Veröffentlicht in

ZCG – Zeitschrift für Corporate Governance

Heft 6 / 2021

Eulerich, M. / Gleißner, W. (2021):

„Lines of Defense und ihre Probleme: Erfahrungen aus vergangenen und aktuellen Unternehmensskandalen“, S. 266 – 273

Mit freundlicher Genehmigung der
ERICH SCHMIDT VERLAG GmbH & Co. KG, Berlin

www.esvmedien.de
www.esv.info
www.zcgdigital.de

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

06.21

16. Jahrgang
Dezember 2021
Seiten 241 – 288

ZCG

Zeitschrift für Corporate Governance

www.ZCGdigital.de

Leitung und Überwachung in der Unternehmens- und Prüfungspraxis

Fachbeirat:

Prof. Dr. Alexander Bassen, Universität Hamburg
Prof. Dr. Dr. h. c. Theodor Baums, Johann Wolfgang Goethe-Universität Frankfurt am Main
Prof. Dr. Thomas Berndt, Universität St. Gallen
WP/StB Prof. Dr. Manfred Bolin, International School of Management, Dortmund
Dr. Christine Bortenlänger, Geschäftsführendes Vorstandsmitglied Deutsches Aktieninstitut e. V.
Prof. Dr. Gerrit Brösel, FernUniversität in Hagen
Prof. Dr. Henning Herzog, Quadriga Hochschule Berlin
Ulrich Hocker, Hauptgeschäftsführer Deutsche Schutzvereinigung für Wertpapierbesitz e. V.
Prof. Dr. Anja Hucke, Universität Rostock
Prof. Dr. Annette G. Köhler, Universität Duisburg-Essen
Prof. Dr. Stefan Müller, Helmut Schmidt Universität Hamburg
Prof. Dr. Patrick Velte, Leuphana Universität Lüneburg
Prof. Dr. Axel von Werder, Technische Universität Berlin
WP/StB Prof. Dr. Norbert Winkeljohann, Norbert Winkeljohann Advisory & Investments
Prof. Dr. Henning Zülch, Handelshochschule Leipzig (HHL)

ZCG Management

Vertrauen durch Integrität
[Butscher/Grüninger, 245]

Combined Assurance im Mittelstand
[Ulrich/Scheuermann/Spitzenpfeil, 249]

ZCG Recht

Corporate Social Performance und Insolvenzwahrscheinlichkeit
[Fischer/Habermann/Burger, 255]

Bankenwirtschaft:
Die Institutsvergütungsverordnung im Wandel
[Waschbusch/Schuster, 259]

ZCG Prüfung

Lines of Defense und ihre Probleme
[Eulerich/Gleißner, 266]

ZCG Rechnungslegung

Qualität des Corporate Governance Reportings der DAX-Unternehmen
[Freidank/Handschumacher, 274]

Naturkapitalbilanzierung: Die Zukunft der Nachhaltigkeitsberichterstattung?
[Baumüller/Scheid, 281]

ESV ERICH SCHMIDT VERLAG

72017

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

Lines of Defense und ihre Probleme

Erfahrungen aus vergangenen und aktuellen Unternehmensskandalen

Prof. Dr. Marc Eulerich / Prof. Dr. Werner Gleißner*

Überraschende Insolvenzen wie die der Wirecard AG haben zu Zweifeln an der Qualität der Risikofrüherkennungssysteme deutscher Unternehmen und der diesbezüglichen Abschlussprüfung geführt. Im Beitrag werden die Lines of Defense einer guten Corporate Governance und die Stellung des Abschlussprüfers in diesem Kontext skizziert. Ausgehend von einer Zusammenfassung typischer Schwächen im Risikomanagement, die empirische Studien zeigen, werden deren Ursachen aufgezeigt und Vorschläge zur Stärkung der Leistungsfähigkeit des Risikomanagements abgeleitet.

1. Problemstellung

Überraschende Insolvenzen und Unternehmensskandale wie der spektakuläre Fall der Wirecard AG führen zu Zweifeln an der Leistungsfähigkeit der Überwachungs- und Risikomanagementsysteme.[1] Bei Insolvenzfällen wie der Euromicron AG[2] und der Gerry Weber AG waren auch gravierende Defizite im Risikofrüherkennungssystem festzustellen. Häufig sind es aber die bereits bestehenden Risiken, die Schieflagen, Verluste oder gar Insolvenzen auslösen. Die zentrale Aufgabe des Überwachungs- und Risikofrüherkennungssystems ist es gemäß § 91 AktG, mögliche bestandsgefährdende Entwicklungen aus solchen Risiken früh zu erkennen. Dabei ist es grundsätzlich belanglos, ob diese aus einem Haftpflichtfall, einer gescheiterten Produktentwicklung, einer makroökonomischen Krise oder aus einem Fraud-Risiko resultieren.

Im Fall Wirecard ist ein langjähriger und schwerer Betrugsfall, begangen offenkundig unter Mitwirkung von Vorstandsmitgliedern, durch keine relevante Stelle entdeckt worden. Dieser Spezialfall darf aber nicht den Blick auf den Sachverhalt verwehren, dass auch unentdeckte Risiken das Aktionärsvermögen schädigen oder gar Insolvenzen auslösen können. Aus Sicht der Aktionäre ist es dabei weitgehend belanglos, ob das Risiko auf eine disruptive Strategie eines Wettbewerbers, eine makroökonomische Krise infolge einer Pandemie oder das mögliche Fehlverhalten von Mitarbeitern, einschließlich der Vorstände, zurückzuführen ist.

In diesem Beitrag wird aus einer ganzheitlichen Perspektive die zentrale Bedeutung eines adäquaten und unternehmensweiten Risikomanagements aus Perspektive der Eigentümer (Aktionäre) betrachtet. Aus dieser Perspektive sind grundsätzlich alle Risiken (bewertungs-)relevant[3], die sich (negativ) auf den aktuellen oder künftigen Unternehmenswert auswirken. Wesentlich ist, dass aus Perspektive der Eigentümer grundsätzlich alle Bereiche eines Unternehmens, und damit auch die Mitglieder des Vorstands, als Risikoverursacher verstanden werden müssen. Insbesondere der Vorstand beeinflusst durch die strategischen und operativen Entscheidungen die aktuelle und zukünftige Risikoposition enorm. Es sind daher diese sorgfältig zu treffenden unternehmerischen Entscheidungen (§ 93 AktG) des Vorstands, die den Risikoumfang des Unternehmens maßgeblich beeinflussen.

Der vorliegende Beitrag zielt vor diesem Hintergrund darauf ab, die Bereiche der unternehmensweiten Überwachung und des unternehmensweiten Risikomanagements kritisch zu analysieren. In Abschnitt 2 wird zunächst das ganzheitliche Risikomanagement (im weiteren Sinn) eines Unternehmens betrachtet, wobei ein erweitertes Lines-of-Defense-Modell skizziert wird. Dies umfasst das (neue) Three Lines Modell (TLM) und weitere für die Risikoüberwachung wesentliche Institutionen: den Vorstand, den Aufsichtsrat[4] und den Abschlussprüfer. Alle Linien sind potenziell wesentlich für ein leistungsstarkes Überwachungs- und Risikomanagementsystem, das im Sinne der Anteilseigner agiert und damit eine Steigerung des Unternehmenswerts erreicht. In Abschnitt 3 wird die aktuelle und potenziell mögliche Rolle der einzelnen Linien diskutiert. Ausgehend von den theoretischen Überlegungen zu Handlungsmöglichkeiten und Interessen der Linien und unter Berücksichtigung empirischer Studien zur Qualität des Risikomanagements deutscher Unternehmen werden im abschließenden Kapitel Verbesserungsvorschläge in Form von Thesen zusammengefasst.

