PRÜFUNG DES RISIKOMANAGEMENTSYSTEMS DURCH DIE INTERNE REVISION

Posted on 16.03.2022 by Dirk Gohr

Category: Risikomanagement

AKTUALISIERTER DIIR REVISIONSSTANDARD NR. 2 – VERSION 2.1

Seit Inkrafttreten des Kontroll- und Transparenzgesetzes (KonTraG) im Jahr 1998 ist es die primäre Aufgabe eines Risikofrüherkennungssystems, mögliche "bestandsgefährdende Entwicklungen" (§ 91 Abs. 2 AktG) früh zu erkennen. Neben bestandsgefährdenden Einzelrisiken sind dabei insbesondere Kombinationseffekte von Einzelrisiken zu untersuchen, die in der Regel Krisen- oder gar Insolvenzen auslösen können, was vor allem eine methodisch fundierte Risikoanalyse sowie Risikoaggregation erfordert.

Die wesentlichen Anforderungen an ein Risikofrüherkennungssystem fasst bereits seit rund 24 Jahren der IDW Prüfungsstandard 340 des Instituts der Wirtschaftsprüfer (IDW) zusammen, der auch auf die zentrale Bedeutung einer Risikoquantifizierung und Risikoaggregation verweist. Die Bedeutung der Risikoaggregation wurde auch im jüngst überarbeiteten IDW PS 340 stärker betont. Mit dem IDW PS 981 existiert ergänzend seit dem Jahr 2017 ein (freiwilliger) Standard, der neben der Risikobewältigung vor allem auch die zentrale Bedeutung von Konzepten für die Messung von Risikotragfähigkeit, Risikotoleranz und Risikoappetit aufzeigt.

Alle Regelwerke haben allerdings eine wesentliche Anforderung an das Risikomanagement noch nicht ausreichend thematisiert: Die notwendige entscheidungsorientierte Ausrichtung von Risikomanagementsystemen. Risikomanagement ist keine isoliertes Managementsystem, das als Sattelitensystem losgelöst von weiteren Managementsystemen agiert. Das Management von Risiken findet vielmehr in vielen Managementsystemen statt. Mit "entscheidungsorientiert" ist ein neues Paradigma des Risikomanagements gemeint, demzufolge das Risikomanagement dazu beitragen soll, bei der Vorbereitung unternehmerischer Entscheidungen die dafür notwendigen Chancen- und Risiko-Informationen zu liefern. Dieser Ansatz wird im neuen Absatz 3 des § 91 AktG in den Fokus gerückt. Ausgelöst durch den "Fall Wirecard" ist am 01.07.2021 das FISG (Gesetz zur Stärkung der Finanzmarktintegrität) in Kraft getreten, um die internen Kontroll- und Risikomanagementsysteme börsennotierter deutscher Aktiengesellschaften zu stärken. Damit sollen Papiertiger-Risikomanagement-Systeme á la Wirecard – immerhin wurde das Voodoo-System auf rund 22 Seiten des Geschäftsberichts ausführlich dokumentiert und in hohen Tönen gelobt und vom Wirtschaftsprüfer testiert – der Vergangenheit angehören. Am Rande sei an dieser Stelle erwähnt, dass alle belastbaren Frühwarnindikatoren (u.a. Datenanalysen und Benchmarks) im Zusammenhang mit Wirecard von Regulatoren, Wirtschaftsprüfern und der Justiz unter den Teppich gekehrt wurden und als Fake-News von Shortsellern dargestellt wurden.

Die Verpflichtung zur Einrichtung eines angemessenen und wirksamen internen Kontrollsystems und eines entsprechenden Risikomanagementsystems ist seit 2021 im neuen Absatz 3 des § 91 AktG zu finden: "Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten."

Das Risikomanagement erfährt damit eine hervorgehobene Positionierung unter allen Managementsystemen, weil nach der Diskussion über die Gesetzesvorlagen beispielsweise andere wesentliche Managementsysteme – wie das Compliance-Management oder das Controlling – im Gesetz nicht genannt werden.

Dieses neue Paradigma eines "entscheidungsorientierten Risikomanagements" findet man vor allem in der neuen Version von COSO Enterprise Risk Management (ERM) aus dem Jahr 2017. Der ökonomische Mehrwert dieser Neuausrichtung von Risikomanagementsystemen ist offensichtlich. Das Risikomanagement soll dazu beitragen, dass schon vor einer Entscheidung deren Auswirkung auf Ertrag und Risiko gegeneinander abgewogen werden (also Handlungsoptionen risikogerecht bewertet werden). Dies geht einher mit einer engeren Verknüpfung von Risikomanagement und Finanzen sowie einer engen Verzahnung des Risikomanagements mit der Unternehmensstrategie.

