

# 04.21

# ZIR

## Zeitschrift Interne Revision

56. Jahrgang  
August 2021  
Seiten 161 – 204

[www.ZIRdigital.de](http://www.ZIRdigital.de)

Herausgeber:

## DIIR

Deutsches Institut für  
Interne Revision e.V.

### Fachzeitschrift für Wissenschaft und Praxis

#### Standards · Regeln · Berufsstand

Der Revisor 2025 164

*Ralf Herold*

Die Implementierungsleitlinien 167

*Michael Bünis*

StARUG, IDW PS 340 und DIIR Revisionsstandard Nr. 2 173

*Prof. Dr. Werner Gleißner*

#### Management · Best Practice · Arbeitshilfen

Die Überwachung des Tax-Compliance-Management-  
Systems 178

*Bernd Peter · Marc Budahn*

#### Wissenschaft · Forschung

Prüfung des Überwachungssystems gemäß § 91  
Abs. 2 AktG 182

*Alexander Schmidt · Prof. Dr. Thomas Henschel*

PROF. DR. WERNER GLEISSNER

# StaRUG, IDW PS 340 und DIIR Revisionsstandard Nr. 2

## Lücken der Abschlussprüfung und Implikationen für die Interne Revision

Die Vorstände vieler Unternehmen sind im Bereich Risikomanagement primär bemüht, dass der Abschlussprüfer bei einer Prüfung orientiert am neuen IDW PS 340 n.F. (2020) keine schwerwiegenden Mängel feststellt und der Bestätigungsvermerk im Jahresabschluss nicht eingeschränkt wird.<sup>1</sup> Viele Vorstände schließen aus einer bestandenen Prüfung nach IDW PS 340, dass damit die gesetzlichen Anforderungen an das Risikomanagement erfüllt seien. Aus dem Hinweis des Instituts der deutschen Wirtschaftsprüfer (IDW), demzufolge Jahresabschlüsse erst ab 2021 nach den präzisierten Anforderungen des IDW PS 340 n.F. (2020) geprüft werden müssen, wird zudem abgeleitet, dass die neuen Anforderungen, zum Beispiel zu Risikoaggregation und Risikotragfähigkeit, erst ab 2021 verbindlich seien. Beide Einschätzungen sind falsch, was nachfolgend erläutert wird.



Prof. Dr. Werner Gleißner  
ist Vorstand der Future-  
Value Group AG und  
Professor für BWL,  
insbesondere Risiko-  
management, an der  
TU Dresden.

### 1. Gesetzliche Anforderungen an das Risikomanagement von Unternehmen und Gegenstand des IDW PS 340 n.F. (2020)<sup>1</sup>

Der Sachverhalt ist insbesondere für die Arbeit der Internen Revision wichtig, was nachfolgend näher erläutert wird.

1. Eine Prüfung des Risikofrüherkennungssystems nach IDW PS 340 ist kein (wissenschaftliches) Gutachten im Hinblick auf die Erfüllung von gesetzlichen Anforderungen an das Risikomanagement<sup>2</sup> und keine Garantie des Abschlussprüfers, dass die gesetzlichen Anforderungen erfüllt werden. Der Abschlussprüfer hat eine Vielzahl von Spielräumen bei der Prüfung und kann wichtige Aspekte, zum Beispiel zur Methode der Risikoaggregation, auslassen oder nur cursorisch prüfen. Entsprechend zeigen auch empirische Studien regelmäßig, dass gesetzliche Mindestanforderungen in den Unternehmen nicht erfüllt sind.<sup>3</sup> Auch kann man in Gutachten meist sehr

leicht beweisen, dass gesetzliche Anforderungen nicht erfüllt werden.<sup>4</sup>

Eine Prüfung nach IDW PS 981 hat gar keinen konkreten und fixen Bezug zu den gesetzten Anforderungen. Prüfungsschwerpunkte nach IDW PS 981 sind prinzipiell in Abstimmung zwischen Mandanten und Abschlussprüfer recht frei wählbar und können zum Beispiel auch betriebswirtschaftlich interessante Themenfelder umfassen, für die es gar keine gesetzlichen Grundlagen gibt (zum Beispiel Effektivität von Risikobewältigungsmaßnahmen).