* Prof. Dr. Marc Eulerich ist Professor an der Universität Duisburg-Essen und Inhaber des Lehrstuhls für Interne Revision, Center for Internal Audit Excellence (marc.eulerich@uni-due.de). Prof. Dr. Werner Gleißner ist Honorarprofessor für „Corporate Risk Management“ und „Risikogerechte Bewertung und Managemententscheidungen“ an der TU Dresden und Vorstand der Future Value Group AG (kontakt@FutureValue.de, www.werner-gleissner.de).

1 Siehe zur Verantwortung des Abschlussprüfers zur Aufdeckung von Bilanzdelikten, erläutert am Fallbeispiel der Wirecard AG, Lenz, KoR 2020 S. 546–552.

2 Siehe Wolfrum, in: RMA e.V. (Hrsg.): Krisenbewältigung mit Risikomanagement – Jahrbuch Risikomanagement 2020, S. 146–154.

3 Siehe zum Einfluss von Risiken auf den Unternehmenswert Gleißner/Dorfleitner, Journal of Risk 2018 S. 1 f.; Gleißner WiSt 2011 S. 345 f.; Gleißner, MRR 2019 S. 1243.

4 Eulerich (ZIR 2012 S. 192) und Gleißner/Theisen (AR 2016 S. 85–87) sprechen hier von the last line of defense.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Risiken sollten nur dann eingegangen werden, wenn diese wertsteigernd sind. ◀

2. Multiple Lines of Defense: Internes Kontrollsystem (IKS), Risikomanagement, Interne Revision, Vorstand, Aufsichtsrat und Abschlussprüfer

2.1 Ziele des Risikomanagements aus Aktionärsperspektive

Bei der wertorientierten Unternehmensführung sollte es das primäre Ziel der Vorstände sein, im Interesse der Aktionäre den Wert des Unternehmens zu steigern.[5] Der Unternehmenswert ist dabei abhängig von der bestehenden bzw. zukünftigen strategischen und operativen Positionierung und der Ressourcenausstattung des Unternehmens.

Der Vorstand sollte durch die eigenen sorgfältig getroffenen unternehmerischen Entscheidungen (§ 93 AktG) die Risikoposition des Unternehmens so steuern, dass der Erwartungswert der zukünftigen Erträge und die Volatilität dieser Erträge (Ertragsrisiko) verbessert und bestandsgefährdende Entwicklungen (§ 91 AktG) oder gar eine Insolvenz abgewendet werden können.[6]

Da jede unternehmerische Tätigkeit mit Risiken verbunden ist, müssen die Entscheidungen des Vorstands genau die Risiken berücksichtigen, die über eine Optimierung des Ertrag-Risiko-Profils zu einer Steigerung des Unternehmenswerts führen.[7]

Aus dieser Zielsetzung lässt sich ableiten, dass das Risikomanagement (im weiteren Sinn) sicherstellen sollte, stets im Interesse des Unternehmens (und damit auch der Eigentümer) bestehende und zukünftige Risiken zu steuern. Insbesondere bedeutet dies, dass der Vorstand durch seine Entscheidungen den Risikoumfang des Unternehmens nicht in unangemessener Weise überzieht[8] und Risiken nur dann eingegangen werden, wenn diese wertsteigernd sind. Diese Anforderung findet man gespiegelt in den §§ 91 und 93 AktG.[9]

Beide Paragraphen richten sich an die Vorstände, wobei aus Sicht der Aktionäre zu hinterfragen ist, inwieweit der Vorstand entsprechend § 91 und 93 AktG tatsächlich Systeme implementiert hat, um mögliche bestandsgefährdende Entwicklungen früh zu erkennen, und auch Risiken bei unternehmerischen Entscheidungen berücksichtigt. Genau an dieser Stelle können die in Abb. 1 dargestellten Organe bzw. Funktionen eingreifen.

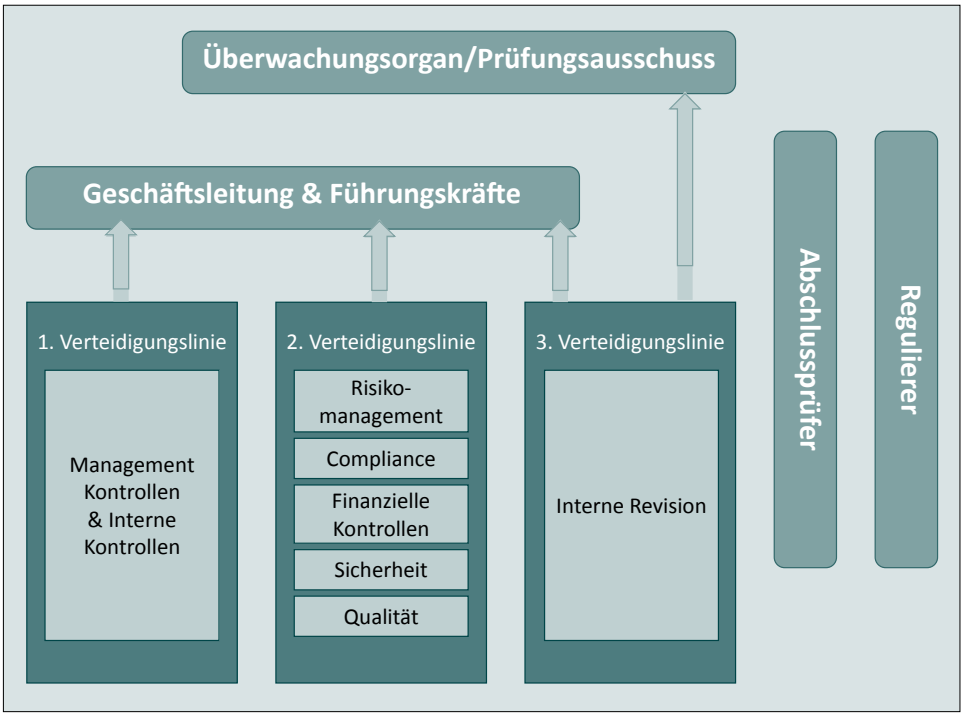

Abb. 1: Three-Lines-of-Defense-Modell[10]

2.2 Das unternehmensweite Risikomanagement im weiteren Sinn: von Three lines zu Multiple Lines of Defense (MLoD)

Ziel des ursprünglichen Three-Lines-of-Defense-Modells (TLoD) ist es, durch die Strukturierung der verschiedenen Governance-Funktionen die Risikoposition des Unternehmens zu steuern bzw. zu reduzieren.[11]

Im ursprünglichen Modell lassen sich die drei Verteidigungslinien wie folgt zusammenfassen:

1. Die erste Verteidigungslinie umfasst die internen Kontrollen und das IKS des Unternehmens, das idealerweise systematisch in alle operativen Tätigkeiten des Unternehmens eingebunden ist. Hierzu zählt auch die Überwa-

