommen bin, habe ich allen Mitgliedern des Aufsichtsrates, des Vorstands und auch Bereichsleitern den Leitfaden des ICV „Entscheidungsvorlagen für die Unternehmensführung – Leitfaden für die Vorbereitung unternehmerischer Entscheidungen (Business Judgement Rule)“ gegeben. Das Thema ist also unternehmensweit adressiert. Daraus abgeleitet erstellen wir bei großen Entscheidungen, bei denen der Vorstand als Organ und nicht als Fachvorgesetzter strategisch entscheidet, eine entsprechende Entscheidungsvorlage.

**Huber:** Herr Reichert, was planen Sie bei HEIDELBERG in der Zukunft?

**Reichert:** Wir haben viel über das Risikomanagement gesprochen. Um verlässliche Zahlenwerke als Basis für die Risikoaggregation etc. zu bekommen, ist ein angemessenes und wirksames Internes Kontrollsystem unabdingbar. Dabei reicht es aus meiner Sicht nicht aus, nur oder ausschließlich sich auf die Rechnungslegung zu fokussieren. Auch wird es erforderlich sein, Prozesse digital zu designen und in Realtime hinsichtlich der Wirksamkeit zu überwachen. Dazu werden wir zukünftig continuous control monitoring (CCM) nicht nur im IT-General Control Bereich anwenden, sondern aus Effizienzgründen auch die implementierten Applikationskontrollen systembasiert überwachen.



**Volker B. Reichert, Head of Internal Audit und Head of Risk Management**

Volker B. Reichert verantwortet bei der Heidelberger Druckmaschinen AG den Bereich der Internen Revision als auch die des weltweiten Risikomanagements & Internen Kontrollsystems. In diesen Funktionen hat er einerseits Berichtslinien zum Vorstand und berichtet andererseits regelmäßig auch sowohl im Prüfungsausschuss des Aufsichtsrates als auch im Aufsichtsrat.

Er hat Betriebswirtschaft an der Universität Paderborn als auch im Rahmen eines Stipendiums an der Universität Louis Pasteur Strasbourg studiert. Nach dem Abschluss als Diplom Kaufmann startete er seine berufliche Karriere bei einer Big4 Gesellschaft – maßgeblich Ernst & Young bevor er anschließend in die Industrie wechselte und dort stets in verantwortlichen Funktionen der 2. und 3. Verteidigungslinie bei börsennotierten Gesellschaften tätig war. Das Thema Risikomanagement begleitet ihn seit seinem Berufsstart im Jahr 2005. ■

Get Ready to Manage Risks!






**Qualifizieren Sie sich zum »Enterprise Risk Manager (Univ.)«**  
Am **13. September 2023** Start des Weiterbildungsprogramms der RMA und der Universität Würzburg

- Sie möchten sich im Bereich Risikomanagement weiterentwickeln?
- Sie suchen Kontakte zu Fachexperten und Praktikern?
- Sie möchten Ihr theoretisches Know-how mit Benchmark-Erfahrungen aus der Praxis verknüpfen?
- Sie suchen eine wissenschaftlich fundierte Weiterbildung mit einem Überblick zum State of the Art im Risikomanagement?

**10-tägiger Risikomanagementkurs von Experten in Theorie und Praxis**

Mehr Infos und Anmeldung unter:  
[rma-ev.org/erm](http://rma-ev.org/erm) [fzrm.de/erm](http://fzrm.de/erm)

**RMA Marketplace**



**Sie suchen ...**

**Sie bieten ...**

**Dienstleistungen & Softwarelösungen zu den Themen Risiko-, Compliance-, Versicherungsmanagement & Rating**

**Wir bringen Sie zusammen:  
[www.rma-ev.org/marketplace](http://www.rma-ev.org/marketplace)**

**Buchtipps**



**Resilienz und ganzheitliches Krisenmanagement (Band 8)**  
**Jahrbuch Risikomanagement 2022/23**

Unter den Bedingungen massiver Krisenlagen und ihrer vielfältigen Folgen für Umwelt, Wirtschaft und Gesellschaft muss sich das installierte Risikomanagementsystem in vielen Unternehmen derzeit neu bewähren. Der neue Band der **RMA Risk Management & Rating Association e.V.** nimmt die aktuell besonders relevanten Fragestellungen und mögliche Lösungsansätze praxisorientiert in den Blick.



104 Seiten, kartoniert,  
ISBN: 978-3-503-21206-4



## Treffen Region West

Anfang März gab es einen „Neustart“ der regionalen Aktivitäten der RMA Risk Management & Rating Association in der Region West. Der erste Stammtisch 2023 fand in den Räumen der Ernst & Young GmbH in Düsseldorf statt und war ein voller Erfolg.

