Risk Management Congress 2017 – eine Nachlese

(Bildquelle: RMA)

Vom großen Bild im Risikomanagement

„Wie umgehen mit Veränderung?“ fragt das Germanische Nationalmuseum in Nürnberg im Rahmen einer aktuellen Ausstellung zu „Luther, Kolumbus und die Folgen“. Nur einen Steinwurf vom Germanischen Nationalmuseum entfernt, tagten am 16. und 17. Oktober 2017 die Risikomanager anlässlich des Risk Management Congress im Le Méridien Grand Hotel. Auch eine ihrer Kernfragen drehte sich darum, wie mit Veränderung umzugehen ist – in einer Welt voller Unsicherheiten und einem gewaltigen Wandlungsdruck für Wirtschaft, Wissenschaft und Politik.

Cyberrisiken, politische Gefahren sowie sich verändernde Gesetze, Normen und Standards im Risikomanagementumfeld setzen Unternehmen vermehrt unter Druck. Daraus resultiert die Suche nach Leitplanken für die Unternehmensführung. „Wir brauchen das große Bild und damit den Gesamtprozess im Risikomanagement“, erklärt Ralf Kimpel die Notwendigkeit zu transparenten Risikomanagementstrukturen und -prozessen.

Klares Fundament: Risiken und Prozesse kennen

Im Zuge des Risk Management Congress standen Best Practice, moderne Methoden und neue Impulse für ein modernes Risikomanagement im Mittelpunkt der zweitägigen Veranstaltung. Und doch fängt alles mit einem klaren Fundament an, das da heißt: „Wenn du deine Risiken und Prozesse kennst, wirst du in keine bestandsgefährdende Situation geraten“, so Ralf A. Huber, Senior Vice President und Chief Risk Officer beim Unternehmen Leoni. In seinem Vortrag zu „Risk & Internal Control – Die Kunst der Transparenz“ zeigte Huber an den Beispielen der Konjunkturentwicklung, dem Lieferkettenausfall in Richtung Kunde sowie dem Anlauf- und Projektkostenentwicklung und dem Thema Compliance, wo Risiken und Chancen bestehen. Während die Entwicklung der Konjunktur sowohl mit einem hohen Risiko als auch einer hohen Chance bewertet werden, wird ein Ausfall der Lieferkette als hohes Risiko (Top 1) bei Leoni identifiziert.

Letzteres war während des Arabischen Frühlings von 2011 in Tunesien und Ägypten eine Herausforderung für das Unternehmen. Aber auch die Krim-Krise oder der Terror durch den Islamischen Staat sind hohe Risikofaktoren im Supply-Chain-Umfeld. Nicht zu vergessen der sogenannte „Fake-President-Angriff“ auf Leoni, bei dem Betrüger rund 40 Millionen Euro erbeuteten. In Folge des Vorfalls wurde mithilfe des Social Engineering und der Vortäuschung einer falschen Identität Druck auf Leoni-Mitarbeiter aufgebaut und so Geldtransfers auf chinesische Konten erwirkt.

Wichtige Schritte sieht Risikomanager Huber vor allem darin, Transparenz und die notwenige Dokumentation in der Organisation zu schaffen. Entscheidend sei seiner Meinung nach unter anderem die Einbindung der Themen in die Managemententscheidungen, der Ausbau des internen Kontrollsystems sowie Schulungen, um das Wissen im Risikomanagement auszubauen.

Ralf A. Huber von Leoni und die Kunst der Transparenz. (Bildquelle: RMA)

Von der Risikoblindheit sowie verpassten Schiffen

Apropos Schulung und Wissen. Für Prof. Werner Gleißner, Vorstand der Future Value Group und Mitglied im Beirat der RMA, fehlt es im Risikomanagement vielfach an Kompetenzen. Gleißner beschreibt es als Krankheit, deren Symptome eine weit verbreitete Risikoblindheit sei. Diese äußert sich unter anderem in einer verzerrten Risikowahrnehmung, mangelnde Zeit für Risikoanalysen sowie einer wenig ausgebildeten Risikoaggregation bestandsgefährdender Entwicklungen. Letzteres ist deshalb so kritisch, weil Unternehmen oft nicht wissen, was eine bestandsgefährdende Entwicklung ist. Stattdessen würde mithilfe von „Risk-Maps“ die Trivialisierung des Risikos erreicht. Gleißner nennt es „Malen nach Zahlen“ und fügt an, dass mit einer solchen Darstellung sowohl der Gesamtrisikoumfang unklar sei sowie der Erwartungswert mit Blick auf den Gesamtschaden kein geeignetes Risikomaß bedeute. Denn einen Mehrwert im Gesamtprozess lässt sich nur herstellen, wenn Risikoinformationen zu besseren Entscheidungen führen.

