Der neue DIIR Revisionsstandard Nr. 2 (2018)

Ein empfehlenswerter Standard für die Prüfung des Risikomanagements

Prof. Dr. Werner Gleißner

Liebe Leserinnen und Leser,

Ende November 2018 wurde der neue Prüfungsstandard für das Risikomanagement, der DIIR Revisionsstandard Nr. 2, veröffentlicht. Er wurde maßgeblich erarbeitet in einem gemeinsamen Arbeitskreis des Deutschen Instituts für Interne Revision mit der Risk Management Association e. V. (RMA).

Die Interne Revision hat Angemessenheit und Wirksamkeit der Maßnahmen und Kontrollen zur internen Risikosteuerung zu beurteilen. Hervorzuheben ist zunächst, dass der neue DIIR Nr. 2 nun erstmals zwei große Prüfungsfelder deutlich getrennt aufzeigt:

1. Die Prüfung von Organisation und Prozessen im Risikomanagement sowie

2. Die Prüfung der im Risikomanagement eingesetzten betriebswirtschaftlichen Methoden (z. B. zur Risikoquantifizierung und Risikoaggregation).

Exemplarisch können hier nur einige Inhalte des DIIR Nr. 2 besonders hervor gehoben werden:

- Risiko wird verstanden als Überbegriff zu möglichen positiven Abweichungen (Chancen) und möglichen negativen Abweichungen (Gefahren, Risiken im engeren Sinn).

- Mit Bezug auf die gesetzliche Anforderung aus §91 (2) AktG im Hinblick auf die Erkennung möglicher „bestandsgefährdender Entwicklungen“ wird die Methode zur Risikoaggregation zum zentralen Prüfungsfeld (weil nur so gewährleistet werden kann, dass auch mögliche bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken erfasst werden).

- Der DIIR Nr. 2 betont klar die Notwendigkeit der Quantifizierung von Risiken (ganz auf Linie des IDW PS 340) und empfiehlt die darauf aufbauende Messung der Risikotragfähigkeit.

- Von grundlegender Bedeutung ist es, dass bei der Prüfung des Risikomanagements auch schon die Implikationen aus §93 AktG im Hinblick auf ein „entscheidungsorientiertes Risikomanagement“ berücksichtigt werden. Entsprechend klar wird zu den Aufgaben des Risikomanagements bei der Vorbereitung „unternehmerisches Entscheidungen“ ausgeführt:

„Es gehört auch zu den Aufgaben des Risikomanagements sicherzustellen, dass schon bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang nachvollziehbar aufgezeigt werden, um zumindest eine mit solchen Entscheidungen möglicherweise einhergehende bestandsgefährdende Entwicklung früh zu erkennen. Neben bereits vorhandenen Risiken sind damit durch das Risikomanagement insbesondere auch geplante Maßnahmen und Entscheidungen zu betrachten, speziell im Hinblick auf durch diese möglicherweise verursachten zukünftigen Risiken.“

Fazit: Der neue Standard ist sehr gut gelungen und eine hervorragende Grundlage, um das eigene Risikomanagement – und zugleich die risikobezogenen Aspekte des Controllings – einmal kritisch zu hinterfragen. Man wird hier sicherlich aus einer Prüfung interessante Anstöße für die in den meisten Unternehmen nun sinnvolle Weiterentwicklung des Risikomanagements finden (auf dem Weg zum neuen Paradigma eines „entscheidungsorientierten Risikomanagements“). Oft wird man hier erkennen, dass gerade im Hinblick auf die

TOPEVENT

18. März 2019 – Treffen des Arbeitskreises „Interne Revision & Risikomanagement“ in München

22. März 2019 – Workshop des Arbeitskreises „Human Risk Factors“ in Bad Homburg

3. April 2019 – Start des nächsten Fortbildungsprogramms Enterprise Risk Manager (Univ.)

3. April 2019 – Münchener Risikomanager-Stammtisch

11. April 2019 – Mittelstandstag der Hochschule für Technik und Wirtschaft in Dresden

12. April 2019 – Treffen des Arbeitskreises „Integriertes Risikomanagement“ in Dresden

21./22. Oktober 2019 – Risk Management Congress in Berlin

Impressum

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

RMA-Geschäftsstelle
Risk Management Association e. V.
Zeppelinstr. 73, D-81669 München
Tel.: +49.(0)1801 – RMA TEL (762 835)
Fax: +49.(0)1801 – RMA FAX (762 329)
E-Mail: office@rma-ev.org
Web: www.rma-ev.org

Prof. Dr. Werner Gleißner
fachartikel@futurevalue.de,
Tel.: +49.(0)711-79735830

im Risikomanagement genutzten Methoden – deutlich mehr als bei Organisation und Prozessen – Verbesserungspotenziale besteht.