Zu beachten ist, dass diese ökonomisch wünschenswerte Neuausrichtung des Risikomanagements auch geboten ist, um die in der Zwischenzeit durch die Rechtsprechung präzisierten Anforderungen an die Vorbereitung "unternehmerischer Entscheidungen" durch Geschäftsführer und Vorstände gerecht zu werden. Gemäß der sogenannten Business Judgement Rule (BJR) in § 93 AktG muss ein Geschäftsleiter bei der Vorbereitung "unternehmerischer Entscheidungen", beispielsweise in Bezug zu einer Investition, Akquisition oder Strategie-Veränderung, beweisbar "angemessene Informationen" vorliegen haben (eine analoge Anforderung gilt für GmbH-Geschäftsführer). Da die Auswirkungen unternehmerischer Entscheidungen unsicher sind, sind es insbesondere die Ergebnisse einer entscheidungsvorbereitenden Risiko- und Chancenanalyse, die in einer Entscheidungsvorlage zu dokumentieren sind. Daraus ergibt sich auch aus rechtlicher Sicht die Notwendigkeit einer entscheidungsorientierten Ausrichtung des Risikomanagements.

Daher ist bei Entscheidungen unter Risiko eine entscheidungsvorbereitende Risikoanalyse erforderlich, die auf einer fundierten Methodik basiert. Weicht der Entscheider negativ von diesem anerkannten Stand der Technik ab, so könnte das eine Pflichtverletzung darstellen, zumindest zur Beweislastumkehr zulasten des Managers führen. Die zentrale These lautet hier, dass ein gewissenhafter, ordentlicher Geschäftsleiter auch die Methoden-Grundlagen einschlägiger betriebswirtschaftlicher, technischer und rechtlicher Werkzeuge, Methoden und des aktuellen Wissens kennen muss, um über deren sachgerechten Einsatz überhaupt urteilen zu können. Dieses Know-how stellt einen wesentlichen Bestandteil der "angemessenen Informationen" im Sinn der Business Judgement Rule dar.

DIIR Revisionsstandard Nr. 2 aktualisiert und ergänzt

Mit dem DIIR Revisionsstandard Nr. 2 des Instituts für Interne Revision e.V. liegt bereits seit vielen Jahren ein praxisorientierter Risikomanagement-Standard vor, der die Anforderungen aus § 91 und § 93 AktG gemeinsam betrachtet. Der Standard ist klar fokussiert auf die Erfüllung der gesetzlichen Kernanforderungen (wie die frühe Identifikation möglicher "bestandsgefährdender Entwicklungen" im Sinne § 91 AktG).

Die Anwendung des DIIR Revisionsstandard Nr. 2 durch die Interne Revision kann dazu beitragen, bestehende Lücken im Risikomanagement aufzudecken und diese zu schließen.

Seit wenigen Tagen liegt Version 2.1 des DIIR Revisionsstandard Nr. 2 vor.

Im Standard wird gleich in der Präambel darauf hingewiesen, dass das unternehmensweite Risikomanagement eine Führungsaufgabe ist und integraler Bestandteil aller Geschäftsprozesse inklusive der Planungs- und Überwachungsprozesse jeder Organisation. Daher komme der Prüfung des Risikomanagementsystems auch eine besondere Bedeutung zu. Diese Bedeutung hat auch der Gesetzgeber auch mit dem neuen Absatz 3 im § 91 AktG (FISG) vorgenommen.

Die Interne Revision ist neben anderen Funktionen in einer Organisation, wie Compliance,

Risikomanagement und Controlling, Bestandteil des internen Überwachungssystems. Gemäß dem Three-Lines-of-Defence-Ansatz hat die Interne Revision als dritte Verteidigungslinie ("Third Line of Defence") neben der "First Line of Defence" (operatives Management als erste Verteidigungslinie) auch die Prozesse und Struktur der Funktionen in der "Second Line of Defence" (z. B. Compliance, Risikomanagement, Controlling, Qualitätsmanagement als zweite Verteidigungslinie) in ihre Prüfungstätigkeiten einzubeziehen.

Ziel des DIIR Revisionsstandards Nr. 2 ist die Darstellung von Grundsätzen für die Prüfung des Risikomanagementsystems durch die Interne Revision. Der Standard bildet damit ein Rahmenwerk zur Planung und Durchführung von Prüfungen des Risikomanagementsystems. Was für Praktiker im Risikomanagement oder der Internen Revision einen echten Mehrwert darstellt ist die Tatsache, dass das DIIR Hinweise zur Prüfung, beispielsweise in Form von Checklisten, veröffentlicht.