2. Eine Prüfung gemäß IDW PS 340 umfasst, wie der Standard auch klar formuliert, nur die Anforderung an das Risikofrüherkennungssystem gemäß § 91 AktG. Andere gesetzliche Anforderungen sind nicht Prüfungsgegenstand und werden entsprechend nicht betrachtet. Dies betrifft einerseits zum Beispiel die Implikationen von § 93 AktG und natür-

1 Siehe § 316 ff im HGB zur Abschlussprüfung.

2 Siehe dazu auch die Stellungnahme Angermüller, N.O. et al. (2020) und Berger, T. et al. (2021).

3 Siehe z.B. Ulrich, P. et al. (2018); Link, M. et al. (2021); Köhlerbrandt, J. et al. (2020).

4 Siehe zur Methode Gleißner, W. (2020a); Gleißner, W./Hofmann (2020) sowie Wolfrum, M. (2020) mit den Fallbeispielen Gerry Weber und Euromicron.

lich die Anforderungen aus StaRUG, gültig ab 1. Januar 2021, die zum Zeitpunkt der Veröffentlichung des IDW PS 340 n.F. (2020) noch nicht relevant waren (siehe dazu 3.).

Die Implikationen der Business Judgement Rule aus § 93 AktG für das Risikomanagement werden zwar im DIIR Revisionsstandard Nr. 2 aufgegriffen, nicht aber im IDW PS 340. Gemäß § 93 AktG sind bei unternehmerischen Entscheidungen zur Vermeidung einer Sorgfaltspflichtverletzung angemessene Informationen zu belegen (die Beweislast dafür liegt beim Vorstand). Da unternehmerische Entscheidung unsichere Auswirkungen haben, sind in der Entscheidungsvorlage insbesondere

**Viele Vorstände schließen aus einer bestanden Prüfung nach IDW PS 340, dass damit die gesetzlichen Anforderungen an das Risikomanagement erfüllt seien. Diese Einschätzung ist falsch.**

re die Implikationen der Entscheidung für den Risikoumfang zu zeigen.<sup>5</sup> Dies bedeutet, dass Risikoanalysen schon bei der Vorbereitung von Entscheidung einzubeziehen sind. Konsequenterweise fordert der DIIR Revisionsstandard Nr. 2 die Einbeziehung des Risikomanagements bei der Vorbereitung unternehmerischer Entscheidungen.<sup>6</sup> Ob und inwieweit das Risikomanagement im Allgemeinen und Risikoanalysen im Speziellen bei der Vorbereitung unternehmerischer Entscheidungen tatsächlich einbezogen werden, wird bei einer Abschlussprüfung nach IDW PS 340 (bisher) nicht untersucht. Ob bei einer zukünftigen Überarbeitung der IDW PS 340 auch die Anforderung aus § 93 AktG berücksichtigt wird, oder hier zum Beispiel ein eigener Prüfungsstandard entsteht, ist offen.

3. Auch die Implikationen aus dem seit 1. Januar 2021 gültigen StaRUG (Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen) werden durch den Abschlussprüfer nicht geprüft.<sup>7</sup> Dies ist natürlich

5 Siehe Graumann, M. et al. (2009); Graumann, M. (2014); Gleißner, W. (2019a und 2021); RMA (2019) und ICV (2021).

6 Siehe Gleißner, W./Kimpel, R. (2019) und die ähnlichen Implikationen der COSO ERM, z. B. bei Hunziker, S. (2019).

7 Siehe zum StaRUG, z. B. Gleißner, W./Haarmeyer, H. (2019); Kühne, F./Lienhard, M. (2020); Braun, E. (2021); Gleißner, W./Lienhard, M./Kühne, F. (2021).