Die beiden Beiträge der RMA in dieser Ausgabe des Controller Magazins können hier möglicherweise schon nützliche Denkanstöße geben. In meinem Beitrag, „Risikoanalyse (I): Grundlagen der Risikoquantifizierung", werden wesentliche Grundlagen für die quantitative Beschreibung von Risiken erläutert (der zweite Teil des Textes in der nächsten Ausgabe des Controller Magazins enthält darauf aufbauend einen konkreten Leitfaden zur Verbesserung der Risikoquantifizierung). Der Text der Autoren Knoll und Trageser, „Risikomanagement und Controlling: Disziplinäre Symbiose auf Fachbuchebene", zeigt aus Perspektive des Schrifttums, wie weit die notwendige Verbindung der beiden Disziplinen fortgeschritten ist (bzw. welche Defizite noch bestehen).

Ich wünsche viel Spaß beim Lesen.
Prof. Dr. Werner Gleißner

Tradition verpflichtet

Der Arbeitskreis „Risikoquantifizierung" tagte wieder am Tag nach dem Risk Management Congress

Am 17. Oktober, am Tag nach dem Risk Management Congress 2018, tagte – ebenfalls in Köln – der Arbeitskreis „Risikoquantifizierung". Die Sitzung fand statt in den Räumlichkeiten der Frey Competence GmbH.

Erster Tagesordnungspunkt war die Diskussion des Umgangs mit Kapitalrisiken und Liquiditätsrisiken. Herr Dr. Daniel Röhrig von der Firma HELLA führte in das Thema ein, erläuterte das Vorgehen zur Risikoquantifizierung in der eigenen Unternehmenspraxis und stellte zur Diskussion, wie insbesondere damit umzugehen ist, wenn Risiken sich (ggf. sogar gegensätzlich) sowohl auf die Kapital- als auch die Liquiditätsposition eines Unternehmens auswirken. Herr Jan Offerhaus aus dem RMA-Vorstand erläuterte regulatorische Vorgaben sowie den praktischen Umgang mit Kapital- und Liquiditätsrisiken im Bankenbereich und zog Parallelen und Empfehlungen daraus für Nicht-Banken. An diese Vorträge schloss sich eine intensive Diskussion über diese Thematik unter allen Teilnehmern an mit dem Fazit, dass diese Thematik in zukünftigen Sitzungen noch weiter vertieft werden wird.

Als weiteren Tagesordnungspunkt gab es einen interessanten Praxisvortrag von Herrn Frank Spalthöfer von der Firma HARTING über die dortige Praxis des Risikomanagements und der Risikoquantifizierung. Auch hier schloss sich eine intensive Diskussion an, bei der insbesondere ein pragmatisches Vorgehen zur Weiterentwicklung von Risikomanagement-Systemen in der Unternehmenspraxis im Zentrum stand.

Zum Schluss der AK-Sitzung wurden Details des weiteren Vorgehens zur Erstellung der Guideline zur Risikoquantifizierung besprochen, die der AK im Rahmen der Buchreihe der RMA in 2019 fertigstellen wird. //

Bei Interesse an der Mitarbeit in diesem AK schicken Sie bitte eine Mail an ak-risikoquantifizierung@rma-ev.org.

Mehr Stahl als beim Eiffel-Turm und größere Tanklager als am Münchener Flughafen

Münchener Risk Manager-Stammtisch beeindruckt von einem der modernsten Rechenzentren Europas

Am 27. November trafen sich 20 Teilnehmer des Münchener RMA-Stammtischs im erst 2017 in Betrieb genommenen Rechenzentrum der noris network AG vor den Toren Münchens in Aschheim. Herr Gerrit Schröder, Information Security and Risk Officer bei noris network sowie RMA-Mitglied, hatte eingeladen.

Die Teilnehmer wurden von Herrn Schröder und einem Kollegen durch die Vereinzelungsschleusen hindurch in verschiedene Bereiche des Rechenzentrums geleitet und konnten die technischen Einrichtungen aus der Nähe betrachten. Besonderen Eindruck machten das Kyoto-Cooling-System mit seinen meterhohen Rädern zur Umwandlung von Warm- in Kaltluft, die Brandfrühesterkennung und -bekämpfung mittels Stickstoff-Inertisierung und anschließender zeitlich unbeschränkter Sauerstoffabsenkung sowie die riesigen Dieselgeneratoren für die Notstromversorgung, die in jedem Kreuzfahrtschiff Dienst tun könnten. Herr