5 Vgl. hierzu allgemein Welge/Al-Laham/Eulerich, Strategisches Management, Wiesbaden 2017.
6 Zu den rechtlichen Anforderungen an das Risikomanagement aus den §§ 91 und 93 AktG Romeike, Rechtliche Grundlagen des Risikomanagement – Haftungs- und Strafvermeidung für Corporate Compliance, 2008; Gleißner, WPg 2017 S. 158–164; Gleißner, DB 2018 S. 2769–2774; Angermüller et al., abrufbar unter https://www.idw.de/blob/121892/0749c64f54f80bdee6c7f29d837a3f93/down-idweps340nf-gem-stn-hochschullehrer-rm-data.pdf (Abruf: 19.10.2021) zu einer Stellungnahme zum IDW PS 340.
7 Siehe zu den Grundlagen der wertorientierten Unternehmensführung Günther, Wertorientiertes Controlling 2009; Arbeitskreis Internes Rechnungswesen der Schmalenbach-Gesellschaft, ZfbF 2016 S. 797–820; Gleißner, Wertorientierte Unternehmensführung, Strategie und Risiko, E-Book 2019.
8 Siehe Graumann et al., BFuP 2009 S. 492–505; also das Insolvenzrisiko akzeptabel bleibt.
9 Gemäß § 91 AktG muss der Vorstand ein Überwachungssystem einrichten, damit mögliche bestandsgefährdende Entwicklungen früh erkannt werden. Solche ergeben sich aus Einzelrisiken oder Kombinationseffekten von Risiken, so dass eine Risikoanalyse und Risikoaggregation erforderlich sind. Gem. § 93 AktG muss jedes Vorstandsmitglied bei einer unternehmerischen Entscheidung belegen können, dass diese auf angemessenen Informationen basiert. Infolge der unsicheren Auswirkungen solcher Entscheidungen sind schon in den Entscheidungsvorlagen die mit diesen verbundenen Risiken zu benennen.
10 In Anlehnung an ECIIA/FERMA: Guidance on the 8th EU Company Law Directive, Article 41, S. 9 und IIA Position Paper: Three Lines of Defense in Effective Risk Management and Control (Stand: Januar 2013), S. 2.
11 Eulerich, ZIR 2012 S. 192.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Der Aufsichtsrat sollte im Rahmen einer für den Vorstand verbindlichen Risikopolitik Grenzen für die Art und den Umfang der akzeptierten Risiken klar formulieren. ◀

chung durch untergeordnete bzw. operative Managementeinheiten.

2. Die zweite Verteidigungslinie umfasst alle Funktionen, die systematisch Unternehmensrisiken abdecken. Hierzu zählen beispielsweise das Risikomanagement, das Controlling und die Compliance-Funktionen. Ihre Aufgabe sind das Bereitstellen adäquater Methoden und Prozesse für den Umgang mit Chancen und Gefahren (Risiken) sowie die Überwachung der risikobezogenen Aktivitäten der ersten Verteidigungslinie und die entscheidungsorientierte Aufbereitung von Risikoinformationen für die Unternehmensführung.
3. Die dritte Verteidigungslinie stellt die Interne Revision als unabhängige und objektive Prüffunktion dar, die die Effizienz und Effektivität der ersten und zweiten Verteidigungslinie überprüft und die Unternehmensführung und den Aufsichtsrat über die Prüfungsergebnisse informiert.

In der Zwischenzeit wurde das Three-Lines-of-Defense-Modell modifiziert und als Three Lines Modell veröffentlicht.[12] Hervorzuheben ist insbesondere, dass in der Modifikation die klassische Trennung der einzelnen Verteidigungslinien aufgebrochen wurde und die zu wählende Struktur der einzelnen genannten Governance-Organe unternehmensspezifisch angepasst werden kann. Hierdurch sind auch integrierte Governance-Funktionen denkbar.[14]

Im neuen TLM fehlt im Gegensatz zum alten TLoD der Begriff „Defense". Man will nicht mehr so stark den alleine defensiven Charakter dieses Corporate-Governance-Modells ausdrücken, sondern z. B. auch die Offenheit für Chancen (Opportunities) klarstellen.[15] Neben dem Schutz von Vermögenswerten soll damit auch eine Verbindung zum Value-Based-Management, also der Schaffung von Unternehmenswert, verdeutlicht werden.[16] Es geht nun nicht mehr darum, einfach Risiken und Bedrohungen zu vermeiden, sondern unter Berücksichtigung bestehender Chancen ein optimales Ertrag-Risiko-Profil und so eine Steigerung des Unternehmenswerts zu erreichen. Wesentlich ist zudem, dass die bisherige starre Trennung zwischen den drei Linien aufgegeben wurde – mit allen damit verbundenen Vor- und Nachteilen.[17] Wie Abb. 2 zeigt, weist das neue TLM mehr Flexibilität auf, insbesondere im Hinblick auf die Möglichkeit, Aufgaben z. B. der ersten und zweiten Linie oder auch der zweiten und dritten Linie zu verbinden und an einer Stelle zu kombinieren.

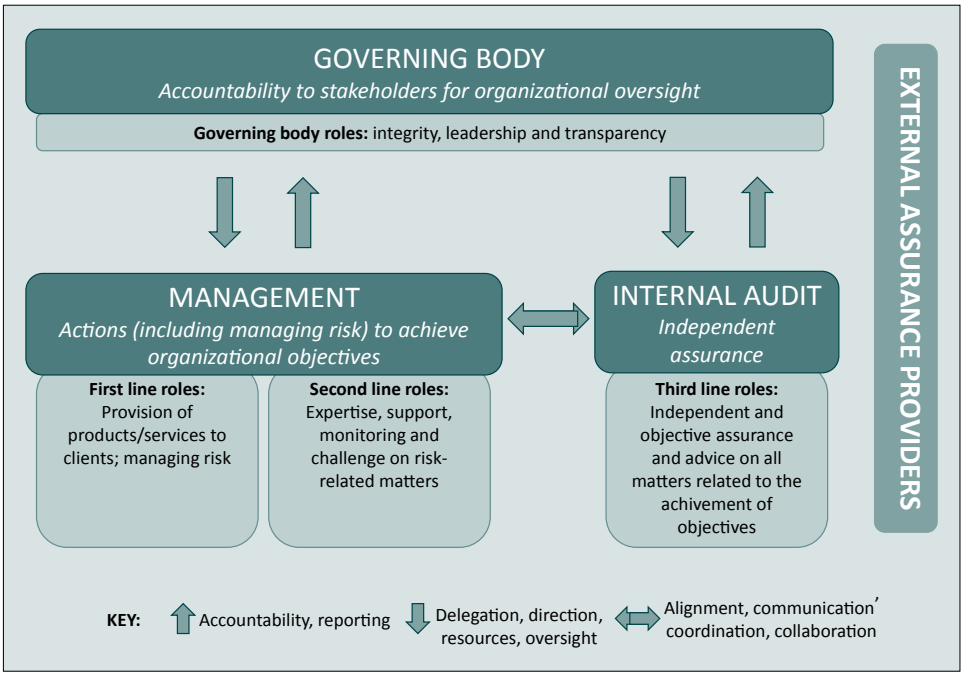

Abb. 2: Das Three Lines Modell (TLM)[13]

Aufbauend auf dem skizzierten TLoD ist daher aus Sicht der Aktionäre für ein ganzheitliches Risikomanagement zusätzlich auch die Rolle von

- Vorstand,
- Aufsichtsrat und
- Abschlussprüfer

zu diskutieren.

