

Das Finanzmarktintegritätsstärkungsgesetz (FISG) Betriebswirtschaftliche Stellungnahme zu FISG und Risikomanagement

06. Oktober 2021, 08:45

Thomas Berger et al.



Wissenschaft

Aufgrund des "Falls Wirecard" hat der Gesetzgeber mit dem FISG (Finanzmarktintegritätsstärkungsgesetz) neue gesetzliche Regelungen geschaffen, die insbesondere das Risikomanagement der Unternehmen stärken sollen. Sie sind eine wesentliche Ergänzung zu den neuen Anforderungen aus § 1 StaRUG [vgl. Braun 2021; Gleißner/Lienhard/Kühne 2021; Nickert/Nickert 2021 und Weitzmann 2021], demzufolge Unternehmen "bestandsgefährdende Entwicklungen" früh erkennen sollen, und erstmalig alle haftungsbeschränkten Unternehmen auch verpflichtet werden, bei Bedarf "geeignete Gegenmaßnahmen" zu initiieren.

Das Anliegen dieser Stellungnahme war es, aus einer betriebswirtschaftlichen Perspektive auf besonders wesentliche Aspekte hinzuweisen; eine Kommentierung einzelner Formulierungen des FISG oder eine Umsetzung unserer Empfehlungen in Formulierungen für einen Gesetzestext ist nicht unsere Absicht. Als Ökonomen sehen die Autoren an einigen Stellen Präzisierungsbedarf [siehe grundlegend auch Velte 2020]. Die Stellungnahme ist insbesondere das Resultat des Sachverhalts, dass – trotz Abschlussprüfung – eine Vielzahl auch der börsennotierten Unternehmen die gesetzlichen Anforderungen aus den §§ 91 und 93 AktG bisher nicht erfüllen [was man meist sehr leicht beweisen kann, siehe vertiefend Gleißner 2020].

Überblick: FISG und Empfehlungen zum Risikomanagement

Die nachfolgend zu lesende Stellungnahme wurde von den Autoren vor Verabschiedung des FISG erstellt, um auf Weiterentwicklungsbedarf im Hinblick auf die gesetzlichen Mindestanforderungen an das Risikomanagement zu verweisen. Die nachfolgend zusammengefasste und im folgenden Abschnitt näher erläuterten Empfehlungen wurden vom Gesetzgeber teilweise, aber nicht vollständig umgesetzt. Ein kurzer Abgleich zwischen dem verabschiedeten Gesetz und diesen Empfehlungen ist im übernächsten Abschnitt zu finden, der in der ursprünglichen Stellungnahme der Autoren nicht enthalten war (verfasst von Werner Gleißner).

Beim FISG sollten nach Einschätzung der an der Studie beteiligten Hochschullehrer folgende Aspekte besonders berücksichtigt werden:

1. Empirische Studien zeigen, dass ein Großteil der deutschen Unternehmen die gesetzlichen Anforderungen aus den §§ 91 und 93 AktG (sowie § 1 StaRUG) nicht erfüllen, obwohl die Abschlussprüfer keine "schwerwiegenden Mängel" aufzeigen (so werden beispielsweise mögliche "bestandsgefährdende Entwicklungen" im Sinne § 91 AktG infolge von Kombinationseffekten von

Einzelrisiken mangels methodischer Defizite, insbesondere bzgl. Risikoaggregation, oft nicht erkannt) [vgl. Scherer 2019, S. 12/13]. Eine Verbesserung des Risikomanagements ist notwendig.

2. Die Defizite im Risikomanagement resultieren insbesondere auch daher, dass die Abschlussprüfer die Methoden des Risikomanagements (anders als Prozesse und Organisationen) kaum analysieren. Durch das FISG sollte die Verpflichtung der Abschlussprüfer zur Prüfung des Risikomanagements erweitert und insbesondere eine Prüfung der Eignung der Methoden vorgeschrieben werden (wie beispielsweise im DIIR Revisionsstandard Nr. 2 des Deutschen Instituts für die Interne Revision). Die Defizite resultieren auch daher, dass Aufsichtsräte durch den Vorstand nur unzureichend über die Risikolage und die Qualität des Risikomanagements informiert werden (vgl. Punkt 4).
3. Mit dem FISG sollte festgehalten werden, dass der Abschlussprüfer die gesetzlichen Anforderungen an das Risikomanagement aus den §§ 91 und 93 AktG und § 1 StaRUG komplett prüfen soll. Bisher betrachtet wird nur § 91 AktG [vgl. Gleißner 2021c; Schmidt/Henschel 2021 und Gleißner 2017]. So wird beispielsweise nicht untersucht, ob bei der Vorbereitung "unternehmerischer Entscheidungen" (§ 93 AktG) deren Auswirkungen auf den Risikoumfang des Unternehmens analysiert werden (Business Judgement Rule). Der Prüfungsgegenstand der Jahresabschlussprüfung ist bisher unangemessen eingeschränkt.
4. Es gibt erkennbares Eigeninteresse eines Vorstands, den Aufsichtsrat über (1) durch den Vorstand selbst verursachte Risiken, (2) einen möglicherweise schon bestandsgefährdenden Gesamttriskoumfang oder (3) methodische Defizite im Risikomanagement, beispielsweise bei der Risikoaggregation, nicht zu informieren. Zu empfehlen ist deshalb, dass ein vom Vorstand möglichst in Abstimmung mit dem Aufsichtsrat zu benennender Gesamtverantwortlicher für das gesamte Risikomanagement (siehe Punkt 3) – wie auch der Leiter interne Revision – regelmäßig über solche Sachverhalte den Aufsichtsrat informiert. Zu seiner persönlichen Absicherung und damit eine "neutrale" Darstellung von Risiko und Risikomanagement gegenüber dem Aufsichtsrat ist es sinnvoll festzuhalten, dass eine Entlassung des Verantwortlichen für das Risikomanagement nur mit Zustimmung des Aufsichtsrats möglich ist.