auch klar, da das StaRUG erst nach der Veröffentlichung des IDW PS 340 fertiggestellt wurde und in Kraft getreten ist. Die Implikationen speziell aus § 1 StaRUG für das Krisen- und Risikofrüherkennungssystem, auch von Aktiengesellschaften, sind jedoch beachtlich. Zunächst wird in enger Anlehnung an § 91 AktG gefordert, dass juristische Personen bestandsgefährdende Entwicklungen<sup>8</sup> früh erkennen müssen. Die direkte Spiegelung der Anforderungen aus § 91 AktG erreicht, dass die betriebswirtschaftlichen Implikationen dieser Anforderungen durch das umfangreiche Schrifttum und die seit 1998 entwickelten Risikomanagementstandards bekannt sind. Insbesondere ist klar, dass eine Risikoanalyse und Risikoaggregation erforderlich sind, um die sich aus diesen ergebenden bestandsgefährdende Entwicklungen zu erkennen.<sup>9</sup> Krisen sind das Resultat der Realisierung bestehender Risiken. Und da im Allgemeinen Kombinationseffekte von Einzelrisiken Krisen auslösen, ergibt sich die zentrale Bedeutung der Risikoaggregation, wie sie auch im neuen IDW PS 340, im DIIR Revisionsstandard Nr. 2 und im wissenschaftlichen Schrifttum betont wird.<sup>10</sup> Auch für Aktiengesellschaften neu [aber (noch) nicht Gegenstand der Abschlussprüfung] sind zwei weitere Folgen des StaRUG:

- a) Die Früherkennung bestandsgefährdender Entwicklungen fordert StaRUG nun von allen juristischen Personen, das heißt neben Aktiengesellschaften speziell auch GmbHs. In der Konsequenz müssen auch die Geschäftsleiter von GmbHs, die Teil eines Konzerns sind, sich selbst mit der Risikoanalyse und der Früherkennung bestandsgefährdender Entwicklungen befassen. Aus Sicht des Risikomanagements eines Konzerns (einer Aktiengesellschaft) bedeutet dies, dass das Risikomanagement konsequent auch bei der Geschäftsleitung von Tochtergesellschaften zu verankern ist. Die Geschäftsleitung trägt die Verantwortung, die nicht auf ein übergeordnetes Risikomanagement des Konzerns delegierbar ist (und trägt hier persönliche Haftungsrisiken).
- b) Im Gegensatz zum Kontroll- und Transparenzgesetz (KonTraG) beziehungsweise

8 Gleißner, W. (2017c).

9 Angermüller, N. O. et al. (2020); Romeike, F. (2008); Gleißner, W. (2017b).

10 Siehe dazu Angermüller, N. O. et al. (2020).

§ 91 AktG reicht seit dem 1. Januar 2020 die Schaffung von Transparenz über das Bestehen bestandsgefährdender Entwicklungen (beziehungsweise deren Wahrscheinlichkeit) nicht mehr aus. Gefordert wird nun, ab einem kritischen Grad der Bestandsgefährdung geeignete Gegenmaßnahmen zur Krisenabwehr zu initiieren. Ein StaRUG-konformes Risikomanagementsystem muss dem Rechnungstragen und zum Beispiel Schwellenwerte festlegen (und die Überschreitung überwachen), ab denen die geforderten Gegenmaßnahmen initiiert werden müssen. Solche Gegenmaßnahmen umfassen auch, wenn auch nicht nur, Verstärkung von Risikobewältigungsmaßnahmen und damit wird auch die Risikosteuerung und insbesondere die Krisenabwehr zum gesetzlichen Aufgabenfeld.

Ergänzend ist zu beachten, dass die Entscheidung über die Gegenmaßnahmen regelmäßig eine unternehmerische Maßnahme im Sinne von § 93 AktG darstellt.<sup>11</sup> Damit gilt hier speziell auch das unter 2. zum entscheidungsorientierten Risikomanagement Erläuterte.