Wie bereits ausführlich dargestellt, nimmt der Vorstand als Organ der Unternehmensführung eine, wenn nicht sogar die, zentrale Rolle bei der Risikosteuerung ein. Der Vorstand entscheidet über die Strategie des Unternehmens genauso wie über die operative Ausrichtung und ist in die unternehmerischen Entscheidungen regelmäßig eingebunden. Zudem ist er als erster Auftraggeber der zuvor dargestellten Verteidigungslinien bzw. der dazugehörenden Funktionen der zentrale Knotenpunkt hinsichtlich der Risikosteuerung und Verarbeitung von Risikoinformationen. Folglich ist natürlich auch die Position des Vorstands in der internen Governance bzw. dem dargestellten TLoD von höchster Relevanz.

Gleiches gilt für die Stellung des Aufsichtsrats. Da sich die Entscheidungen des Vorstands in dem vom Aufsichtsrat definierten Rahmen bewegen und der Aufsichtsrat zudem bei wichtigen Entscheidungen mitwirkt, kann man den Aufsichtsrat neben seiner Rolle als Aufsichtsorgan und Überwachungsinstanz als Mitverantwortlichen für unternehmerische Entscheidungen auffassen. Der Aufsichtsrat sollte im Rahmen einer für den Vorstand verbindlichen Risikopolitik Grenzen für die Art und den Umfang der akzeptierten Risiken klar formulieren. Dabei ist der Fokus eines traditionellen

12 Eulerich, ZIR 2020 S. 208–216.
13 Quelle: The Institute of Internal Auditors (IIA), The IIA's Three Lines Model – An update of the Three Lines of Defense, 2020, S. 4.
14 Eulerich, Corporate Ownership & Control 2021 S. 180–187.
15 Siehe Eulerich, Corporate Ownership and Control 2021 S. 186.
16 Siehe Eulerich, Corporate Ownership and Control 2021 S. 180–187.
17 Eulerich, Corporate Ownership and Control 2021 S. 180–187.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Dem Abschlussprüfer kommt eine zusätzliche Risikoidentifikationsfunktion zu. ◀

Risikomanagements, das im Wesentlichen vorhandene Risiken überwacht und turnusgemäß Risikoberichte bereitstellt, nicht ausreichend. Ergänzend sollte der Aufsichtsrat die ökonomische Leistungsfähigkeit bzw. die Wirksamkeit des Risikomanagements regelmäßig prüfen (siehe hierzu auch § 107 Abs. 3 Nr. 2 AktG).

Darüber hinaus empfiehlt sich die Etablierung eines Qualitätssicherungssystems für Entscheidungsvorlagen, das klar formulierte Mindestanforderungen erfüllt, z. B. die zugrunde liegenden Annahmen, die Chancen und Risiken sowie die Implikationen der Entscheidung für die Performance und den Unternehmenswert. Der Aufsichtsrat sollte die relevanten Entscheidungsvorlagen als Advocatus Diaboli kritisch prüfen. Durch diese umfangreichen Möglichkeiten des Einflusses auf das Ertrag-Risiko-Profil des Unternehmens und die letztendliche (Mit-)Verantwortung für alle Risiken kann man den Aufsichtsrat als interne Last Line of Defense bei der Absicherung des Unternehmens auffassen.[18]

Erweitern lässt sich dieses Konzept durch die Hinzunahme von unternehmensexternen Organen bzw. Funktionen. Hierzu zählen einerseits der Abschlussprüfer und andererseits der Regulator. Weil der Abschlussprüfer aufgrund seiner gesetzlichen Pflicht mittlerweile nicht nur die Ordnungsmäßigkeit der Finanzberichterstattung prüfen muss, sondern auch die Umsetzung zahlreicher anderer Governance-Komponenten, kommt ihm eine zusätzliche Risikoidentifikationsfunktion zu.[19] Diese Aufgaben und die gesamte Prüfung sollen insbesondere im Interesse der Aktionäre die Qualität der Finanzberichterstattung und die positive Fortführungsprognose gewährleisten und damit potenzielle, verdeckte Risiken frühzeitig identifizieren.

Der Regulator kann entweder durch eigenständige Prüfungshandlungen, wie z. B. im Rahmen der Bankenaufsicht, oder durch die Gesetzgebung in die Risikosteuerung einsteigen und durch die Kodifizierung von Vorgaben das Risikomanagement von Unternehmen beeinflussen.

3. Aktuelle Bewertung des Risikomanagements

3.1 Anforderungen an ein Risikomanagement

Die verschiedenen empirischen Studien zum Risikomanagement deutscher Unternehmen orientieren sich an unterschiedlichen Anforderungen, die sich aus Gesetz, Standards (wie dem IDW PS 340) oder ökonomischen Überlegungen ableiten lassen. Zu den aus den gesetzlichen Grundlagen ableitbaren Anforderungen an das Risikomanagement gibt es ein umfangreiches Schrifttum, dessen Kernaussagen sich wie folgt zusammenfassen lassen:[20]

1. Aus § 91 Abs. 2 AktG folgt, dass die Unternehmensführung geeignete Systeme zur frühen Erkennung möglicher bestandsgefährdender Entwicklungen implementieren muss. Da sich solche bestandsgefährdenden Entwicklungen aus negativen Auswirkungen wesentlicher Einzelrisiken oder Kombinationseffekten mehrerer Risiken ergeben, erfordert dies die Etablierung von Verfahren für die Risikoanalyse und Risikoaggregation; letztere um die Kombinationseffekte der Einzelrisiken auswerten zu können. Da bestandsgefährdende Entwicklungen sich im Allgemeinen durch eine (drohende) Illiquidität ergeben, sind hier insbesondere die Liquiditätsauswirkungen von Risiken und die Wirkungen von Risiken auf Ratinganforderung und Covenants, die eine Kreditkündigung zur Folge haben können, zu beachten (was der neue IDW PS 340 n. F. 2020 klarstellt). Von börennotierten Gesellschaften wird seit 1.1.2021 ein umfassendes und angemessenes und wirksames Risikomanagementsystem gefordert (§ 91 Abs. 3 AktG).

2. Aus § 93 AktG folgt, dass Risikoanalysen bei der Vorbereitung unternehmerischer Entscheidungen einzubeziehen sind, weil ein zentrales Charakteristikum unternehmerischer Entscheidungen gerade deren unsichere Auswirkungen sind.[21]

3. Mit dem StaRUG (§ 1) werden Geschäftsleiter haftungsbeschränkter Gesellschaften über die Früherkennung möglicher bestandsgefährdender Entwicklungen (siehe Punkt 1) zusätzlich verpflichtet, Gegenmaßnahmen zu initiieren, wenn eine solche schwere Krise festgestellt wird.

Die gesetzliche Anforderung gemäß Punkt 1 wird aufgegriffen im IDW PS 340 n. F. und im DIIR RS Nr. 2, der zusätzlich die Anforderungen aus § 93 AktG berücksichtigt und fordert, dass das Risikomanagement durch Risikoanalysen bei der Vorbereitung unternehmerischer Entscheidungen mitwirken soll. Die neuen Implikationen aus StaRUG (3.) sind in keinem der beiden Standards bisher explizit erfasst (eine Berücksichtigung in DIIR RS Nr. 2 ist geplant). Aus der Rechtsprechung und der zumindest in § 93 AktG formulierten Beweislast beim Vorstand ergibt sich zudem im Hinblick auf Risikomanagementsystem und Ergebnisse der Risikoanalyse eine weitreichende Dokumentationspflicht, die auch der IDW PS 340 n. F. (2020) betont.