Es kamen eine Reihe von Risiko-, Compliance- und Internal Audit-Experten aus der Region zusammen und diskutierten die neuesten Trends und Entwicklungen im Bereich des Supply Chain Risk Management und Resilienz sowie der hierzu relevanten regulatorischen Entwicklungen im Bereich Nachhaltigkeit und ESG (Environmental Social and Governance).

Nach der Begrüßung durch Ralf Kimpel, Vorstandsvorsitzender der RMA, übernahm die regionale Ansprechpartnerin der RMA, Ines Janßen, Senior Managerin EY, die Moderation und führte souverän mit ihren Experten von EY durch die Workshops.

### Workshop I

Geopolitische Instabilität, Naturkatastrophen, Cyber Risiken und viele weitere Ausgangsfaktoren können zu Ausfällen in der Lieferkette führen und u.a. mit erheblichen Kosten, Qualitätseinbußen und Imageschäden verbunden sein. Ein effektives Supply Chain Risk Management schützt die E2E Supply Chain, macht sie widerstandsfähiger (resilient) und schafft einen Wettbewerbsvorteil durch die frühzeitige und kontinuierliche Identifikation von Risiken und Chancen. Insbesondere durch ein integriertes und datengestütztes Risikomanagement können Trends frühzeitig identifiziert und systematisch entgegengesteuert werden. Hierbei spielt die Zusammenarbeit der Supply Chain Stakeholder eine wesentliche Rolle.

Es wurden Supply Chain Risiken und Maßnahmen in den Prozessen Plan, Source, Make und Deliver/Return besprochen sowie die wesentlichen Faktoren für eine effektive Umsetzung und Stärkung des Supply Chain Risk Management, um frühzeitig Störungen in der Lieferkette zu antizipieren und minimieren. Erste Erfahrungen zum Reifegrad des Supply Chain Risikomanagements wurden ausgetauscht. Generell hat sich in den letzten Jahren einiges getan und eine Integration der Supply Chain Silos ist sichtlich vorangeschritten. Jedoch ist die gewünschte Transparenz in der Lieferkette und die Nutzung von Daten zur besseren Vorhersehbarkeit von Risiken noch in großen Teilen ausbaubar. Als eine der wesentlichen Herausforderungen wurde die teilweise noch unklare Verantwortung für Supply Chain Risk Management genannt. Das Risikomanagement agiert oft als Unterstützer des Prozesses und methodischer Vermittler, jedoch liegt die Verantwortung in den einzelnen Bereichen. Ziel sollte es sein, klare Supply Chain Risk Management Governance Strukturen und Prozesse zu schaffen, die durch die richtige Technology unterstützt werden, um so frühzeitig Risiken antizipieren und steuern zu können und einen Wettbewerbsvorteil zu generieren.

### Workshop II

Als weiterer Aspekt wurden die regulatorischen Anforderungen an die Lieferketten bezüglich Nachhaltigkeit diskutiert. Neben einem kurzen Überblick stand das Lieferkettensorgfaltspflichtgesetz (LkSG) sowie die kommende europäische Corporate Sustainability Due Diligence Directive (CSDDD) im Fokus. Anforderungen betreffen hier das gesamte Governance-Modell, die Risikoanalyse, das Risikomanagement, die Beschwerdeverfahren und die Berichterstattung. Für Unternehmen mit über 3.000 Mitarbeitern ist das LkSG bereits seit dem 01.01.2023 umgesetzt.

Erste Erfahrungen zum Umsetzungsstand gerade in Bezug auf die Risikoanalyse im eigenen Geschäftsbereich und in der Lieferkette wurden ausgetauscht. Klare Herausforderungen liegen in der teilweise vorliegenden organisatorischen Komplexität (u.a. hohe Anzahl an Stakeholdern und Gesellschaften) und Fragestellungen im Rahmen der Integration der Anforderungen in bestehende Prozesse und die IT-Landschaft. Es wurde aber auch klar betont, dass die Einbindung der relevanten Stakeholder gerade von Beginn an für den jetzigen Umsetzungsstand ein zentraler Erfolgsfaktor ist. Die Kooperation zwischen Einkauf, Risikomanagement, Compliance und der Nachhaltigkeitsabteilung ist für den Umsetzungsfortschritt essenziell.

Insgesamt war die erste Veranstaltung des RMA West ein großer Erfolg und bot wertvolle Einblicke und Diskussionen für alle Teilnehmer. Wir freuen uns auf die Fortsetzung. ■



## 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