Veröffentlicht in

Der Betrieb

Heft 46/2021

Berger, T. / Ernst, D. / Gleißner, W. / Hofmann, P. / Meyer, M. / Schneck, O. / Ulrich, P. / Vanini, U. (2021):

„Die Prüfung von Risikomanagementsystemen und die Defizite des IDW Prüfungsstandards 340“,

S. 2709 – 2714

Abschlussprüfung »DB1356932

Prof. Dr. Thomas Berger, Stuttgart / Prof. Dr. Dr. Dietmar Ernst, Nürtingen-Geislingen / Prof. Dr. Werner Gleißner, Dresden / Prof. Dr. Kay H. Hofmann, Osnabrück / Prof. Dr. Matthias Meyer, Hamburg / Prof. Dr. Ottmar Schneck, Riedlingen / Prof. Dr. Patrick Ulrich, Aalen / Prof. Dr. Ute Vanini, Kiel

Die Prüfung von Risikomanagementsystemen und die Defizite des IDW Prüfungsstandards 340

Prof. Dr. Thomas Berger, Duale Hochschule BW Stuttgart; **Prof. Dr. Dr. Dietmar Ernst**, Hochschule für Wirtschaft und Umwelt (HfWU) Nürtingen-Geislingen; **Prof. Dr. Werner Gleißner**, Technische Universität Dresden; **Prof. Dr. Kay H. Hofmann**, Hochschule Osnabrück; **Prof. Dr. Matthias Meyer**, Technische Universität Hamburg; **Prof. Dr. Ottmar Schneck**, SRH Fernhochschule, Riedlingen; **Prof. Dr. Patrick Ulrich**, Hochschule Aalen – Technik und Wirtschaft; **Prof. Dr. Ute Vanini**, Fachhochschule Kiel.
Kontakt: autor@der-betrieb.de

Der neue IDW Standard zur Prüfung von Risikofrüherkennungssystemen (IDW PS 340) stellt einen deutlichen Fortschritt gegenüber dem Vorgänger dar, z.B. durch die Betonung der Bedeutung von Risikoaggregation und Risikotragfähigkeit. Einige Schwächen können aber dazu führen, dass Abschlussprüfer – wie bisher – Risikofrüherkennungssysteme akzeptieren, die schwerwiegende Mängel aufweisen. Diese können z.B. dazu führen, dass unvertretbare methodische Schwächen von Unternehmen bei der Aggregation von Risiken und Risikoanalyse oder der Vorbereitung von unternehmerischen Entscheidungen (i.S.d. Business Judgement Rule) ignoriert werden. Es wird zudem daran erinnert, dass bei einer Prüfung nach IDW PS 340 die neuen Anforderungen an das Risikomanagement aus 2021 noch nicht berücksichtigt werden (§ 1 StaRUG und § 91 Abs. 3 AktG).

I. Einführung

Bei einer nicht sicher vorhersehbaren Zukunft sind die Fähigkeiten eines Unternehmens im Umgang mit Chancen und Gefahren (Risiken) von grundlegender Bedeutung für den Unternehmenserfolg. Es ist offensichtlich wichtig, schon bei der Vorbereitung einer „unternehmerischen Entscheidung" (§ 93 AktG) zu wissen, welche Veränderung des Risikoumfangs sich durch diese ergibt. Die zentrale Aufgabe des Risikomanagements ist es, die Existenz des Unternehmens abzusichern und risikobedingte Krisen nicht nur früh zu erkennen, sondern präventive sowie reaktive Maßnahmen zu planen und bei Bedarf diese anzustoßen. Überraschende Insolvenzen, wie die von Euromicron oder Vapiano, sowie empirische Studien deuten jedoch darauf hin, dass in den Risikomanagementsystemen deutscher Unternehmen, trotz der zentralen ökonomischen Bedeutung, gravierende Schwächen bestehen.[1]

Um zumindest sinnvolle „Mindestanforderungen" zu erfüllen, gibt es gesetzliche Vorgaben, die in den §§ 91 und 93 AktG geregelt sind und deren Einhaltung bei börsennotierten Unternehmen durch die Abschlussprüfer zu untersuchen ist. Diese orientieren sich dabei an Standards, insb. am IDW Prüfungsstandard (PS) 340, der im Juni 2020 als IDW PS 340 n.F. in überarbeiteter Form veröffentlicht wurde. Trotz der vorgeschriebenen Prüfungen werden gravierende Defizite im Risikomanagement vieler Unternehmen jedoch häufig nicht aufgedeckt.[2]

Der vorliegende Beitrag fasst die Eckpunkte des neuen IDW PS 340 n.F. zusammen, der wesentliche Verbesserungen im Vergleich zum alten Standard aufweist. Jedoch lässt dieser bei der Prüfung von Risikofrüherkennungssystemen weiterhin Spielräume zu, die dazu führen können, dass trotz Testats der Abschlussprüfer Unternehmen die gesetzlichen Anforderungen nicht erfüllen. Auf diese für Aktionäre und Gläubiger problematischen „Lücken" wird im Folgenden näher eingegangen. Der Beitrag schließt mit weiterführenden Überlegungen und Empfehlungen zur weiteren Anpassung bestimmter Formulierungen.[3]