Das Risikofrüherkennungssystem eines Unternehmens zielt nur auf die Früher-

18 Risk Management Association e.V. (RMA), Managemententscheidungen unter Risiko. Haftung – Recht – Business Judgement Rule, 2019.

19 Gegenstand der Abschlussprüfung ist heute das Risikofrüherkennungssystem. Diese Prüfung ist verpflichtend nur für börsennotierte Aktiengesellschaften. Die Beschränkung der Prüfung auf Anforderungen aus § 91 Abs. 2 AktG, der Grundlage ist für den IDW PS 340 n. F. (2020), ist als ein Problem der bestehenden Prüfungspraxis aufzufassen, weil sich Anforderungen an das Risikomanagement z. B. auch aus § 93 AktG ergeben, was später näher erläutert wird.

20 Siehe dazu Romeike, Rechtliche Grundlagen des Risikomanagement – Haftungs- und Strafvermeidung für Corporate Compliance, 2008; Gleißner, WPG 2017 S. 158–164; Gleißner, DB 2018 S. 2769–2774; Angermüller et al., abrufbar unter https://www.idw.de/blob/121892/0749c64f54f80bdee6c7f29d837a3f93/down-idweps340nfgem-stn-hochschullehrer-rm-data.pdf (Abruf: 19.10.2021); Berger et al., abrufbar unter https://www.risknet.de/themen/risknews/betriebswirtschaftliche-stellungnahme-zu-fisg-und-risikomanagement/ (Abruf: 19.10.2021).

21 Siehe dazu Graumann et al, BFuP 2009 S. 492–505; Hartmann/Romeike, Zeitschrift für das gesamte Kreditwesen 2015 S. 227–230; Risk Management Association e.V. (RMA), Managemententscheidungen unter Risiko. Haftung – Recht – Business Judgement Rule, 2019; Gleißner, CM 2021 S. 16–23; Hering/Toll, in: Petersen et al. (Hrsg.), Handbuch der Unternehmensbewertung, 2013, S. 173–183.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Die Risikomanagementsysteme vieler Aktiengesellschaften erfüllen selbst die gesetzlichen Mindestanforderungen aus §§ 91 und 93 AktG nicht. ◀

kennung möglicher bestandsgefährdender Entwicklungen aus Einzelrisiken oder deren Kombinationseffekt (siehe Punkt 1). Das Risikomanagement hat darüberhinausgehende Aufgaben, z. B. im Hinblick auf Risikosteuerung und Risikobewältigung, die z. B. im IDW PS 981 thematisiert werden. Da aus unternehmerischen Entscheidungen (§ 93 AktG, siehe Punkt 2) durch die mit diesen verbundenen zusätzlichen Risiken bestandsgefährdende Entwicklungen entstehen können, ist die Betrachtung solcher Entscheidungen für eine Früherkennung bestandsgefährdender Entwicklungen notwendig (was so auch im DIIR RS Nr. 2 zu lesen ist).

3.2 Empirische Studien

Fälle wie Euromicron[22], Gerry Weber[23] oder Wirecard[24], bei denen es ohne Angabe einer vorausgehenden bestandsgefährdenden Entwicklung zu einer plötzlichen Insolvenz bzw. Schieflage kam, sind nur spektakuläre Einzelfälle, die nicht auf grundlegende Defizite in Risikomanagementsystemen deutscher Unternehmen schließen lassen.

Im Allgemeinen lässt sich belegen, dass ein Risikomanagementsystem den gesetzlichen Anforderungen nicht genügt. Eine Vielzahl empirischer Studien mit unterschiedlichen Schwerpunkten verweist auf gravierende Defizite in den Risikomanagementsystemen.[25] Besonders eklatante Schwächen findet man in Bereichen, die zur Erfüllung der gesetzlichen Anforderungen gemäß 3.1 erforderlich sind. Meist kann man schon mit den öffentlich verfügbaren Daten leicht belegen, dass gesetzliche Anforderungen nicht oder nur eingeschränkt erfüllt werden können. Bei Gleißner (2020) findet man z. B. folgende Ansatzpunkte:[26]

- Es gibt keine Risikoaggregation mit einer adäquaten Methode (z. B. Monte-Carlo-Simulation).
- Das Risikomanagementsystem betrachtet seltene, aber relevante Extremrisiken mit potenziell bestandsgefährdenden Auswirkungen nicht.
- Liquiditätswirkungen von Risiken und Refinanzierungsrisiken werden nicht betrachtet.
- Es fehlt eine Präzisierung und Analyse des Gesamtfeldes möglicher bestandsgefährdender Entwicklungen (z. B. Vernachlässigung der Gefährdung durch Verletzung von Rating-Anforderungen oder Covenants).
- Die Risikoquantifizierung basiert nur auf Eintrittswahrscheinlichkeit und erwarteter Schadenshöhe, obwohl z. B. die Unsicherheit der Schadenshöhe betrachtet werden muss.

Um konkrete Schwächen in Risikomanagementsystemen im Hinblick auf § 93 AktG aufzuzeigen, lassen sich insbesondere die folgenden Ansatzpunkte heranziehen:

- Man zeigt, dass kein Prozess im Unternehmen vorgesehen[27] und implementiert ist, der gewährleistet, dass bei der Vorbereitung unternehmerischer Entscheidungen dokumentiert wird, welche Veränderung von Chancen und Gefahren (Risiken) sich durch diese Entscheidung ergeben würde.
- Man zeigt, dass in Entscheidungsvorlagen i. d. R. keine neutralen und quantitativen Risikoinformationen enthalten sind und damit unklar bleibt, welche Veränderung des Risikoumfangs sich durch die Entscheidung ergeben würde.[28]
- Man zeigt, dass nach einer Entscheidung an sich leicht erkennbare Risiken Planabweichungen ausgelöst haben, die in der Entscheidungsvorlage nicht genannt wurden, aber leicht erkennbar waren (z. B. weil unsichere Plananahmen immer auf hier bestehende Chancen und Gefahren, also Risiken, hinweisen).[29]

Die Risikomanagementsysteme vieler Aktiengesellschaften erfüllen selbst die gesetzlichen Mindestanforderungen aus §§ 91 und 93 AktG nicht.[30] Eine Studie zum Risikomanagement der DAX und MDAX-Unternehmen zeigt z. B. Folgendes:[31]

1. Bei den meisten Unternehmen muss bezweifelt werden, ob bestandsgefährdende Entwicklungen auch aus der Kombinationswirkung mehrerer Einzelrisiken erkannt werden.[32] Die dafür notwendige Risikoaggregation (Monte-Carlo-Simulation), die die Auswirkung auch mehrerer Risiken z. B. auf Covenants und das Rating untersucht, wird bei vielen Unternehmen (d. h. knapp drei Viertel) nicht durchgeführt.
2. Nur bei wenigen Unternehmen ist erkennbar, dass konsequentes Risikomanagement bei der Vorbereitung unternehmerischer Entscheidungen bereits konsequent einbezogen wird (siehe dazu DIIR RS Nr. 2).