Der im Jahr 2022 überarbeitete DIIR Revisionsstandards Nr. 2 berücksichtigt die neuen gesetzlichen Anforderungen aus § 91 Absatz 2 und 3 sowie aus § 107 Absatz 3 bis 4 AktG sowie aus § 1 StaRUG (Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen). Hierbei geht es im Kern um die frühe Erkennung bestandsgefährdender Entwicklungen, die sich meist aus Kombinationseffekten mehrerer Einzelrisiken ergeben. Prüfungsgegenstand ist das gesamte Überwachungssystem, d. h. das Risikomanagementsystem im weiteren Sinn, dass alle Managementsysteme umfasst, die sich mit Risiken befassen.

Ein besonderes Augenmerk legt der überarbeitete Standard auf das am 01.01.2021 in Kraft getretenen StaRUG. So wird im Revisionsstandard klargestellt, dass analog zu § 91 Abs. 2 AktG die Geschäftsleitungen aller Gesellschaften ohne natürliche Personen als Vollhafter, speziell damit auch GmbH und GmbH & Co. KG, verpflichtet sind, mögliche bestandsgefährdenden Entwicklungen zu erkennen. Erstmalig wird von der Geschäftsleitung gefordert, bei einer kritischen Bestandsgefährdung nun "geeignete Gegenmaßnahmen" der Krisen- und Risikobewältigung, bis hin zu einem Restrukturierungsplan zu ergreifen.

Die Entscheidung über solche "Gegenmaßnahmen" ist grundsätzlich als eine "unternehmerische Entscheidung" im Sinne von § 93 AktG aufzufassen. Der DIIR Revisionsstandards Nr. 2 greift die infolge § 93 AktG kodifizierte entscheidungsorientierte Ausrichtung des Risikomanagements auf. Insbesondere ist bei der Entscheidungsvorbereitung aufzuzeigen, welche Chancen und Gefahren (Risiken) mit der beabsichtigten Entscheidung verbunden sind und wie sich der Risikoumfang durch die Entscheidung verändern würde.

Der ergänzte Prüfungsstandard greift in der Version 2.1 auch die Implikationen des am 01.07.2021 in Kraft getretenen FISG auf. Damit ergeben sich für die betreffenden börsennotierten Aktiengesellschaften Anforderungen, die über die allgemeinen Anforderungen aus § 1 StaRUG hinausgehen. Für die Interne Revision börsennotierter Aktiengesellschaften bedeutet dies, dass die Angemessenheit und Wirksamkeit (!) eines umfassenden Risikomanagementsystems und eines internen Kontrollsystems zu prüfen sind. Neben der Risikofrüherkennung umfasst dieses insbesondere auch die Risikobewältigung und die Einbeziehung von Risikoanalysen bei "unternehmerischen Entscheidungen" (§ 93 AktG).

Wirksamkeit von Risikomanagementsystemen wird in den Mittelpunkt gestellt

Der vom DIIR überarbeitete Revisionsstandards Nr. 2 hat zeitnah (was für die Agilität des DIIR spricht) die regulatorischen Änderungen der vergangenen Monate (FISG, StaRUG etc.) aufgegriffen und dies zum Anlass genommen, eine aktualisierte Fassung zu veröffentlichen. Insbesondere werden im

Standard die Anforderungen an ein "entscheidungsorientiertes Risikomanagement" berücksichtigt, wie dies auch bereits im überarbeiteten COSO-Standard umgesetzt wurde. Für den Praktiker liefert der DIIR Revisionsstandard Nr. 2 Impulse, wie man Lücken im Risikomanagement eines Unternehmens erkennen und beheben kann.

So sollten sich Risikomanager vor allem fragen, in welcher Form sie in Entscheidungsprozessen überhaupt um Rat gefragt werden. Und sie sollten sich selbstkritisch fragen, wie sie die vom Gesetzgeber geforderten angemessenen Informationen mit geeigneten Methoden aufbereiten. Denn später vor Gericht muss der Entscheider beweisen können, dass der unternehmerische Entscheidungsprozess durch Methoden unterstützt wurde, die den aktuellen Stand von Wissenschaft und Praxis widerspiegeln. Dieser Nachweis dürfte bei vielen heute in der Praxis existierenden Methoden (beispielsweise einfache Checklisten, Gefährdungskataloge, qualitative Risikomatrizen, FMEA etc.) vielen Entscheidern schwerfallen.