4. Entgegen des Eindrucks trifft es nicht zu, dass die neu im IDW PS 340 von 2020 formulierten Anforderungen erst ab 2021 durch die Unternehmen zu erfüllen sind. Die gesetzlichen Grundlagen haben sich 2020 nicht verändert. Die im IDW PS 340 formulierten neuen Anforderungen, zum Beispiel im Bereich Risikoaggregation, sind jetzt und schon seit längerer Zeit für die Unternehmen verpflichtend – unabhängig davon, ob, wann und wie intensiv der Abschlussprüfer diese tatsächlich prüft. Bei der Überarbeitung des IDW PS 340 in 2020 wurden betriebswirtschaftliche Implikationen der gesetzlichen Grundlagen aufgegriffen, die längst für die Unternehmen verbindlich waren. Dies betrifft beispielsweise die Risikoaggregation, die Erläuterung, dass insbesondere (drohende) Illiquidität eine bestandsgefährdende Entwicklung darstellt. Noch immer sind viele Risikomanagementsysteme auf die Beurteilung der EBIT- oder Gewinnauswirkungen durch Risiken ausgerichtet. Tatsächlich entstehen bestandsgefährdende Entwicklungen fast immer

durch (drohende) Illiquidität.<sup>12</sup> Illiquidität tritt beispielsweise ein, wenn Mindestanforderungen an das Rating durch Risikoauswirkung nicht mehr erreicht oder Covenants verletzt werden, die zur Kreditkündigung führen. Entsprechend ist es richtig, dass nun auch (verspätet) im IDW PS 340 klargestellt wird, dass die Auswirkungen von Risiken auf Rating und Covenants untersucht werden müssen. Die entsprechende Anforderung solcher „bestandsgefährdender Entwicklungen“<sup>13</sup> zu untersuchen, ergibt sich qua Gesetz für die Unternehmen aber schon längst. Es ist eine zentrale Aufgabe des Unternehmens klarzustellen, was unter einer bestandsgefährdenden Entwicklung verstanden wird, um dann zu prüfen, mit welcher Wahrscheinlichkeit bestandsgefährdende Entwicklungen (durch Einzelrisiken oder deren Kombinationseffekte) auftreten. Diese Anforderung besteht unabhängig davon, dass der Abschlussprüfer bis 2021 dieses wichtige Themenfeld nicht untersucht hat.

Seit 2020 reicht die Schaffung von Transparenz über bestandsgefährdende Entwicklungen nicht mehr aus. Es sind ab einem kritischen Grad der Bestandsgefährdung auch geeignete Gegenmaßnahmen zu initiieren.

## 2. Implikationen für die Interne Revision

Die oben genannten Punkte zeigen, dass der Abschlussprüfer bei einer Prüfung nach IDW PS 340 bei Weitem nicht alle gesetzlichen Anforderungen an das Risikomanagement eines Unternehmens betrachtet. Selbst bei den Implikationen von § 91 AktG (KonTraG) bestehen, wie empirische Studien und Einzelfälle belegen, oft Prüfungslücken und Prüfungsdefizite.<sup>14</sup> Es ist gerade für Interne Revisoren und natürlich die Vorstände wichtig zu sehen, dass bei der Abschlussprüfung nur eine Teilmenge der relevanten Anforderungen betrachtet wird, obwohl natürlich alle gesetzlichen Anforderungen zu erfüllen sind, wenn man persönliche Haftungsrisiken vermeiden möchte. Aus diesem Sachverhalt ergeben sich einige we-

<sup>12</sup> Seit BASEL II (im StaRUG wird nur noch auf Illiquidität Bezug genommen).

<sup>13</sup> Siehe zur Erläuterung und Herleitung Gleißner, W. (2017c).

<sup>14</sup> Vgl. Gleißner, W. (2020b).

<sup>11</sup> Graumann, M. et al. (2009); Gleißner, W. (2019b und 2021).

sentliche Anforderungen für das Risikomanagement, und speziell auch die Interne Revision:

1. Die Interne Revision sollte dem Vorstand und auch dem Aufsichtsrat (Prüfungsausschuss) verdeutlichen, dass im Bereich Risikomanagement bei der Abschlussprüfung signifikante Prüfungslücken bestehen. Der Vorstand sollte im eigenen Interesse wissen, dass ein Bestätigungsvermerk des Abschlussprüfers nicht bedeutet, dass alle gesetzlichen Anforderungen an das Risikomanagement erfüllt sind (zum Beispiel, weil § 93 AktG Anforderungen und solche aus StaRUG überhaupt nicht betrachtet werden).