Ähnliche Schwächen zeigt auch die Benchmark-Studie Risikomanagement 2020 von Deloitte auf.[33] Gemäß der Umfrage betrachten Unternehmen kaum die Möglichkeit einer Illiquidität. Zudem führen nur bestenfalls 24 Prozent der Unternehmen eine sachgerechte Risikoaggregation durch.[34]

22 Lenz (KoR 2020 S. 546–552) kommt bei einer Analyse des Fallbeispiels Wirecard zum Resultat, dass wesentliche Mängel im rechnungslegungsbezogenen Internen Kontrollsystem vom Konzernabschlussprüfer nicht erkannt und nicht angemessen beurteilt wurden.
23 Gleißner/Hofmann, DBW 2021 S. 139–150.
24 Wolfrum, in: RMA e.V. (Hrsg.): Krisenbewältigung mit Risikomanagement – Jahrbuch Risikomanagement 2020, S. 146–154.
25 Siehe z. B. Ulrich et al., KSI 2018 S. 154–160; Schwaiger/Brandstätter, CM 2020 S. 73–77; Köhlbrandt et al., CF 2020 S. 248–258.
26 Siehe Gleißner, RWZ 2020 S. 273–280.
27 Meist genügt hier eine Angemessenheitsprüfung (die Wirksamkeitsprüfung hat sekundäre Bedeutung).
28 Insb. wird man hier betrachten, ob das Risikomanagement entscheidungsorientiert ausgerichtet ist (siehe Gleißner/Hunziker, Expert Focus 2019 S. 745–749; Gleißner/Kimpel, ZIR 2019 S. 148–159), also in die Vorbereitung unternehmerischer Entscheidungen – also Entscheidungen unter Risiko – eingebunden wird.
29 In manchen Standards, wie dem DRS 20, wird begrifflich zwischen Chancen und Risiken unterschieden. Aus betriebswirtschaftlicher Perspektive sind Risiken mögliche Planabweichungen, die positiv (Chancen) oder negativ (Gefahren) sein können. Daher erscheint es sinnvoll, von den drei Begriffen – Risiken, Chancen und Gefahren – den Begriff Risiko als Überbegriff für Chance und Gefahr zu verwenden. Der DRS 20 verwendet den Risikobegriff wie Gefahr, oft auch Risiken im engeren Sinn genannt.
30 Vgl. z. B. auch Ulrich, ZCG 2019 S. 214–218.
31 Siehe Köhlbrandt et al., CF 2020 S. 248–258.
32 Was der IDW PS 340 und der DIIR Nr. 2 fordern.
33 Deloitte, Risikomanagement Benchmarkstudie 2020, abrufbar unter https://www2.deloitte.com/de/de/pages/audit/articles/risikomanagement-benchmarkstudie-2020.html (Abruf: 19.10.2021).
34 43 Prozent der Unternehmen geben an, eine Addition von Schadenserwartungswerten vorzunehmen, was nicht hilft, um eine Bestandsgefährdung zu erkennen.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Der Vorstand als zusätzliche Verteidigungslinie ist nur dann für die Aktionäre im Sinne eines guten Risikomanagements hilfreich, wenn die Interessenslage gleichgerichtet ist. ◀

Trotz der Prüfung seitens der Abschlussprüfer bestehen also insbesondere bei Risikoquantifizierung, Risikoaggregation und der Nutzung von Risikoinformationen bei der Vorbereitung unternehmerischer Entscheidungen gravierende Defizite. Die bisherige Prüfungspraxis ist folglich unbefriedigend. Ein Aktionär kann nämlich nicht darauf vertrauen, dass Unternehmen adäquate Risikomanagementsysteme haben, wenn ein Jahresabschluss uneingeschränkt testiert wird.

Die zentrale Anforderung aus § 91 Abs. 2 AktG ist darin zu sehen, dass das Risikofrüherkennungssystem bzw. das Risikomanagementsystems mögliche bestandsgefährdende Entwicklungen früh erkennt. Diese ergeben sich aus sehr seltenen Extremrisiken, die potenziell sehr hohe Schäden auslösen, oder aus Kombinationseffekten von Einzelrisiken. Diese auszuwerten und den Gesamtrisikoumfang zu bestimmen, ist Aufgabe der Risikoaggregation. Bei der Risikoaggregation muss unter Bezugnahme auf die Unternehmensplanung untersucht werden, wie wahrscheinlich Kombinationen von Einzelrisiken sind, die zur Illiquidität führen können. Überschuldung hat heute eine eher nachrangige Bedeutung. Zu beachten sind also die Liquiditätswirkungen von Risiken und die Auswirkungen der Risiken auf das zukünftige Rating und auf Kreditvereinbarungen (Covenants), die zur Kreditkündigung führen können.

Die Forderung zur Prüfung auch der Methoden des Risikomanagements, speziell der Risikoaggregationsverfahren, durch die Interne Revision findet man seit 2018 im DIIR Revisionsstandard Nr. 2. Auf die Notwendigkeit der Risikoaggregation mittels Monte-Carlo-Simulation wurde das IDW im Zusammenhang mit der Überarbeitung des IDW PS 340 von einer Gruppe von 16 Hochschullehrern hingewiesen.[35]

Im Ergebnis ist festzuhalten, dass die Risikomanagementsysteme deutscher Unternehmen (im weiteren Sinn) offenbar eklatante Schwächen aufweisen, weil

- gesetzliche Mindestanforderungen aus den §§ 91 und 93 AktG nicht erfüllt sind und
- das Ziel der Aktionäre (als Prinzipal) eines adäquaten Umgangs mit Risiken, speziell bei unternehmerischen Entscheidungen, nicht gewährleistet ist.

Es ist notwendig, dass nach der Veröffentlichung des neuen IDW Prüfungsstandards 340 n. F. (2020) Risikofrüherkennungssysteme konsequent geprüft werden.

3.3 Schwächen und ihre Ursachen

Für Erklärungen dieses Sachverhalts sind die o. g. Lines zu betrachten. Damit diese im Umgang mit Risiken im Sinne der Aktionäre agieren, sind zwei Voraussetzungen zu erfüllen:

1. Man benötigt die notwendigen Fähigkeiten und Ressourcen.
2. Die Interessen müssen kongruent zu denjenigen der Aktionäre sein.

Die relevanten Tätigkeiten und die dazu notwendigen Fähigkeiten im Umgang mit Risiken sind bekannt[36]: Identifikation, Quantifizierung, Aggregation und Überwachung von Risiken sowie die Fähigkeit, Risiken adäquat bei der Vorbereitung unternehmerischer Entscheidungen zu berücksichtigen (risikogerechte Bewertung). Nachfolgend werden die Linien im Hinblick auf (1) Interessenslage und (2) Fähigkeit diskutiert, um (a) mögliche bestandsgefährdende Entwicklungen früh zu erkennen und (b) die Berücksichtigung von Risiken bei unternehmerischen Entscheidungen zu gewährleisten.

