ein Volumen von 630.000 €. Die Noventiq verpflichtete sich zudem zu einem weiteren Liquiditätseinschuss von 3 Mio. €. Im *Beschl. v. 27.11.2023* hält das zuständige *AG Dresden*[20] „Ein-Gruppen-Restrukturierungspläne", die lediglich Eingriffe in Rechte der Anteilseigner vorsehen, für grds. zulässig, wenn und weil dadurch Eingriffe in Fremdgläubigerrechte verhindert werden und die Sanierungsverantwortung bei den Gesellschaftern als wirtschaftliche Eigentümer des Unternehmens bleibe. Restrukturierungsrecht überlagert danach bereits im Zustand der drohenden Zahlungsunfähigkeit das Gesellschaftsrecht.

Etwas anders sah dies das *AG München*[21] im Fall der *Banovo GmbH*. Dort wurden im Restrukturierungsplan zwei Anteilseignergruppen gebildet, von denen sich die Gesellschafter der einen Gruppe im Vorfeld zur Sanierung und Finanzierung bereit erklärt hatten und die der anderen eben nicht. Das Gericht erklärte die Gruppenbildung für nicht sachgerecht, weil vermutlich nur darauf gerichtet, um die Voraussetzungen für einen „cram down" zu schaffen. Nach Argumentation der Planverfasser reiche auch bei Gesellschafterplänen gem. § 26 Abs. 1 Nr. 3 HS. 2 StaRUG bei nur zwei Gruppen die Zustimmung einer aus, da ein Überstimmen von Fremdgläubigern nicht zu befürchten sei, was die Vorschrift allein verhindern wolle. Dem erteilte das *AG München* im *Vorprüfungsbeschl. v. 15.2.2023* aber eine Absage, da § 26 Abs. Nr. 3, 2. HS StaRUG die Zustimmung einer Gruppe verlange, die beim Alternativszenario einer Insolvenz nicht „out of the money" wäre, woran es hier bei nur zwei Anteilseignergruppen fehle. I.Ü. diene der gruppenübergreifende Mehrheitsentscheid nicht dazu, Kleinstgesellschafter unter Mithilfe der Geschäftsführung mit der Mehrheit der Gesellschafter aus der Gesellschaft zu drängen.

d) In diesem im Ergebnis noch offenen Meinungsstreit bietet sich eine klare Differenzierung an: Gesellschafterpläne mit gesellschaftsrechtlichen Kapitalmaßnahmen sollten schon deshalb *grds*. zulässig sein, weil dies neben Eingriffen in Fremdgläubigerrechte in § 7 Abs. 4 StaRUG ausdrücklich vorgesehen ist und der bloße Eingriff in Anteilsrechte das mildere Mittel zur Sanierung darstellt, weil die Finanzierungsverantwortung nun einmal in erster Linie bei den Gesellschaftern liegt. Soweit der Grundsatz.

Im *konkreten Einzelfall* sollte die Zulässigkeit von Gesellschafterplänen stets davon abhängen, ob die geplanten Eingriffe in Gesellschafterrechte tatsächlich und ganz maßgeblich der Sanierung dienen und nicht etwa nur zur Klärung von Gesellschafterstreitigkeiten herangezogen werden. StaRUG darf als Sanierungsinstrument nur diesem Zweck dienen, und nur in solchen Fällen kann es angezeigt sein oder hingenommen werden, dass Sanierungsrecht Gesellschafsrecht dominiert.

20 572 RES 01/23, FD-InsR 2024, 801732.
21 1507 RES 3229/22, ZIP 2023, 603.

„GRC" – die Basis für nachhaltige Transformation, Restrukturierung & Sanierung

von Rechtsanwalt Dr. Volker Beissenhirtz LL.M. (London), CTP (EACTP), ZCF (Steinbeis), Berlin*

„Meistens ist die Krise die Mutter der Veränderung."