**Die Interne Revision sollte Vorstand und Aufsichtsrat verdeutlichen, dass im Bereich Risikomanagement bei der Abschlussprüfung signifikante Prüfungslücken bestehen.**

2. Die Abschlussprüfer sehen ihren Auftrag (momentan) offenbar nicht in einer umfassenden Prüfung<sup>15</sup> der gesetzlichen Anforderungen des Risikomanagements (eine gewisse Erweiterung des Prüfungsauftrags ist durch FISG denkbar). Aber es ist als Aufgabe der Internen Revision anzusehen, sämtliche Anforderungen zu prüfen und den Vorstand über hier bestehende Defizite zu informieren. Besser als der IDW PS 340 ist hier der DIIR Revisionsstandard Nr. 2 geeignet, weil er die Anforderungen aus den §§ 91 und 93 gemeinsam betrachtet. Er ist in vielen Punkten auch klarer und schärfer, weil die primäre Zielsetzung darin besteht, die Implikationen der gesetzlichen Anforderungen für das Risikomanagement deutlich darzustellen, während der IDW PS 340 aus der Perspektive und auch Interessenlage der Abschlussprüfer einen anderen Fokus hat (und aus verständlichen Gründen hier auch mehr Spielräume für den Abschlussprüfer bietet). Ergänzend sollte der Interne Revisor bei der Prüfung auch die neuen Anforderungen aus dem StaRUG mitberücksichtigen, also insbesondere betrachten, ob Mechanismen geschaffen sind, um rechtzeitig Gegenmaßnahmen bei einer drohenden Krise zu initiieren.

## Literaturverzeichnis

- Angermüller, N.O./Berger, T./Blum, U./Erben, F./Ernst, D./Gleißner, W./Grundmann, T./Heyd, R./Hofmann, K.H./Mayer, C./Meyer, M./Rieg, R./Schneck, O./Ulrich, P./Vanini, U. (2020): Gemeinsame Stellungnahme zum IDW EPS 340, <https://www.idw.de/blob/121892/0749c64f54f80bdee6c7f29d837a3f93/down-idweps340nf-gem-stn-hochschullehrer-rm-data.pdf> (Stand: 21.01.2020).
- Berger, T./Ernst, D./Gleißner, W./Hofmann, K./Meyer, M./Schneck, O./Ulrich, P./Vanini, U. (2021): Die Prüfung von Risikomanagementsystemen und die Defizite des IDW Prüfungsstandards 340, Der Betrieb, erscheint in Kürze.
- Braun, E. (2021): StaRUG: Unternehmensstabilisierungs- und -restrukturierungsgesetz, C.H. Beck, München 2021.
- Gleißner, W. (2017a): Grundlagen des Risikomanagements, 3. Auflage, Verlag Franz Vahlen, München 2017.
- Gleißner, W. (2017b): Risikomanagement, KonTraG und IDW PS 340, WPg – Die Wirtschaftsprüfung, 3/2017, S. 158–164.
- Gleißner, W. (2017c): Was ist eine „bestandsgefährdende Entwicklung“ im Sinne des § 91 Abs. 2 AktG (KonTraG)?, Der Betrieb, 47/2017, 24.11.2017, S. 2749–2754.
- Gleißner, W. (2018): Risikomanagement 20 Jahre nach KonTraG: Auf dem Weg zum entscheidungsorientierten Risikomanagement, Der Betrieb, 46/2018, S. 2769–2774.
- Gleißner, W. (2019a): Business Judgement Rule – Das neue Paradigma eines entscheidungsorientierten Risikomanagements, GRC aktuell, Vol. 2, 4/2019, S. 148–153.
- Gleißner, W. (2019b): Cost of capital and probability of default in value-based risk management, Management Research Review, Vol. 42, 11/2019, S. 1243–1258.
- Gleißner, W. (2020a): Wie beweist man, dass das Risikomanagement den Anforderungen der §§ 91 und 93 AktG nicht genügt (obwohl bestätigende Prüfberichte der Abschlussprüfer existieren)?, RWZ, 7-8/2020, S. 273–280.
- Gleißner, W. (2020b): Blindheit der Risikofrüherkennung – Wirecard: Schwächen bei Risikomanagement und Abschlussprüfung, <https://www.risknet.de/themen/risknews/wirecard-schwaechen-bei-risikomanagement-und-abschlusspruefung/> (Stand: 24.11.2020).
- Gleißner, W. (2021): Unternehmerische Entscheidungen – Haftungsrisiken vermeiden (§ 93 AktG, Business Judgement Rule), Controller Magazin, 1/2021, S. 16–23.
- Gleißner, W./Hofmann, K.H. (2020): Unerwartete Unternehmensinsolvenz trotz testiertem Risikomanagement? – Lessons Learned aus der Insolvenz der Gerry Weber International AG, 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