Aus der Diskussion lässt sich folgendes festhalten: Das IKS (First Line) hat einen sehr unvollständigen Blick auf die Risiken und beschäftigt sich nur mit speziellen operationellen Risiken (ausgelöst durch Mitarbeiter unterhalb des Vorstands). Es schließt im Allgemeinen unternehmerische Entscheidungen der Vorstandsmitglieder nicht ein. Das Risikomanagement auf der Second Line of Defense ist bei den meisten Unternehmen, wie die Studien zeigen, schwach entwickelt.[37] Es ist bisher meist insbesondere noch nicht darauf ausgerichtet, bei unternehmerischen Entscheidungen systematisch durch Risikoanalysen einbezogen zu werden.[38] IKS und Risikomanagement sind dem Vorstand zugeordnet und haben zudem typischerweise nicht das Mandat, die durch den Vorstand selbst verursachten Risiken, die Managementrisiken,[39] zu betrachten. Weder IKS noch Risikomanagement befassen sich mit den Risiken, die durch die Entscheidung des Vorstands ausgelöst werden oder Fraud-Risiken infolge eines möglichen Betrugs durch ein Vorstandsmitglied. Die Verantwortlichen für IKS und Risikomanagement sind disziplinarisch dem Vorstand zugeordnet und von diesem disziplinarisch abhängig, so dass durch diese kein neutrales Bild der durch den Vorstand selbst verursachten Risiken erwartet werden kann (und es ist naheliegenderweise der Vorstand, der durch seine Entscheidungen die Risikoposition eines Unternehmens hauptsächlich bestimmt).

Auch die Interne Revision als Third Line of Defense ist zumeist disziplinarisch dem Vorstand zugeordnet und ist damit in einer gleichen Konstellation, die problematisch wird, wenn die risikospezifischen Interessen des Vorstands von denjenigen der Aktionäre abweichen sollten. Jedoch lassen sich durch bestehende zusätzliche Reportinglines zum Aufsichtsrat bzw. Prüfungsausschuss diese Probleme reduzieren.[40]

Der Vorstand als zusätzliche Verteidigungslinie ist nur dann für die Aktionäre im Sinne eines guten Risikomanagements hilfreich, wenn die Interessenslage gleichgerichtet ist und die unternehmerischen Entscheidungen in Abstimmung oder

35 Siehe Angermüller et al., abrufbar unter https://www.idw.de/blob/121892/0749c64f54f80bdee6c7f29d837a3f93/down-idweps340nf-gem-stn-hochschullehrer-rm-data.pdf (Abruf: 19.10.2021); Schmidt/Henschel, ZIR 2021 S. 182–194.

36 Siehe z. B. Gleißner, Grundlagen des Risikomanagement 2017; Romeike/Hager, Erfolgsfaktor Risiko-Management 4.0, 2020; Vanini/Rieg, Risikomanagement, 2020.

37 Dies zeigen die in den Abschnitten 3.1 und 3.2 angegebenen empirischen Studien, z. B. von Deloitte (2020).

38 Siehe dazu Köhlbrandt et al., CF 2020 S. 248–258.

39 Siehe Gleißner, Grundlagen des Risikomanagements, 2017, S. 130.

40 Siehe Eulerich, ZIR 2012 S. 292–298; Regierungsentwurf zum FISG, abrufbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Finanzmarktintegritaet.html (Abruf: 19.10.2021).

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Die heute primär auf die Risikofrüherkennung ausgerichteten Systeme sollten erweitert werden zu entscheidungsorientierten Risikomanagementsystemen. ◀

mindestens im Interesse des Aufsichtsrats bzw. der Anteilseigner erfolgen.

Grundsätzlich kann man aufgrund der Besetzung von einer an den Interessen der Aktionäre orientierten Betrachtung von Risiko und Risikomanagementsystem auf Seiten des Aufsichtsrats ausgehen. Dieser steht aber vor dem Problem, dass er oft nur Informationen über die Risikolage des Unternehmens erhält, die vom Vorstand freigegeben werden. Auch Vorlagen über anstehende unternehmerische Entscheidungen, die bei zustimmungspflichtigen Geschäften vom Aufsichtsrat freigegeben werden müssen, zeigen das Bild aus Sicht des Vorstands. Noch problematischer wird die Konstellation, wenn Vorstand und Aufsichtsrat nicht unabhängig voneinander sind und entgegen der gesetzlichen Intension ein starker Vorstand die Besetzung des Aufsichtsrats, der seine Arbeit kontrollieren soll, beeinflussen kann oder beide Organe in enger Abstimmung der Mitglieder, aber nicht im Interesse der Anteilseigner agieren.

Es bleibt der Abschlussprüfer als Interessensverwalter der Aktionäre. Aber auch hier ist die Konstellation nicht einfach. Will man erklären, warum so viele Risikomanagementsysteme deutscher Unternehmen die gesetzlichen Anforderungen nicht erfüllen, sieht man die oben skizzierte Problemlage: Die wirtschaftlichen Interessen der Abschlussprüfer und die bestehende Wettbewerbssituation könnte erklären, dass der Abschlussprüfer Konflikte mit seinem Auftraggeber eher vermeiden möchte. Fehlende fachliche Kompetenzen, fehlende Budgets, Angst vor Konflikten mit dem Mandanten und die möglicherweise fehlende Sorge, dass Defizite bei der Prüfung der Risikoaggregationsverfahren für den Wirtschaftsprüfer selbst zu einem Problem werden können, mögen – in irgendeiner Kombination – erklären, warum die zur Erfüllung der gesetzlichen Anforderungen aus den §§ 91 und 93 AktG so zentralen Verfahren der Risikoaggregation noch immer keinen Prüfungsschwerpunkt darstellen.[41] Mögliche Ursachen für Prüfungsdefizite sind zusammenfassend:

- Fehlende Kompetenz bei der Prüfung der Methoden der Risikoaggregation
- Mangel an Budget
- Vermeidung von Konflikten mit Mandanten
- Fehlende Sanktionierung der Wirtschaftsprüfer

Als Fazit ist festzuhalten, dass aus fachlichen Defiziten insbesondere aber auch persönlichen Interessen der involvierten Personen momentan nicht gewährleistet ist, dass die Risiken eines Unternehmens im Sinne der Aktionäre als Eigentümer und Prinzipal gesteuert werden. Man kann leicht Fälle zeigen, in denen es nicht im Interesse der Vorstände ist, auf eine mögliche bestandsgefährdende Entwicklung rechtzeitig hinzuweisen. Man kann auch verstehen, dass Vorstände die mit einer unternehmerischen Entscheidung verbundenen Risiken nicht neutral darstellen und im Entscheidungskalkül berücksichtigen. Infolge der Unterstellung des IKS, des Risikomanagements und der Internen Revision unter den Vorstand kann man nicht erwarten, dass diese drei Bausteine des TLoD erreichen können, dass in einem Unternehmen konsequent orientiert an den Interessen der Eigentümer orientiert mit Risiken umgegangen wird. Wie gezeigt, ergeben sich in der momentanen Struktur auch Probleme auf Ebene von Aufsichtsrat und Abschlussprüfer. Aufgrund von eingeschränkter Informationsverfügbarkeit und wirtschaftlichen Interessen ist hier auch nicht gewährleistet, dass Risiken im Sinne der Aktionäre gehandhabt werden. Auch wenn es für die hier bestehenden Probleme keine einfache Lösung gibt, kann man aus der obigen Diskussion von Problemfeldern doch einige Verbesserungspotenziale ableiten. Diese werden im nachfolgenden Abschnitt zusammengefasst.

4. Stärkung der Leistungsfähigkeit des Risikomanagements im Interesse der Aktionäre

Die folgenden Diskussionspunkte können helfen, das Risikomanagement von Unternehmen im Interesse der Aktionäre zu verbessern.