Holger Rathgeber

Seit Jahren steigt die Zahl der Pflichten der Geschäftsleitung, die auf die Durchsetzung einer „guten Unternehmensführung" abzielen, genauso wie die Zahl der entsprechenden Publikationen. Empirische Untersuchungen zeichnen allerdings ein eher ernüchterndes Bild der Umsetzung und erst recht der Erfolge in der Praxis. So weisen Studien seit Jahrzehnten den Zusammenhang zwischen dem Scheitern von Unternehmen und Fehlern in der Unternehmensführung und im Controlling nach. In neuerer Zeit treten Fälle von Mehrfachinsolvenzen hinzu, bei denen Anhaltspunkte für ähnliche Schwächen in der „Sanierungsführung" nicht von der Hand zu weisen sind. Viel spricht somit dafür, dass die Pflichtenkataloge (noch) nicht in der Praxis angekommen sind.

Dabei kann eine Ausrichtung der Unternehmensführung an etablierten Standards Unternehmenskrisen – wenn nicht verhindern, dann zumindest – abmildern und zudem die Basis für die notwendige operative Transformation von Unternehmen bilden. Die Verfolgung eines an der unternehmerischen Entscheidungsfindung ausgerichteten, (modifizierten) Ansatzes der Integration von Governance, Risk & Compliance (GRC)-Systemen eröffnet zudem die Chance zu mehr Effizienz im Vergleich zur Implementierung von Einzelsystemen.

Der nachfolgende Beitrag skizziert zunächst die Grundlagen und die rechtlichen Rahmenbedingungen von GRC in ihren Einzelkomponenten. In einem zweiten Teil werden die Gründe untersucht, warum sich gerade der deutsche Mittelstand bei der Implementierung schon der einzelnen Komponenten ziert. Die Ergebnisse dieser Untersuchung bilden die Basis für die im dritten

* Der Autor ist Partner der gunner*cooke* GmbH.

Teil folgende Darstellung der in mittelständischen Unternehmen zu beachtenden Mindeststandards und der Implementierung eines integrierten (und modifizierten) GRC-Systems. Abgerundet wird der Artikel durch einige prinzipielle Hilfestellungen für die Umsetzung eines integrierten Systems.

I. Hintergrund und Problemaufriss

1. Typische Insolvenzursache: Managementfehler

Empirische Studien der letzten Jahrzehnte führten immer wieder zu der Erkenntnis, dass wesentlicher Faktor für den Eintritt der Unternehmenskrise und Insolvenz strukturelle Managementfehler ist. Dementsprechend fasste schon *Hesselmann* seine Studie aus dem Jahr 1995 wie folgt zusammen: „*Übereinstimmend kommt die Mehrzahl der Autoren zu dem Ergebnis, dass der überwiegende Teil der Krisenursachen im endogenen Bereich anzusiedeln ist, wobei – unabhängig von Unternehmensgröße, Alter, Branche etc. – den Fehlern der Unternehmensführung ein besonderes Gewicht beizumessen ist. Managementfehler sind dabei nicht nur als interne Krisengründe feststellbar. Oftmals ist das Unvermögen des Managements, die tatsächliche wirtschaftliche Lage des Unternehmens und Kundenbedürfnisse richtig beurteilen zu können und rechtzeitig auf externe Veränderungen zu reagieren, ursächlich für die Krise. […] Eine rückläufige Konjunktur deckt häufig Fehler des Managements und spezielle Fehler im Finanzierungsverhalten erst auf.*"[1] Aber auch eine Studie des *ZIS* aus dem Jahr 2006[2] folgert, dass die „*Insolvenz meist Folge mehrerer Managementfehler*" sei. Diese Analysen werden durch eine aktuelle Studie der Unternehmensberatung *Meritus* bestätigt, in der „schlechte Führungskompetenz" als Hauptrisikofaktor für eine Insolvenz identifiziert wurde.[3]