Die hier zusammengefassten Kernpunkte, die im folgenden Abschnitt entsprechend des Textes der Stellungnahme erläutert werden, wurden in Teilen durch das Gesetz abgebildet. Die wesentlichen Aspekte des FISG sind zur Einordnung nachfolgend wiedergegeben (der nachfolgende Abschnitt ist in der Originalstellungnahme nicht enthalten und wurde durch Werner Gleißner nach Inkrafttreten des Gesetzes ergänzt).

Mit dem FISG ergeben sich neue Anforderungen für das Risikomanagement insbesondere durch den neuen Absatz 3 des § 91 AktG:

"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 Kontrollsysteem und Risikomanagementsystem einzurichten."

Das Risikomanagement erfährt damit eine hervorgehobene Positionierung unter den Managementsystemen.

Neben der Risikofrüherkennung zum Zweck der Identifikation möglicher "bestandsgefährdender Entwicklungen" befasst sich ein umfassendes Risikomanagement mit der Risikobewältigung (siehe analog §1 StaRUG mit der Forderung nach "geeigneten Gegenmaßnahmen") und gewährleitet die Berücksichtigung von Risikoinformationen bei "unternehmerischen Entscheidungen" (§ 93 AktG).

Bei den börsennotierten Aktiengesellschaften soll nun erreicht werden, dass ein "umfassendes" Risikomanagementsystem implementiert ist, das sich – unabhängig von möglichen bestandsgefährdenden Entwicklungen – mit allen wesentlichen Chancen und Gefahren (Risiken) befasst, und auch geeignete Methoden für Risikosteuerung und Risikobewältigung bereitstellt. Ein solches Risikomanagementsystem hat entsprechend § 93 AktG insbesondere die Aufgabe bei der Vorbereitung "unternehmerischer Entscheidungen" durch Risikoanalysen mitzuwirken ("entscheidungsorientiertes Risikomanagement") [vgl. hierzu Gleißner/Romeike 2020].

Gemäß §107 AktG ist nun zudem auch eine direkte Kommunikation zwischen dem Aufsichtsrat (Prüfungsausschuss) einerseits und dem Risikomanagement (sowie interner Revision und internem Kontrollsyste) andererseits vorgesehen. Zielsetzung ist es sicherzustellen, dass der Aufsichtsrat ein eigenständiges – auch vom Vorstand möglichst wenig beeinflusstes – Bild von Risikolage und Qualität des Risikomanagementsystems erhält.

Empfehlungen zum FISG

1. Defizite im Risikomanagement und Abschlussprüfung des Risikomanagements

Status: Empirische Studien zeigen Schwächen der Risikomanagementsysteme eines großen Teils der deutschen börsennotierten Aktiengesellschaften in Bezug auf die Erfüllung der gesetzlichen Anforderungen aus den §§ 91 und 93 AktG auf. So zeigt beispielsweise die aktuelle Benchmark-Studie von Deloitte (2020), dass 41 % der befragten Unternehmen nicht über eine dokumentierte Risikostrategie und 52 % nicht über ein ganzheitliches Risikotragfähigkeitskonzept verfügen. Eine im Jahr 2021 durchgeführte Benchmark-Studie von RiskNET aus dem Jahr 2021 bestätigt diese Aussage. 63 % der befragten 160 Unternehmen, die aktuell noch über keinen Ansatz zur Berechnung des Risikodeckungspotenzials (RDP) verfügen, haben keine Pläne, in naher Zukunft ein Risikotragfähigkeitskonzept bzw. ein Ansatz zur Berechnung des Risikodeckungspotenzials (RDP) zu entwickeln und zu dokumentieren. Die Benchmark-Studie zeigt auf, dass rund 50 % der Unternehmen mit semi-quantitativen oder rein qualitativen Ansätzen zur Risikobewertung arbeiten, was im Umkehrschluss bedeutet, dass eine "Bestandsbedrohung" des Unternehmens nicht ermittelt werden kann. Nur 36 % der befragten Unternehmen bewerten Risiken mithilfe geeigneter und für das jeweilige Risiko passende Verteilungsfunktionen, was die Grundlage für eine fundierte Risikoaggregation liefert [vgl. RiskNET 2021b].