1. Die heute primär auf die Risikofrüherkennung ausgerichteten Systeme sollten erweitert werden zu entscheidungsorientierten Risikomanagementsystemen (siehe dazu DIIR RS Nr. 2 und COSO ERM). Auf diese Weise ließe sich regeln, dass schon bei der Vorbereitung unternehmerischer Entscheidungen die mit diesen verbundenen Risiken durch eine neutrale Stelle, zum Beispiel durch den Aufsichtsrat, analysiert und dokumentiert werden (dies ist genau die Intention des DIIR Revisionsstandards Nr. 2 von 2018). Die Abschlussprüfung könnte durch einen IDW Prüfungsstandard explizit diese Anforderung aus § 93 AktG zum Prüfungsgegenstand machen.
2. Das Risikomanagement und die Interne Revision müssen gestärkt werden. Einher mit einer Verstärkung der personellen Ausstattung sollte dabei ein Ausbau der Fähigkeiten gehen, um insbesondere die bisher bestehenden Defizite im Bereich quantitativer Risikoanalyse und Risikoaggregation zu beseitigen. Zudem sollte gewährleistet sein, dass sowohl die Interne Revision als auch das Risikomanagement gegenüber Vorstand und Aufsichtsrat gemeinsam verantwortlich sind. Neben einem regelmäßigen Reporting an den Aufsichtsrat wäre es hier zur Absicherung der entsprechenden Person auch hilfreich, wenn Einstellungen und Entlassungen der hier verantwortlich tätigen Mitarbeiter nur mit Zustimmung des Aufsichtsrats möglich wäre.
3. Die bisher bestehenden potenziellen Schwächen der Abschlussprüfung im Risikofrüherkennungssystem sollten daher beseitigt werden. Einerseits sollte die Prüfung dabei auch auf den Bereich der Anforderungen ausgeweitet werden, für die es seitens des Instituts der deutschen Wirtschaftsprüfer (IDW) bisher keinen Prüfungsstandard gibt. Es sollte also untersucht werden, ob im Unternehmen geeignete Systeme implementiert sind, die gewährleisten, dass bei der Vorbereitung unternehmerischer Entscheidungen angemessene Informationen vorliegen, insbesondere auch Risikoinformationen (und diese entsprechenden Regelungen auch eingehalten werden). Zudem muss er-

41 Vgl. Gleißner, RWZ 2020 S. 273–280.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13

Lizenziert für Herrn Prof. Dr. Werner Gleißner.
Die Inhalte sind urheberrechtlich geschützt.

▶ Die Corporate-Governance-Diskussion wird zu stark dominiert durch die Perspektiven einzelner Akteure, Verbände oder Gruppen. ◀

reicht werden, dass die Wirtschaftsprüfer konsequent die hierfür erforderlichen Methoden, etwa der Risikoanalyse und Risikoaggregation, prüfen und hier bestehende Defizite auch aufzeigen.

Gewisse Verbesserungen ergeben sich bereits durch StaRUG (Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen) seit dem 1.1.2021. Die neue Verpflichtung für die Geschäftsleiter aller haftungsbeschränkten Gesellschaften zur Initiierung von Gegenmaßnahmen bei einer erkannten bestandsgefährdenden Entwicklung (§ 1) verzahnt Risikofrüherkennungssystem und Krisenpräventionsmaßnahmen. Zumindest bei einer sich abzeichnenden bestandsgefährdenden Entwicklung sind mögliche Maßnahmen zur Krisenvermeidung zu planen und es ist eine Entscheidung über deren Durchführung erforderlich. Da eine derartige Entscheidung durchgängig als unternehmerische Entscheidung i. S. d. § 93 AktG anzusehen ist, werden nun auch die §§ 91 und 93 AktG über das StaRUG miteinander verknüpft. Offenkundig ist zu dokumentieren, welche Veränderung des Risikoumfangs – des Grads der Bestandsgefährdung – durch die Gegenmaßnahmen erreicht werden soll

Weitere Verbesserungen können durch das FISG (Gesetz zur Stärkung der Finanzmarktintegrität) erreicht werden. So ist die Forderung nach einem angemessenen und wirksamen Risikomanagement im neuen § 91 Abs. 3 AktG sinnvoll. Dieses soll sich mit allen wesentlichen Risiken befassen, auch mit deren adäquater Bewältigung, und bei unternehmerischen Entscheidungen mitwirken.[42] Die Früherkennung möglicher bestandsgefährdender Entwicklungen setzt ein adäquates Risikofrüherkennungssystem voraus. Die Stärkung des Risikomanagements soll erreicht werden, indem die Verantwortlichen für das Risikomanagement eine direkte Reportinglinie zum Aufsichtsrat bzw. dessen Prüfungsausschuss erhalten. Dies ist wesentlich, damit der Aufsichtsrat als wesentliches ergänzendes Element der Lines of Defense[43] auch Informationen erhält, die ein Vorstand möglicherweise aus eigenem Interesse „unterdrücken" möchte. Dies können beispielsweise durch den Vorstand selbst verursachte Risiken sein[44], Risiken, deren hohe Relevanz ein Vorstand nicht angeben möchte oder eben auch methodische Schwächen im Risikomanagement selbst (z. B. bei der Risikoaggregation). Auch die Änderung der Rolle des Abschlussprüfers und die Erhöhung der Haftung spielen hier eine Rolle.[45] Es wäre auch klarzustellen, dass Anforderungen aus den §§ 91 *und* 93 AktG sowie § 1 StaRUG für das Risikomanagement Gegenstand der Prüfung durch den Abschlussprüfer sein müssen.

Unternehmensskandale wie der Fall Wirecard machen deutlich, dass trotz gesetzlicher und quasigesetzlicher Vorgaben die tatsächliche Risikoposition von Unternehmen mit der durch den Kapitalmarkt bewerteten Situationen nicht immer übereinstimmen. Natürlich ist Wirecard aufgrund des Top-Management-Frauds ein Sonderfall. Allerdings veranschaulicht dieses Beispiel, wie alle der zuvor dargestellten Verteidigungslinien nicht mehr agieren können bzw. nicht mehr leistungsfähig sind, wenn z. B. der Vorstand Risiken verschleiert.

Die Corporate-Governance-Diskussion wird vor diesem Hintergrund noch immer zu stark dominiert durch die Perspektiven einzelner Akteure, Verbände oder Gruppen. Gute Corporate Governance funktioniert nur dann, wenn alle Verteidigungslinien innerhalb und außerhalb des Unternehmens ineinandergreifen, mit angemessenen Mitteln ausgestattet und mit verantwortungsvollen Personen besetzt sind. Denn nur durch eine gute Corporate Governance und die damit einhergehende Abstimmung von Führung und Überwachung können sich Unternehmen im Interesse der Aktionäre und der übrigen Stakeholder weiterentwickeln und langfristig Wert generieren.

42 Berger et al., abrufbar unter https://www.risknet.de/themen/risknews/betriebswirtschaftliche-stellungnahme-zu-fisg-und-risikomanagement/ (Abruf 19.10.2021).
43 Gleißner/Theisen, Der Aufsichtsrat 2016 S. 85–87, sprechen von der 4. Line of Defense.
44 Wie Fraud-Risiken, siehe Fall Wirecard.
45 Siehe dazu auch kritisch die IDW-Stellungnahme zum FISG, abrufbar unter https://www.idw.de/blob/128450/6029dfe719016e6b4125e2151ee79a2c/down-fisg-rege-data.pdf (Abruf 19.10.2021).

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2021 (http://www.zcgdigital.de) - 06.12.2021 10:13