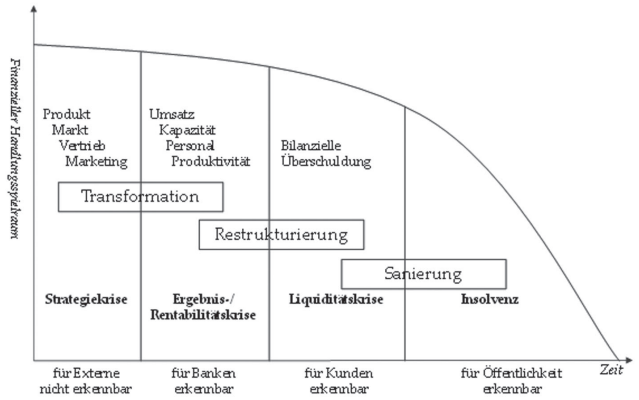

Abb. 1 – Krisenverlaufskurve

2. „Chapter 22" & Co.

Dass selbst vermeintlich erfolgreiche Sanierungen im Insolvenzverfahren letztendlich scheitern können, bewies zuletzt etwa die dreifache Insolvenz von *Galeria Karstadt Kaufhof*[4] oder die gar fünffache Insolvenz des Felgenherstellers *BBS*.[5] Derartig gescheiterte Sanierungen in der Insolvenz sind keine Einzelfälle, wie *Behrend/Möller* bereits 2020 belegten.[6] Nach dem Ende des „billigen" Geldes dürfte es noch schwerer werden, Unternehmen aus der Insolvenz heraus zu sanieren.[7] Vor diesem Hintergrund dürften sich zukünftig auch Insolvenzverwalter vermehrt mit der (haftungsrelevanten) Frage konfrontiert sehen, warum „ihre" jeweilige Sanierung in der Insolvenz letztlich dann doch nicht nachhaltig war – und zur erneuten Insolvenz führte.

3. Probleme häufig schon im normalen Geschäftsbetrieb und in der „Transformationsphase"

Aktuelle Beispiele, wie die teils fehlende Compliance bei *Boeing*,[8] das offensichtlich fehlende Risikomanagement bei *BayWa*[9] oder bei der *Meyer-Werft*,[10] die bei allen drei Unternehmen jeweils zu einer existenzbedrohenden Krise führten, bestätigen als anekdotische Evidenz die Ergebnisse der o.g. Studien für Unternehmen bereits im „normalen" Geschäftsbetrieb.

Aber auch die auf der Krisenverlaufskurve zeitlich vor Insolvenz, Sanierung & Restrukturierung angeordneten Transformationsprojekte scheitern mit schöner Regelmäßigkeit.[11] Sprich, das Management versagt häufig nicht erst in der existenziellen Krise des Unternehmens, sondern schon in den vorherigen Phasen, was jedoch nicht oder nur für ein begrenztes Publikum sichtbar ist. Damit drohen nicht nur massive Beträ-

1 Zitiert in *Seghorn*, Forschungsreihe, Bd. 3, „Insolvenzursachen und Insolvenzprophylaxe", S. 7.

2 „Zentrum für Insolvenz und Sanierung" der Universität Mannheim, „Ursachen von Insolvenzen", Nr. 414, in Zusammenarbeit mit *Euler Hermes*, S. 7, abrufbar unter: *https://www.uni-mannheim.de/media/Einrichtungen/zis/Studien/414_wiko.pdf*, gute Zusammenfassung: *https://anwalt-kg.de/newsbeitrag/gesellschaftsrecht/gruendungsberatung/13-gruende-fuer-die-insolvenz-von-unternehmen/*.

3 Meritus, „Insolvenzstudie 2024: Insolvenzgeschehen in Deutschland", abrufbar unter: *https://meritus-advisors.de/insolvenzstudie-2024-2/*.

4 FAZ, „Galeria Karstadt Kaufhof ist zum dritten Mal in kurzer Zeit insolvent", 9.1.2024, abrufbar unter: *https://www.faz.net/aktuell/wirtschaft/unternehmen/dritte-insolvenz-bei-galeria-karstadt-kaufhof-die-schuld-von-signa-19435373.html*.