<sup>15</sup> Vgl. Gleißner, W./Sassen, R./Behrmann, M. (2019).



- Risikomanagement im Fokus, ZIR, Vol. 54, 4/2019, S. 148–159.
- Gleißner, W./Lienhard, F./Kühne, M. (2021): Neue gesetzliche Anforderungen an das Krisen- und Risikofrüherkennungssystem: Implikationen des StaRUG, Zeitschrift für Risikomanagement, erscheint in Kürze.
- Gleißner, W./Sassen, R./Behrmann, M. (2019): Prüfung und Weiterentwicklung von Risikomanagementsystemen – Ökonomische und aktienrechtliche Anforderungen, springer essentials, Springer Fachmedien Verlag, Wiesbaden 2019.
- Graumann, M. (2014): Die angemessene Informationsgrundlage bei Entscheidung, WISU, 3/2014, S. 317–320.
- Graumann, M./Linderhaus, H./Grundeis, J. (2009): Wann ist die Risikobereitschaft bei unternehmerischen Entscheidungen „in unzulässiger Weise überspannt“?, BFuP, 5/2009, S. 492–505.
- Gleißner, W./Haarmeyer, H. (2019): Die „bestandsgefährdende Entwicklung“ (§ 91 AktG) als „Tor“ in ein präventives Restrukturierungsverfahren, ZInsO, 45/2019, S. 2293–2299.
- Hunziker, S. (2019): Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward, Springer Gabler, Wiesbaden 2019.
- Internationaler Controllerverein (Hrsg.) (2021): Entscheidungsvorlagen für die Unternehmensführung, 2021, erscheint in Kürze.
- 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, Corporate Finance, 07-08/2020, S. 248–258.
- Kühne, M./Lienhard, F. (2020): Ausgestaltung eines Risikofrüherkennungssystems gemäß § 1 StaRUG und die Haftungsfolgen für die Geschäftsleitung, in: Der Sanierungsberater, 4/2020, S. 144–149.
- Link, M./Scheffler, R./Flath, T./Oehlmann, D./Dommers, C. (2021): Risikomanagement in deutschen Industrieunternehmen, Controller Magazin, 2/2021, S. 54–61.
- Link, M./Scheffler, R./Oehlmann, D. (2018): Quo vadis Risikomanagement?, Controller Magazin, 1/2018, S. 72–78.
- Risk Management Association e.V. (RMA) (2019): Managemententscheidungen unter Risiko. Haftung – Recht – Business Judgement Rule, ESV, Berlin 2019.
- Romeike, F. (2008): Rechtliche Grundlagen des Risikomanagements – Haftungs- und Strafvermeidung für Corporate Compliance, Erich Schmidt Verlag, Berlin 2008.
- Ulrich, P./Scheuermann, I./Spitzenpfeil, T. (2018): Status Quo von Risikomanagement und Risikocontrolling – Empirische Erkenntnisse und Implikationen für die Controllingpraxis, Controller Magazin, 6/2018, S. 62–68.
- Wolfrum, M. (2020): Der Fall Euromicron AG – Beispiel für die Nutzlosigkeit von Risikomanagementtestaten durch den Wirtschaftsprüfer, RMA e.V. (Hrsg.): Krisenbewältigung mit Risikomanagement – Jahrbuch Risikomanagement 2020, Erich Schmidt Verlag, Berlin 2020, S. 146–154.