Auch Einzelanalysen zu Insolvenzfällen, wie Euromicron [siehe Wolfrum 2020], Gerry Weber [siehe Gleißner/Hofmann 2021] oder Wirecard [vgl. Glaser 2021] zeigen, dass bei diesen Unternehmen jeweils auch gravierende Defizite im Risikofrüherkennungssystem festzustellen waren. Die Risikomanagementsysteme sind oft nicht in der Lage, mögliche "bestandsgefährdende Entwicklungen" früh zu erkennen. Defizite bestehen insbesondere im Bereich Risikoquantifizierung und Risikoaggregation. Nur durch eine simulationsbasierte Risikoaggregation, die viele Unternehmen immer noch nicht implementiert haben, lässt sich untersuchen, ob aus Kombinationseffekten von Einzelrisiken bestandsgefährdende Entwicklungen entstehen können. In der Regel sind bestandsgefährdende Entwicklungen das Resultat von Kombinationseffekten von Einzelrisiken, so dass das Fehlen einer Risikoaggregation grundsätzlich einen schwerwiegenden Mangel darstellt. Auch zeigen die Studien, dass die meisten Risikofrüherkennungssysteme noch primär die EBIT- oder Gewinnauswirkungen von Risiken betrachten, nicht aber die potenziell bestandsgefährdenden Auswirkungen auf die Liquidität (speziell auf das Rating und die Erfüllung von Covenants, die zur Kreditkündigung führen könnten) [siehe zu den Studien beispielsweise Köhlbrandt et al. 2020; Link et al. 2021; RiskNET 2021b; Ulrich 2019 sowie Gleißner 2020].

Meist ist sehr leicht beweisbar [siehe Gleißner 2020], dass gesetzliche Mindestanforderungen nicht erfüllt werden. Die Schwächen der implementierten Risikofrüherkennungssysteme sind im Ergebnis auch ein Resultat der unzureichenden Prüfung durch die Abschlussprüfer. Noch immer werden zentrale Anforderungen

an das Risikomanagement – wie z. B. die Risikoaggregation – in den meisten Fällen gar nicht oder nur oberflächlich geprüft.

Der im Jahr 2020 veröffentlichte neue IDW Prüfungsstandard 340 stellt hier eine deutliche Verbesserung dar, weist aber weiterhin gravierende Defizite auf (siehe dazu die Stellungnahme Angermüller et al. 2020). Neben fachlichen Kenntnisdefiziten im Bereich speziell der quantitativen Verfahren des Risikomanagements ist anzunehmen, dass auch die wirtschaftlichen Interessen der Abschlussprüfer zur Erklärung der gravierenden Prüfungsdefizite beitragen könnten [siehe Drewes et al. 2021].

Empfehlung:

Eine Präzisierung der Verpflichtung des Abschlussprüfers und eine Überwachung der Qualität der Abschlussprüfung sind zu empfehlen. Der vom Institut der Wirtschaftsprüfer verfasste IDW PS 340 (2020) lässt weiterhin sachlich unangemessene Spielräume bei der Abschlussprüfung. Eine konsequente methodische Prüfung des nach § 91 einzurichtenden Risikofrüherkennungssystems, speziell der Methoden für Risikoanalyse und Risikoaggregation, sollte gesetzlich vorgeschrieben sein.

Eine konsequenterne neutrale Prüfung der Qualität der Abschlussprüfung im Hinblick auf das Risikofrüherkennungssystem von Unternehmen ist zudem geboten. Auch ohne konkreten Anlass sollte zumindest stichpunktmaßig überprüft werden, ob ein seitens des Abschlussprüfers ohne schwerwiegende Mängel testiertes Risikofrüherkennungssystem eines Unternehmens den gesetzlichen Anforderungen genügt [siehe zu solchen Methoden der Begutachtung Gleißner 2020]. Ein solcher "Qualitätssicherungsdruck" dürfte die Qualität der Abschlussprüfung im Bereich Risikofrüherkennungssysteme verbessern. Die Abschlussprüferaufsicht ist entsprechend zu verstärken.

2. Schwache Stellung des Risikomanagements und fehlender Kontakt zum Aufsichtsrat

Status: Stellung und Ausstattung des Risikomanagements sind in den meisten Unternehmen vergleichsweise schwach. Es besteht insbesondere das Problem, dass der oder die Verantwortlichen für das Risikofrüherkennungssystem ausschließlich dem Vorstand gegenüber organisatorisch verantwortlich sind. Zudem gibt es weitere, etwaige konkurrierende Verantwortlichkeiten von Compliance, Risikomanagement, Treasury und Controlling. Dies führt zu einer Reihe gravierender Probleme:

1. Der Vorstand kann jederzeit erreichen, dass ihm unliebsame Risiken gar nicht bekannt werden oder die Quantifizierung eines Risikos nach eigenem Belieben festsetzen. Bei einer Reduzierung der Risikoeinschätzung beispielsweise infolge der Interessenslage des Vorstands ergibt sich in der Konsequenz, dass an sich erkennbare "bestandsgefährdende Entwicklungen" (§ 91 AktG) nicht aufgedeckt werden.
2. Risiken, die vom Vorstand selbst ausgehen, werden systematisch durch das vom Vorstand abhängige Risikomanagementsystem nicht erfasst, was auch oft durch mangelhafte Verknüpfung von Risk und Compliance gefördert wird. Neben einem "Vorstands-Fraud", wie bei Wirecard [vgl. Knake/Ströhmann 2020 und Lenz 2020], gehören in die hier nicht aufgedeckte Risikokategorie auch die sogenannten "Managementrisiken". Das sind insbesondere Risiken, die durch nicht sachgemäß vorbereitete oder durch persönliche Interessen getriebene "unternehmerische Entscheidungen" (§ 93) des Vorstands entstehen. Vom Vorstand selbst ausgelöste und zu verantwortende Risiken findet man in Risikoinventaren nur in den seltensten Fällen.
3. Fachkompetenten Verantwortlichen für das Risikomanagement eines Unternehmens ist meist durchaus klar, dass gesetzliche Mindestanforderungen aus den §§ 91 und 93 AktG nicht vollständig erfüllt sind (beispielsweise im Bereich Risikoaggregation). Die Verantwortlichen für das Risikomanagement haben

jedoch keine Möglichkeit, einen an den gesetzlichen Anforderungen orientierten Ausbau des Risikomanagements zu erreichen oder auch nur den Aufsichtsrat über bestehende Defizite zu informieren. Viele an sich im Unternehmen bekannte Defizite des Risikomanagementsystems bleiben so unerkannt (zumal die Abschlussprüfer sich bisher nicht adäquat mit den Problemen befassen) [vgl. Scherer 2019, S. 29/30].

4. Durch die oft mangelhafte Verknüpfung von Risk und Compliance werden die Risiken von Fraud nicht erfasst, da sie aus Sicht des Risikomanagements oft "systemimmanente" Risiken sind, die sich einer formalen Erfassung (und Bewertung selbst mit einfachen Value-at-Risk-Methoden) aus Sicht der Praxis entziehen, obwohl das natürlich kein Problem wäre.

Empfehlung:

Die jetzt schon im Gesetzesentwurf FISG vorgesehene direkte Verbindung und Kommunikationsrichtlinie von Risikomanagern zum Aufsichtsrat ist wichtig und notwendig. Wir empfehlen hier, gesetzlich die Stellung des Risikomanagements sogar noch weiter zu verstärken. Der Leiter Risikomanagement sollte regelmäßig bei Aufsichtsratssitzungen informieren über

- die Risikosituation, inklusive des "Grads der Bestandsgefährdung" (Insolvenzrisikos), also das Hauptergebnis der Risikoaggregation und speziell systemimmanente Risiken ("Fraud") sowie
- bekannte Defizite des Risikomanagementsystems selbst (beispielsweise fehlende Risikoaggregation).

Zur Absicherung der Position des Risikomanagers sollte zudem geregelt sein, dass dieser nicht ohne Zustimmung des Aufsichtsrats entlassen werden kann (für den Leiter Interne Revision sind ähnliche Regelungen sinnvoll). Ohne eine Absicherung der persönlichen Risiken des Verantwortlichen für das Risikomanagement kann nicht erreicht werden, dass der Aufsichtsrat über problematische Entwicklungen der Risikolage oder Defizite des Risikomanagements adäquat informiert wird [vgl. Scherer 2019, S. 40].

3. Unvollständige Prüfung des Risikomanagements durch den Abschlussprüfer (nur § 91 AktG und nicht § 93 AktG und nicht StaRUG)

Status: Die Prüfung des Risikomanagements durch den Abschlussprüfer ist bisher entsprechend § 317 HGB nur ausgerichtet auf das Risikofrüherkennungssystem (§ 91 AktG). Bisher nicht betrachtet werden die Anforderungen aus den §§ 93 AktG und § 1 StaRUG (seit 01.01.2021).

Das StaRUG ist nicht nur relevant für Unternehmen in der Krise, sondern für alle Unternehmen, weil es auch Anforderungen an die Krisenfrüherkennung und damit das Risikomanagement formuliert (GmbHs) [siehe Gleißner/Haarmeyer 2019; Nickert/Nickert 2021 und Gleißner/Lienhard/Kühne 2021].

Wichtig ist insbesondere § 1 StaRUG:

"§ 1 Krisenfrüherkennung und Krisenmanagement bei haftungsbeschränkten Unternehmensträgern

(1) Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht. [...]"

Der erste Satz entspricht weitgehend den Anforderungen des KonTraG (§ 91 AktG), demzufolge Systeme zur Früherkennung von "bestandsgefährdenden Entwicklungen" einzurichten sind. Schon aus den Erläuterungen zum KonTraG ist bekannt und in den diversen Standards festgehalten, dass die Krisenfrüherkennung ein Risikofrüherkennungssystem erfordert (siehe beispielsweise IDW PS 340 n. F. (2020) und DIIR RS Nr.2) [siehe Gleißner/Kimpel, 2019.].