Schröder und sein Kollege beantworteten die vielen Fragen der Teilnehmer zu Sicherheits- und Risikomanagement-Aspekten. Sie erläuterten u. a., dass im Rechenzentrum zwecks Flexibilisierung der Räumlichkeiten mehr Stahl verbaut wurde als im gesamten Eiffel-Turm und dass die Kraftstofftanklager für die Dieselgeneratoren größer dimensioniert sind als am Münchener Flughafen. In einer nahegelegenen bayerischen Wirtschaft wurde bei Bier und Essen sowie intensiven Diskussionen rund um Risikomanagement der Nachmittag/Abend gebührend abgeschlossen. Vielen Dank an Herrn Gerrit Schröder für das gelungene Event! //

Der nächste RMA-Stammtisch, dann wieder im üblichen Stammtischformat, findet am 3. April ab 19 Uhr statt. Sie sind herzlich zur Teilnahme eingeladen. Anmeldungen schicken Sie bitte an die RMA-Geschäftsstelle unter office@rma-ev.org.

Vom Fernrohr Napoleons bis zu disruptiven Technologien als strategisches Risiko

Gemeinsame Sitzung der Arbeitskreise „Integriertes Risikomanagement“ und „Risikomanagement-Standards“

Napoleon hatte zwar ein für damalige Verhältnisse leistungsstarkes Fernrohr, um die auf ihn zukommenden Risiken in der Schlacht von Waterloo frühzeitig abschätzen zu können, seine Niederlage bei Waterloo konnte er dennoch nicht verhindern. Nun befindet sich sein Fernrohr im Museum für Optik im Zeiss Forum in Oberkochen.

Im Zeiss Forum in Oberkochen trafen sich am 16. November auf Einladung von Dr. Andreas Kempf, Leiter Corporate Auditing, Risk and Quality Management bei der Carl Zeiss AG, Mitglieder der RMA-Arbeitskreise „Integriertes Risikomanagement“ und „Risikomanagement-Standards“ zu einer gemeinsamen Sitzung. Als Themen auf der Agenda standen Einblicke in die Praxis des Risikomanagements bei Carl Zeiss mit Fokus auf strategische Risiken sowie „Fluch und Segen“ von Risikomanagement-Standards und deren Bedeutung für andere Managementsystem-Standards. Abgerundet wurde die Sitzung mit einem Gang durch das Museum für Optik, in dem historische bis hochmoderne technische Exponate von Carl Zeiss, aber auch aus anderer Herkunft gezeigt wurden.

Ausgehend von einer Vorstellung des Unternehmens Carl Zeiss AG mit seinem Anspruch auf Technologie-Führerschaft in einem heterogenen und komplexen Umfeld, stellte Dr. Kempf zunächst die Organisation und den Prozess des Risikomanagements im Unternehmen vor. Besonders hervorgehoben wurde die herausgehobene Rolle der Risikoidentifikation. Dr. Kempf erläuterte, dass bei der Carl Zeiss AG das Konzept des „Competitive Mapping“ entwickelt wurde, um ausgehend von einer Analyse des dynamischen Markt-und Wettbewerbsumfelds des Unternehmens im Rahmen einer Mikro-und Makroanalyse Risiken, aber auch Potenziale und Chancen identifizieren zu können. Ein Schwerpunkt im Vortrag lag auf dem Umgang mit strategischen Risiken, da nur das konsequente Management dieser Risiken das Überleben der Unternehmung und den Erfolg auf Dauer sichern kann. Hingewiesen wurde dabei darauf, dass Nachhaltigkeitsmanagement hierbei als eine Überlebensstrategie zum Erhalt lebensnotwendiger strategischer Ressourcen anzusehen ist.

Nach dem Rundgang durch das Museum für Optik mit vielen Informationen zur Unternehmensgeschichte der Carl Zeiss AG sowie mit interessanten Exponaten und einem gemeinsamen Mittagessen im Zeiss Forum eröffnete Jan Offerhaus den Nachmittag mit einem Vortrag zu den Aktivitäten des Arbeitskreises „Risikomanagement-Standards“ und einem Einblick in die Entwicklung von ISO-Standards. Dabei wurde hervorgehoben, dass die Hauptaufgabe des Arbeitskreises darin besteht, einerseits über Standards zu informieren (z.B. über Neuerungen oder durch Interpretationshilfen) und andererseits Anregungen aus der RMA aufzugreifen und in die Normungsarbeit hineinzutragen. So wirkte der AK in den letzten Jahren bei der Erstellung des IDW PS 981 sowie bei der Ergänzung von DRS 20 bezüglich der nichtfinanziellen Berichterstattung im Lagebericht mit und begleitete aktiv die Neufassung von ISO 31000.