Spricht sich gegen die „Trivialisierung des Risikos“ aus: Prof. Werner Gleißner. (Bildquelle: RMA)

Dabei sind die Anforderungen vom Gesetzgeber klar formuliert. So schreibt beispielsweise §91 Abs. 2 Aktiengesetz vor: „Der Vorstand hat geeignet Maßnahmen zu treffen, insbesondere ein Managementsystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“ Trotzdem fehle es nach Gleißners Worten an der Umsetzung. Um die Risikoblindheit zu überwinden, empfiehlt der Experte Risikomanagement als Querschnittsfunktion in der eigenen Organisation zu etablieren und eine Risikoaggregation als „Schlüsseltechnologie“ zu verstehen. Zudem sollten bei einer nicht sicher vorhersehbaren Zukunft alle Mitarbeiter jedes Management auch als Risikomanagement verstehen.

Mit Blick auf die Unternehmensstrukturen und deren Entwicklungen in volatilen Zeiten steht für Anja Förster der Veränderungsprozess im Mittelpunkt. Es geht darum, bestehende Märkte optimal auszuschöpfen sowie neue Quellen für Wachstum und Gewinn zu erschließen. Wer letzteres verpasst, der verpasst im übertragenen Sinne das Schiff. Doch Vorsicht: „Das was Dir am besten gelingt, wird Dir zur Falle.“ Damit zitierte Förster den französischen Lyriker Paul Valery. Die dahinter stehende Herausforderung ist die Aufforderung Glaubenssätze zu hinterfragen und die Spielregeln zu ändern. Hierzu gehört beispielsweise der Mut, schlechte Ideen zu kreieren. Denn ein Unternehmen ohne Niederlagen sei tot. Um das zu verhindern, müssen Organisationen sich hinterfragen, wandeln und die eigene Zukunft gestalten.

Anja Förster fordert Unternehmer auf, ihre Glaubenssätze zu hinterfragen. (Bildquelle: RMA)

Datenschutz, Standards, Arbeitskreise

Mit der Zukunft in Sichtweite beschäftigte sich Dr. Manfred Stallinger, Geschäftsführender Gesellschafter der calpana business consulting. Hintergrund ist die neue EU-Datenschutzgrundverordnung (EU-DSGVO). In seinem Referat zu den „Auswirkungen der EU-DSGVO und dem IT-Sicherheitsgesetz im Enterprise Risk Management“ stellt Stallinger klar: „Bislang war das Thema Datenschutz ein ‚zahnloser Tiger‘. Mit der Europäischen Datenschutz Grundverordnung EU-DSGVO hat sich vieles verändert.“ Darauf müssen sich Unternehmen einstellen, erklärte Stallinger. Und auch Samuel Brandstätter von der avedos GRC nahm in seinem Vortrag die EU-DSGVO unter die Lupe. Neben den wesentlichen Neuerungen – wie das Recht auf Datenübertragung und des Vergessen werden sowie die Nachweispflicht – hob Brandstätter die Möglichkeit einer Zielarchitektur eines Datenschutz-Managementsystems hervor. Das Lösungsszenario zum Datenschutz determiniere sich dadurch, wer gefragt werde. Denn die Bandbreite der möglichen Adressaten sei groß – angefangen bei Auditoren über Rechtsanwälte und Wirtschaftsprüfer bis zu IT-Beratern, Behörden und Interessenvertretungen.

Im Grunde funktionieren Lösungen für ein besseres Risikomanagement nur mit einer Betrachtung der Gesamtorganisation und im Zusammenspiel mit den dahinter liegenden Prozessen. Leitplanken können in diesem Kontext Standards bieten. Dennis L. Chesley, Global Risk Consulting Leader bei der Wirtschaftsprüfungsgesellschaft PwC, zeigt am Beispiel des „COSO Updated ERM Framework – Integrating with Strategy and Performance“ wie wichtig ein durchgängiges Enterprise Risk Management für die Organisation ist. Die „DNA“ des COSO ERM Frameworks besteht aus fünf miteinander verzahnten Komponenten die da heißen: Governance & Culture, Strategy and Objective-Setting, Performance, Review and Revision und Information, Communication, and Reporting.