StaRUG geht über bisherige gesetzliche Anforderungen hinaus. Die Geschäftsleiter werden nun mit § 1 StaRUG verpflichtet "geeignete Gegenmaßnahmen" zu ergreifen, wenn eine schwere, also bestandsgefährdende, Krise droht. Es wird also eine Planung von Gegenmaßnahmen und eine "unternehmerische Entscheidung" zu Krisenbewältigungsmaßnahmen gefordert [vgl. RMA 2019 und Gleißner 2021a]. Dies ist für die Stärkung des Risikomanagements entscheidend.

Zudem ist § 93 AktG für das Risikomanagement von grundlegender Bedeutung. Gefordert wird hier nämlich, dass bei "unternehmerischen Entscheidungen" die dafür erforderlichen "angemessenen Informationen" belegbar vorliegen sollen. Da unternehmerische Entscheidungen unsichere Auswirkungen haben, gehört zu diesen Informationen insbesondere die Erkenntnisse einer Risikoanalyse. Es ist aufzuzeigen, welche Veränderungen des Risikoumfangs durch die Entscheidung erfolgen. Diese Anforderung an ein entscheidungsorientiertes Risikomanagement ist ökonomisch von grundlegender Bedeutung, weil sich der Risikoumfang eines Unternehmens gerade durch Entscheidungen der Unternehmensführung verändert – und damit eben bereits vor der Entscheidung klar sein soll, welcher Risikoumfang nach der Entscheidung besteht [siehe dazu Gleißner 2017 und 2018 sowie weiterführend Hartmann/Romeike 2015; Romeike 2014; Graumann et al. 2009; Angermüller et al. 2020 sowie RMA 2019].

In einer Vielzahl von Veröffentlichungen und auch Risikomanagement-Standards wurde auf diesen Sachverhalt hingewiesen (siehe den DIIR RS Nr. 2, 2018). Es ist zu erwähnen, dass auch schon aus § 91 AktG alleine geschlossen werden kann, dass die Einbeziehung des Risikomanagements und Risikoanalysen erforderlich sind, um unternehmerische Entscheidungen vorzubereiten. Nach § 91 AktG ist nämlich "früh" auf mögliche bestandsgefährdende Entwicklungen hinzuweisen; was natürlich impliziert, dass schon vor einer Entscheidung – und erst nicht danach – bekannt sein sollte, ob und in welchem Umfang durch die mit der Entscheidung einhergehenden Risiken "bestandsgefährdende Entwicklungen" entstehen [siehe Gleißner 2017]. Der jüngere § 93 AktG ist hier im Hinblick auf den Umgang mit Risiken im Wesentlichen eine Klarstellung.

Tatsächlich wird die entscheidungsorientierte Ausrichtung des Risikomanagements (§ 93 AktG) und die Einbeziehung von Risikoanalysen bei der Vorbereitung "unternehmerischer Entscheidungen" vom Abschlussprüfer bisher in der Regel nicht betrachtet. Damit besteht eine gravierende Lücke in der Beurteilung des Risikofrüherkennungssystems. Es wird nämlich damit beispielsweise nicht aufgedeckt, dass bei einem Unternehmen möglicherweise eine bestandsgefährdende Entwicklung gerade durch eine unternehmerische Entscheidung (beispielsweise bezüglich einer Akquisition) auftreten kann, die mangels entscheidungsvorbereitender Risikoanalyse aber übersehen wird [vgl. Scherer 2019, S. 28-35].

Empfehlung:

Es wird empfohlen gesetzlich mit dem FISG klarzustellen, dass die Abschlussprüfer bei der Beurteilung des Risikomanagements eines Unternehmens die Implikationen aus den §§ 91 und 93 AktG sowie § 1 StaRUG gemeinsam berücksichtigen sollen. Der Abschlussprüfer muss entsprechend den gesetzlichen Vorgaben an die Unternehmen also beurteilen, ob

- das Unternehmen in der Lage ist, mögliche "bestandsgefährdende Entwicklungen", aus Einzelrisiken oder deren Kombinationseffekte früh zu erkennen (§ 91 AktG/§ 1 StaRUG),
- bei der Vorbereitung "unternehmerischer Entscheidungen" deren Implikationen für Risikoumfang analysiert und gewürdigten wurden (§ 93 AktG) und

- Regelungen im Unternehmen bestehen, damit bei einer erkennbaren "bestandsgefährdenden Entwicklung" die nach §1 StaRUG geforderten "geeigneten Gegenmaßnahmen" realisiert werden.

Ergänzend empfehlen wir zur begrifflichen Klarstellung zu verdeutlichen, dass die im Gesetz genannten "bestandsgefährdenden Entwicklungen" das Resultat sein können von Einzelrisiken oder deren Kombinationseffekten.