Wenngleich die Anregungen der RMA nicht immer vollumfänglich in den Normungsgremien aufgegriffen werden, ist dennoch die Mitwirkung im Interesse der Mitglieder ein wichtiger Aspekt der RMA-Arbeit als Interessensvertretung für Risikomanager im deutschsprachigen Raum. Ein wichtiges Arbeitspaket besteht für den AK aktuell darin, eine vergleichende Übersicht zu Risikomanagement-Standards zu erstellen, die Praktikern Hilfestellungen und Hinweise zur Anwendung von Risikomanagement-Standards liefern soll. Hierzu wurde aufbauend auf Vorarbeiten des AK im Rahmen einer Master Thesis von Tim Killig, Master-Student der FHDW Hannover, ein Kriterienraster entwickelt und dieses auf 5 relevante Normen angewendet. Einige Ergebnisse daraus wurden während der Sitzung durch Jan Offerhaus und Tim Killig vorgestellt. Der AK plant, sich mit den Ergebnissen der Master-Arbeit intensiv auseinanderzusetzen, diese weiterzuentwickeln und für Unternehmenspraktiker mittels Veröffentlichungen aufzubereiten.

RMA intern

Im zweiten Teil des Vortrags wurden die aktuellen Entwicklungen bei der ISO, nicht nur bezüglich ISO 31000, sondern generell mit Blick auf Managementsystem-Standards, vorgestellt. Alle neuen sog. Managementsystem-Standards (z.B. ISO 9001 für Qualitätsmanagement) müssen der sog. High Level Structure folgen. Diese gemeinsame Struktur erleichtert die Integration der verschiedenen Management-Systeme zu einem Gesamtsystem. Der Umgang mit Risiken im Rahmen eines jeden Management-Systems ist dabei ein wichtiger Bestandteil der neuen High Level Structure. Diese Klausel sorgte und sorgt in der Praxis oft für Konfusion, da die Interpretationen teilweise dahingehen, dass nun quasi jedes Management-System, wie etwa ein Qualitätsmanagement-System, zu dem Risikomanagement-System eines Unternehmens wird. Jan Offerhaus verwies darauf, dass es sich hierbei allerdings um eine Fehlinterpretation handelt. Die Klausel der High Level Structure soll „nur" dazu führen, dass die mit den Zielen des jeweiligen Management-Systems verbundenen Risiken systematischer behandelt werden. Ein Risikomanagement-System im Sinne eines Enterprise Risk Management Systems wird dadurch nicht geschaffen.

Im letzten Vortrag des Sitzungstages präsentierte Dr. Peter Meier, Steinbeis Transferzentrum Risikomanagement, Informationen und Thesen zur Integration von (Risiko-)Managementsystemen basierend auf Konzepten und Praxis innerhalb und außerhalb der ISO. Dr. Meier zeigte in Detailanalysen auf, wie wenig konkret das Thema der Integration von Management-Systemen in den verschiedenen ISO-Standards dargestellt wird und wie unterschiedlich die Begrifflichkeiten in den verschiedenen ISO-Standards verwendet werden. Ausgehend von diesem sehr kritischen Blick auf die „ISO-Welt" wurde auf die Vorstellung einer fiktiven Norm „f iso 1001:2018 Wertemanagementsysteme – Anforderungen" übergeleitet. Diese von Dr. Meier und Mitarbeitern am Steinbeis Transferzentrum Risikomanagement entwickelte „Norm" bedient sich übergreifend aus den ISO- und COSO ERM-Konzepten, stellt dabei aber das Management von Werten als zentralem Aspekt der Unternehmensführung in den Mittelpunkt. Hierdurch kann eine Integration der verschiedenen Management-Systeme gelingen, und letztendlich auch ein übergreifendes Management von Risiken. Das gedankliche Konstrukt dieser fiktiven Norm wurde von Dr. Meier bereits in vielen Projekten angewendet und sollte den Sitzungsteilnehmern Anregungen für die eigene Unternehmenspraxis liefern.

Alle Vorträge boten viel Gelegenheit für Diskussionen im Teilnehmerkreis. Viele Anregungen für die eigene Arbeit im Risikomanagement konnten mitgenommen werden. So gewappnet sollte keinem der Teilnehmer zukünftig ein „Waterloo" in der Arbeit als Risikomanager / in drohen. //

Bei Interesse an der Teilnahme an den nächsten Sitzungen der beiden Arbeitskreise in 2019 wenden Sie sich bitte an Geva Johänntgen (AK Integriertes Risikomanagement / geva.johaenntgen@rma-ev.org) bzw. Jan Offerhaus (AK Risikomanagement-Standards / jan.offerhaus@rma-ev.org).