II. Rechtliche Anforderungen und die Entwicklung im regulatorischen Umfeld

Seit Inkrafttreten des Kontroll- und Transparenzgesetzes (KonTraG) 1998[4] ist es die primäre Aufgabe des Risikomanagements mögliche „bestandsgefährdende Entwicklungen" (§ 91 AktG) früh zu erkennen. Neben bestandsgefährdenden Einzelrisiken sind dabei insb. Kombinationseffekte von Einzelrisiken zu untersuchen, die i.d.R. Krisen oder gar Insolvenzen auslösen können, was eine quantitative Risikoanalyse sowie Risikoaggregation mittels stochastischer Simulation (Monte-Carlo-Simulation) erfordert.[5]

Die wesentlichen Anforderungen an ein Risikofrüherkennungssystem fasst auch schon seit dem Jahr 1998 der IDW PS 340 zusammen, der auch auf die zentrale Rolle einer Risikoquantifizierung und Risikoaggregation verweist. Die Bedeutung der Risikoaggregation wird auch in der Überarbeitung, nämlich im IDW PS 340 n.F. noch stärker betont. Mit dem IDW PS 981 für die freiwillige Prüfung von Risikomanagementsystemen gibt es seit 2017 einen ergänzenden Standard, der sich auch mit Risikobewältigung befasst und vor allem den Konzepten für die Messung von Risikotragfähigkeit, Risikotoleranz und Risikoappetit einen hohen Stellenwert beimisst.

Eine weitere zentrale Anforderung an das Risikomanagement wird jedoch in keinem dieser Regelwerke thematisiert: Die notwendige entscheidungsorientierte Ausrichtung von Risikomanagementsystemen. Gemeint ist damit ein neues Paradigma des Risikomanagements, demzufolge das Risi-

1 Siehe z.B. Ulrich, ZfKE 2018 S. 13-33; Schwaiger/Brandstätter, CM 2/2020 S. 73 ff.; Köhlbrandt/Gleißner/Günther, CF 2020 S. 248 ff.; Deloitte, Benchmarkstudie Risikomanagement 2020. Ausgestaltung von Risikomanagementsystemen nach IDW PS 981 und IDW PS 340 n.F., abrufbar unter https://hbfm.link/11312 (Abruf: 19.10.2021).

2 Siehe dazu Köhlbrandt/Gleißner/Günther, CF 2020 S. 248-258; und Deloitte, a.a.O. (Fn. 1).

3 Siehe Angermüller et al., Gemeinsame Stellungnahme zum IDW EPS 340, abrufbar unter https://hbfm.link/6882 (Abruf: 19.10.2021).

4 BGBl. I 1998 S. 786.

5 Siehe vertiefend Gleißner, Grundlagen des Risikomanagements, 3. Aufl. 2017; und ders., WPg 2017 S. 158 ff.; sowie Romeike, CFO aktuell 2018 S. 167 ff.; und Romeike/Hager, Erfolgsfaktor Risikomanagement 4.0: Methoden, Prozess, Organisation und Risikokultur, 4. Aufl. 2020.

komanagement dazu beitragen soll, bei der Vorbereitung unternehmerischer Entscheidungen die dafür notwendigen Informationen zu liefern. Speziell sollte durch eine Risikoanalyse aufgezeigt werden, wie sich der Umfang an Chancen und Gefahren (Risiken) infolge einer Entscheidung verändern würde und welchen Einfluss dies auf die Wertschöpfung des Unternehmens hätte. Ein solches „entscheidungsorientiertes Risikomanagement" findet man vor allem in der neuen Version des 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 sowie den Unternehmenswert gegeneinander abgewogen und somit Handlungsoptionen risikogerecht bewertet werden. Dies geht einher mit einer engeren Verknüpfung von Risikomanagement und Controlling[6] sowie einer Verzahnung des Risikomanagements mit der Unternehmensstrategie.[7]

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. Gem. der sog. Business Judgement Rule (BJR) in § 93 AktG muss ein Geschäftsleiter bei der Vorbereitung „unternehmerischer Entscheidungen", z.B. bezüglich einer Investition, Akquisition oder Strategie-Veränderung, beweisbar „angemessene Informationen" vorliegen haben (eine analoge Anforderung gilt für GmbH-Geschäftsführer). Da der anerkannte Stand von Wissenschaft und Technik zu berücksichtigen ist,[8] muss eine entscheidungsvorbereitende Risikoanalyse erfolgen, die auf einer fundierten Methodik basiert.