Dennis L. Chesley und die „DNA“ des COSO ERM Frameworks. (Bildquelle: RMA)

Und auch der Bericht aus dem RMA-Arbeitskreis „Interne Revision und Risikomanagement“ des RMA-Vorstandvorsitzenden Ralf Kimpel und Matthias Meyer, Leiter der Governance Academy, Volkswagen AG, unterstrichen die enge Verzahnung von Prozessschritten im Risikomanagement. Im Mittelpunkt ihrer Betrachtungen stand die Beurteilung des Risikomanagementsystems mithilfe eines Prüfungsleitfadens. In der praktischen Anwendung des Prüfleitfadens ist der Prozessablauf in sieben aufeinander aufbauenden Schritten gegliedert – von der Sichtung der Fragen und Grundsatzkriterien über die eigentliche Prüfung bis zur Qualitätssicherung und dem Prüfbericht. „Wirksam ist ein Risikomanagementsystem, wenn es so ausgestaltet und in der Organisation umgesetzt ist, dass die beschriebenen Risikomanagementphasen aufeinander aufbauend und ordnungsgemäß durchlaufen werden“, erklärt Meyer. Bei der Frage nach dem Verhältnis zum Standard IDW PS 981 stellten beide Referenten klar, dass sich die praktische Anwendung des Prüfleitfadens auf ein ganzheitliches Risikomanagement fokussiert, inklusive „Wie“ etwas zu prüfen sei und nicht nur „Was“.

Wichtig ist den Machern des Prüfleitfadens vor allem die praktische Hilfestellung in den Punkten der Durchführung sowie der Berichterstattung. Und auch an anderer Stelle zeigte sich, wie mithilfe klarer Prozesse ein wichtiger Schritt zu mehr Qualität erzielt werden konnte. Die Rede ist vom Informationssicherheits-Management (ISMS), das die „infra fürth“ als regionaler Energieversorger erfolgreich einführten. Hintergrund ist die verschärfte Gesetzeslage durch das IT-Sicherheitsgesetz, welches im Juli 2015 in Kraft trat. Die infra fürth setzt hierbei auf ein ISMS-Tool mit einer klaren Mandantenstruktur sowie durchgängigen Prozessen und Assets sowie deren Risikobewertung.

Dass am Ende vieles vom Menschen abhängt, zeigte Matthias Schmidt vom Bayerischen Landeskriminalamt in seinem Vortrag zu „Cyber Risk Management“. Denn Leichtsinn bricht sich bei den IT-Anwendern immer wieder Bahn. Seien es unzureichende Passwörter, ein zu laxer Umgang mit Sicherheitsvorkehrungen oder wenig sensibilisierte Mitarbeiter. Die Folgen sind zahllose Hackerangriffe mit enormen Schäden, die Unternehmen in massive Turbulenzen stürzen können oder gar in die Knie zwingen. In dieser Welt mit ihren technischen Möglichkeiten, einer umfassenden Digitalisierung und globalen Vernetzung, braucht es klare Leitplanken. Und damit wären wir wieder beim Einstieg des Beitrags.

Denn die knapp 200 Teilnehmer des Risk Management Congress 2017 erhielten im Rahmen der beiden Konferenztage das große Bild im Risikomanagement. Auch mithilfe der vielfältigen Vorträge, Inhalte und Impulse, einem ausgesprochenen Netzwerkgedanken und den Sponsoren, ohne die eine solche Veranstaltung nicht umsetzbar wäre. Wir danken antares, avedos, calpana business consulting, Deloitte, der Funk Stiftung, OpRiskSolutions, Palisade, Schleupen und WS InnoCon für ihr Engagement. Führen wir es fort – im Herbst 2018.

Der gesamte RMA-Vorstand freut sich auf das Wiedersehen beim Risk Management Congress 2018: Jan Offerhaus (Kassenwart), Prof. Dr. Christoph Mayer, Brigitta John, Dirk Schäfer, Marco Wolfrum (Stellvertretender Vorsitzender des Vorstands), Dr. Roland Spahr, Ralf Kimpel (Vorsitzender des Vorstands (von links). (Bildquelle: RMA)