4. Fehlende Prüfung der Methoden zu Risikoanalyse und Risikoaggregation

Status: Wie unter 1. erwähnt, erfordert die Früherkennung möglicher "bestandsgefährdender Entwicklungen" im Sinne § 91 AktG bzw. § 1 StaRUG insbesondere den Einsatz adäquater Verfahren für die quantitative Risikoanalyse und eine simulationsbasierte Risikoaggregation, zur Auswertung von Kombinationseffekten der Risiken (i.d.R. eine Monte-Carlo-Simulation).

Ohne eine Prüfung der verwendeten Methoden – und die bisher in Praxis übliche primäre Betrachtung von Organisation und Prozessen des Risikomanagements – kann, wie die vorliegenden Studien zeigen, nicht erreicht werden, dass Risikofrüherkennungssysteme den gesetzlichen Anforderungen genügen. Wie eine deutlich klarere, auch die Prüfung der Methoden einbeziehende Grundlage für die Prüfung von Risikomanagementsystemen aussehen kann, zeigt beispielhaft der hier wesentlich präzisere Standard des deutschen Instituts für interne Revision (DIIR Revisionsstandard Nr. 2, von 2018).

Empfehlung:

Da ohne sachgerechte Methoden die gesetzlichen Anforderungen nicht erfüllt werden können, sollte gesetzlich explizit gefordert werden, dass die hierfür im Unternehmen verwendeten Methoden durch den Abschlussprüfer formal und materiell zu prüfen sind. Bisher ist die Prüfung der Abschlussprüfer primär auf Organisation und Prozesse ausgerichtet, und vernachlässigt die Methoden. Dies ist in DIIR RS Nr. 2 von 2018 bereits umgesetzt.

Fazit und Ausblick

Mit dem FISG und speziell dem neuen § 91 Abs. 3 AktG kann die angestrebte Stärkung des Risikomanagements erreicht werden [dieser Abschnitt ist eine Ergänzung zur Stellungnahme Berger et al 2021 und wurde durch Werner Gleißner nach Inkrafttreten des Gesetzes verfasst]. Viele der oben genannten Empfehlungen wurden grundsätzlich aufgegriffen. Neben der Verpflichtung zu einem "umfassenden Risikomanagement" bei börsennotierten Aktiengesellschaften, das sich auch mit nicht bestandsgefährdenden Risiken, Risikobewältigung und der Vorbereitung unternehmerischer Entscheidungen befassen sollte, ist hier insbesondere die Möglichkeit eines direkten Informationsflusses zwischen Aufsichtsrat und Risikomanagement zu nennen (§107 AktG). Anzumerken ist allerdings, dass einige in den Empfehlungen vorgeschlagenen Präzisierungen nicht zu finden sind, was (unnötige) Unsicherheiten impliziert. Es wäre entsprechend der Stellungnahme empfehlenswert klarzustellen, dass beispielsweise das Risikomanagement entsprechend § 93 AktG auch bei der Vorbereitung unternehmerischer Entscheidungen mitzuwirken hat und auch diese gesetzliche Anforderung Gegenstand der Prüfung durch den Abschlussprüfer sein sollte. Der Informationsfluss zwischen Aufsichtsrat einerseits und Risikomanagement (sowie interner Revision) andererseits, ist durch das FISG verbessert worden; aber weniger konsequent als in dieser Stellungnahme vorgeschlagen. Auch die Stellung von internen Kontrollsystmen zum Risikomanagement bleibt offen. Aus betriebswirtschaftlicher Sicht sollte das interne Kontrollsystem als Teil eines umfassenden Risikomanagements aufgefasst werden, und zwar als der Teil, der sich mit von Menschen verursachten operationellen Risiken befasst.

Autoren:

Prof. Thomas Berger | Duale Hochschule Baden-Württemberg Stuttgart

Prof. Roland Erben | Hochschule für Technik Stuttgart

Prof. Dietmar Ernst | Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen

Prof. Werner Gleißner | TU Dresden

Prof. Hans-Ulrich Holst | Hochschule Osnabrück)

Prof. Matthias Meyer | Technische Universität Hamburg-Harburg

Prof. Josef Scherer | Technische Hochschule Deggendorf

Prof. Ottmar Schneck | SRH Fernhochschule, Riedlingen

Prof. Patrick Ulrich | Hochschule Aalen

Prof. Ute Vanini | Fachhochschule Kiel

Weiterführender Literaturhinweise:

- Angermüller, N. O./Berger, Th. B./Blum, U./Erben, R. F./Ernst, D./Gleißner, W./Grundmann, Th./Heyd, R./Hofmann, K. H./Mayer, Ch./Meyer, M./Rieg, R./Schneck, O./Ulrich, P./Vanini, U. (2020): Gemeinsame Stellungnahme zum IDW EPS 340, Stand 17.02.2020, Download unter:
<https://www.idw.de/blob/121892/bdef576a6a3bfff52ee039511482c6057/down-idweps340nf-gem-stn-hochschullehrer-rm-data.pdf>, abgerufen am 23.04.2021.
- Berger, Th./Erben, R./Ernst, D./Gleißner, W./Holst, H.-U./Meyer, M./Scherer, J./Schneck, O./Ulrich, P./Vanini, U. (2021): Gemeinsame Stellungnahme zum FISG, Stand 18.05.2021.
- Braun, E. (2021): StaRUG: Unternehmensstabilisierungs- und -restrukturierungsgesetz, C.H.Beck, München.
- Deloitte (2020): Benchmarkstudie Risikomanagement 2020. Ausgestaltung von Risikomanagementsystemen nach IDW PS 981 und IDW 340 n.F., Download unter:
<https://www2.deloitte.com/de/de/pages/audit/articles/risikomanagement-benchmarkstudie-2020.html>, abgerufen am 15.04.2021.
- Deutsches Institut für Interne Revision e.V. (2018): DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision, Version 2.0, 2018, Download unter:
https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr._2_Version_2.0.pdf, abgerufen am 06.10.2021.
- Drewes, M./Follert, F./Widmann, M. (2021): Der Fall Wirecard und die Folgen. Rechtsökonomische Analyse eines deutschen Gesetzesvorhabens, in: Zeitschrift für Corporate Governance (ZCG), 16. Jg., Heft 2/21 (April 2021), S. 72-79.
- Glaser, C. (2021): Wirecard & Co. -Warum sich große Betrugsfälle immer wieder ereignen. Erkenntnisse der größten Finanzskandale unserer Zeit, Kindle Edition, Heilbronn 2021.
- Gleißner, W. (2017): Risikomanagement, KonTraG und IDW PS 340, in: WPg, 3/2017, S. 158-164.
- Gleißner, W. (2018): Risikomanagement 20 Jahre nach KonTraG: Auf dem Weg zum entscheidungsorientierten Risikomanagement, in: Der Betrieb vom 16.11.2018, Heft 46, S. 2769-2774.
- Gleißner, W. (2020): Wie beweist man, dass das Risikomanagement den Anforderungen der §§ 91 und 93 AktG nicht genügt (obwohl bestätigende Prüfberichte der Abschlussprüfer existieren)?, in: RWZ, Heft 7-8/2020 (August 2020), S. 273-280.
- Gleißner, W. (2021a): Unternehmerische Entscheidungen. Haftungsrisiken vermeiden (§ 93 AktG, Business Judgement Rule), in: Controller Magazin, Heft 1, Januar/Februar 2021, S. 16-23.
- Gleißner, W. (2021b): Strategisches Management unter Unsicherheit: Das robuste Unternehmen, in: REthinking Finance, Heft 1/2021, S. 33-41.
- Gleißner, W. (2021c): IDW PS 340, DIIR RS Nr. 2 und StaRUG: Lücken der Abschlussprüfung und Implikationen für die interne Revision, ZIR, Heft 4/21, S. 173-177.