Problematisch ist allerdings, wenn nach einer unternehmerischen Entscheidung Planabweichungen eintreten, die nicht auf in der Entscheidungsvorlage genannte Risiken zurückzuführen sind oder wenn diese in einem Umfang auftreten, der durch die entscheidungsvorbereitende Risikoanalyse nicht erklärt werden kann. Dies kann als Indiz dafür gesehen werden, dass die Entscheidungsvorlage grundlegende Schwächen aufgewiesen hat und möglicherweise eine Sorgfaltspflichtverletzung des Vorstands vorliegt, die der Aufsichtsrat – gestützt auf die der „unternehmerischen Entscheidung" zugrunde liegenden Entscheidungsvorlage – zu untersuchen hat.

Im Rahmen der Jahresabschlussprüfung wendet der Abschlussprüfer den risikoorientierten Prüfungsansatz i.S.d. IDW PS 261 n.F. an (Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken)[9], um seine Prüfung effizient planen und durchführen zu können. Im Gegensatz zum traditionellen Prüfungsansatz, der insb. auf einer Beurteilung des Internen Kontrollsystems (IKS) fußt, wird im Rahmen des risikoorientierten Prüfungsansatzes die gesamte Kontrollstruktur (Control Structure) beurteilt (z.B. Identifikation von Umfeld- oder Branchenrisiken).[10]

III. Zustand der Risikomanagementsysteme deutscher Unternehmen: eine Übersicht

Bevor der IDW PS 340 n.F. näher betrachtet wird, lohnt ein Blick auf den Status der Risikomanagementsysteme deutscher Unternehmen. Es ist nämlich festzustellen, dass trotz der seit 1999 regelmäßig durchgeführten Prüfung der Risikofrüherkennungssysteme durch den Abschlussprüfer Studien regelmäßige gravierende Defizite aufzeigen.[11]

Die aktuelle „Benchmark-Studie"[12] von Deloitte zeigt, dass 43% der befragten Unternehmen die Gesamtrisikopositionen auf „Basis der Addition von Schadenserwartungswerten von Risiken" bestimmen. Dies ist methodisch nicht zu halten, wenn man dieses Vorgehen als Verfahren für die Risikoaggregation zur Früherkennung möglicher „bestandsgefährdender Risiken" auffasst. Folgendes einfaches Beispiel zeigt, dass eine Risikoaggregation über die Berechnung des Gesamtschadenserwartungswerts gar nicht möglich ist.

Beispiel:

Angenommen ein Unternehmen mit einem Eigenkapital i.H.v. 50 GE hat genau zwei Risiken: R1 und R2. R1 hat eine erwartete Schadenshöhe von 200 GE und eine Eintrittswahrscheinlichkeit von 10%. R2 eine erwartete Schadenshöhe von 100 GE und eine Eintrittswahrscheinlichkeit von 20%. Der Gesamtschadenserwartungswert ist damit 200 GE × 10% + 100 GE × 20% = 40 GE. Dieser ist zwar niedriger als das angenommene Eigenkapital, dennoch tritt eine Insolvenz durch Überschuldung auf, wenn auch nur eines der beiden Risiken eintritt und erst recht, wenn beide gemeinsam eintreten.

Die Summe der Schadenserwartungswerte der Risiken ist für die Beurteilung der „Bestandsgefährdung" somit irrelevant und dieses Verfahren kein geeignetes Aggregationsverfahren, da es nicht in der Lage ist, mögliche „bestandsgefährdende Entwicklungen" i.S.d. § 91 AktG aus Kombinationseffekten von Risiken zu identifizieren. Ein Risikofrüherkennungssystem, das dieses Verfahren nutzt, erfüllt die gesetzlichen Anforderungen daher nicht und darf seitens der Abschlussprüfer eigentlich nicht akzeptiert werden.

Dass in der Studie von Deloitte aber 43% der Unternehmen diese Verfahren angeben und weitere 25% darauf verweisen, überhaupt keine Risikoaggregation vorzunehmen, kann als Indiz für eine nicht vollständige Umsetzung der Anforderungen aus § 91 AktG interpretiert werden. Dazu kommen weitere Defizite von Risikomanagementsystemen, wie z.B.:[13]

6 Siehe z.B. Vanini/Leschenko, CM 1/2017 S. 36 ff.
7 Siehe z.B. Gleißner, GRC aktuell 4/2019 S. 1-6; oder Hofmann/Fink, CM 3/2019 S. 36 ff.
8 Vgl. hierzu Scherer, CCZ 6/2012; sowie Romeike, AR 2014 S. 70-72; und Romeike/Hartmann, ZfgK 2015 S. 227 ff.
9 Vgl. IDW PS 261 n.F., Rn. 10-12, FN-IDW 2012 S. 239 ff.
10 Vgl. Freidank, Unternehmensüberwachung. Die Grundlagen betriebswirtschaftlicher Kontrolle, Prüfung und Aufsicht, 2012, S. 282 ff.