- Gleißner, W./Haarmeyer, H. (2019): Die "bestandsgefährdende Entwicklung" (§ 91 AktG) als "Tor" in ein präventives Restrukturierungsverfahren, in: ZInsO, Heft 45/2019, S. 2293-2299.
- Gleißner, W./Hofmann, K. H. (2021): Unerwartete Unternehmensinsolvenz trotz testiertem Risikomanagement? – Lessons Learned aus der Insolvenz der Gerry Weber International AG, in: Der Betriebswirt, Vol. 61, Nr. 3, S. 139-154.
- Gleißner, W./Kimpel, R. (2019): Prüfung des Risikomanagements und der neue DIIR Revisionsstandard Nr. 2 – Anforderungen der §§ 91 und 93 AktG an das Risikomanagement im Fokus, in: ZIR – Zeitschrift Interne Revision, Vol. 54, Heft 4/2019, S. 148-159.
- Gleißner, W./Romeike, F. (2020): Entscheidungsorientiertes Risikomanagement nach DIIR RS Nr. 2, in: Der Aufsichtsrat, Ausgabe 04/2020, S. 55-57.
- Gleißner, W./Lienhard, F./Kühne, M. (2021): Implikationen des StaRUG. Neue gesetzliche Anforderungen an das Krisen- und Risikofrüherkennungssystem, in: Zeitschrift für Risikomanagement (ZfRM), 2. Jg., Heft 2.21, S. 32-40.
- Graumann, M./Linderhaus, H./Grundei, J. (2009): Wann ist die Risikobereitschaft bei unternehmerischen Entscheidungen "in unzulässiger Weise überspannt"? in: BFuP, Heft 5/2009, S. 492–505.
- Hartmann, W./Romeike, F. (2015): Business Judgement Rule – Maßstab für die Prüfung von Pflichtverletzungen, in: Zeitschrift für das gesamte Kreditwesen, 68. Jg., Ausgabe 05-2015, S. 227-230.
- Knake, Ch./Ströhmann, M. (2020): Das "FinTech"-Unternehmen Wirecard und die Folgen – Ausgewählte Stakeholder und ihre Stellung im (bisherigen) Verfahren, in: Corporate Finance, Nr. 11-12, S. 319-321.
- Köhlbrandt, J./Gleißner, W./Günther, Th. (2020): Umsetzung gesetzlicher Anforderungen an das Risikomanagement in DAX- und MDAX-Unternehmen. Eine empirische Studie zur Erfüllung der gesetzlichen Anforderungen nach den §§ 91 und 93 AktG, in: Corporate Finance, Heft Nr. 07-08, S. 248-258.
- Lenz, H. (2020): Die Verantwortung des Abschlussprüfers zur Aufdeckung von Bilanzdelikten (Täuschungen, Vermögensschädigungen), in: Internationale und kapitalmarktorientierte Rechnungslegung (KoRIFRS), 20. Jg. (Dezember 2020), S. 546 ff.
- Link, M./Scheffler, R./Flath, T. (2021): Risikomanagement. Zwischen Pflichtübung und betriebswirtschaftlicher Wertschaffung, in: Zeitschrift für Risikomanagement (ZfRM), Heft 1.21, S. 19-24.
- Link, M./Scheffler, R./Flath, T./Oehlmann, D./Dommers, C. (2021): Risikomanagement in deutschen Industrieunternehmen, in: Controller Magazin, Heft 2/2021, S. 54-61.
- Nickert, A./Nickert, C. (2021): Früherkennungssystem als Instrument zur Krisenfrüherkennung nach dem StaRUG, in: GmbHR, Heft 8 (April 2021), S. 401-413.
- Scherer, J. (2019): Das interessiert Kapitalgeber: Antifragilität und der "Achilleskörper" des Ordentlichen Kaufmanns – Vermeidung der persönlichen Haftung für Missmanagement am Beispiel "Governance, Risk und Compliance ("GRC")" und Geschäftsprozessdigitalisierung, Download unter: <https://www.scherer-grc.net/files/fil/kapitalgeber.pdf>, abgerufen am 17.05.2021.
- Schmidt, A./Henschel, Th. (2021): Prüfung des Überwachungssystems gemäß § 91 Abs. 2 AktG. Kritische Analyse der Neufassung des IDW PS 340, in: ZIR, Heft 4/21, S. 182-194.
- Risk Management Association e. V. (RMA) (Hrsg.): Managemententscheidungen unter Risiko, erarbeitet von Werner Gleißner, Ralf Kimpel, Matthias Kühne, Frank Lienhard, Anne-Gret Nickert und Cornelius Nickert, Erich Schmidt Verlag Berlin, 2019.
- RiskNET (2021a): IDW PS 340 n. F. und StaRUG. Studie zur wirksamen Risikofrüherkennung, 05.05.2021, www.risknet.de/themen/risknews/studie-zur-wirksamen-risikofruherkennung/, abgerufen am 06.05.2021.
- RiskNET (2021b): Benchmark-Studie PS340: Umsetzung wirksamer Risikofrüherkennungssysteme, München 2021 [erscheint in Q4/2021].
- Romeike, Frank (2014): Risikomanagement im Kontext von Corporate Governance, in: Der Aufsichtsrat, 05/2014, S. 70-72.
- Ulrich, P. (2019): Risikomanagement im Mittelstand. Empirische Implikationen für Aufsichtsräte und Beiräte, in: Der Aufsichtsrat, Heft 12/2019, S. 173-175.
- Ulrich, P./Scheuermann, I. (2018): Bewertung des Risikomanagements - Empirische Ergebnisse aus der Unternehmenspraxis, in: Zeitschrift Risk, Fraud & Compliance, 13. Jg., No. 4, S. 151-156.

- Velte, P. (2020): Der Referentenentwurf für ein Finanzmarktintegritätsstärkungsgesetz (FISG). Reform der internen Corporate Governance nach dem Wirecard-Skandal, in: Steuer- und Bilanzpraxis (StuB), Heft 21/2020, S. 817-826.
- Velte, P./Eulerich, M. (2021): Das geplante Finanzmarktintegritätsstärkungsgesetz (FISG). Eine kritische Diskussion aus Sicht der Internen Revision, in: Zeitschrift Interne Revision (ZIR), 56. Jg., Heft 2/2021, S. 64-69.
- Weitzmann, J. (2021): Teil 1 Krisenfrüherkennung und -management, in: Pannen, K./Riedemann, S./Smid, S. (Hrsg.): StaRUG. Unternehmensstabilisierungs- und -restrukturierungsgesetz, C.H.Beck, S. 61-94.
- Wolfrum, M. (2020): Der Fall Euromicron AG – Beispiel für die Nutzlosigkeit von Risikomanagementtestaten durch den Wirtschaftsprüfer, in: RMA Risk Management & Rating Association e. V. (Hrsg.): Krisenbewältigung mit Risikomanagement – Jahrbuch Risikomanagement 2020, ESV, Berlin, S. 146-154.

[Bildquelle Titelbild: Adobe Stock.com / By skd]