5 Auto Motor Sport, „Felgenhersteller zum 5. Mal Pleite", 2.8.2024, abrufbar unter: *https://www.auto-motor-und-sport.de/verkehr/felgenhersteller-bbs-insolvenz-v1/*.

6 *Behrend/Möller*, KSI 2020, 271.

7 S. dazu nur WirtschaftsWoche, „Wir werden mehr Betriebsschließungen sehen", abrufbar unter: *https://www.wiwo.de/unternehmen/handel/insolvenzen-wir-werden-mehr-betriebsschliessungen-sehen/29954132.html*.

8 S. nur Tagesschau „Von Pannen und Whistleblowern", 15.5.2024, abrufbar unter: *https://www.tagesschau.de/wirtschaft/boeing-timeline-flugzeughersteller-probleme-100.html*.

9 S. nur *Gleißner*, in: WirtschaftsWoche, „Bei BayWa gab es „im Vorfeld genug Alarmsignale" (2024), abrufbar unter: *https://www.wiwo.de/my/unternehmen/industrie/agrarkonzern-in-der-krise-bei-baywa-gab-es-im-vorfeld-genug-alarmsignale-/29908088.html*.

10 S. nur *Gleißner* auf Linked-In, „Die Krise und drohende Insolvenz der bekannten Meyer Werft ist – wie fast immer - zurückzuführen auf ein zu lange ignoriertes Risiko (und Schwächen im Risikomanagement)", abrufbar unter: *https://www.linkedin.com/posts/werner-glei%C3%9Fner-1790215_kreuzfahrtschiffbauer-der-unbegreifliche-activity-7214530580233752576-SCsY/*.

11 Kearny, „Transformation in Deutschland" (2024), abrufbar unter: *https://www.de.kearney.com/documents/d/germany/fokus-future_-kearney-transformation-report-2024*; s. auch Kearny, „More than seventy percent of planning transformations fail" (2024), abrufbar unter: *https://www.kearney.com/service/operations-performance/article/more-than-seventy-percent-of-planning-transformations-fail-start-recovery-now*.

ge in derartigen Maßnahmen „versenkt", sondern auch der Krisenverlauf beschleunigt zu werden. Und das, obwohl mit Blick auf die nicht nur konjunkturellen, sondern tatsächlich strukturellen Schwächen der deutschen Wirtschaft über die grundsätzliche Notwendigkeit der Transformation deutscher Unternehmen grds. Konsens bestehen dürfte.[12] Die Unternehmensberatung *Roland Berger* bringt es auf den Punkt: „*Unternehmen im Krisenmodus muss künftig zweierlei gelingen: mit hoher Analyse- und Umsetzungsgeschwindigkeit die finanzielle Lage zu stabilisieren und zugleich die Weichen für die Zukunft zu stellen. Eine transformationsorientierte Restrukturierung ist der Weg zum Erfolg*."[13] Sprich, die Grenzen zwischen Transformation und Restrukturierung werden – auch aufgrund der hohen Volatilität und Geschwindigkeit der politischen und wirtschaftlichen Entwicklung – zunehmend verwischt.

II. Und GRC ist jetzt DIE Lösung?

Die Lösung zur identifizierten Insolvenzursache der schlechten Unternehmensführung (alternativ der letztlich nicht nachhaltigen Sanierung oder einer gescheiterten Transformation) ist natürlich eine gute Unternehmensführung, die situationsgerechte unternehmerische Entscheidungen trifft – so weit, so banal. Doch existiert mit dem Deutschen Corporate Governance Kodex (DCGK)[14] denn nicht bereits das optimale Instrument zur „*(Good) Corporate Governance*"? Zwar gibt der DCGK in seinen Grundsätzen 4 und 5 Unternehmen tatsächlich den Aufbau und Betrieb von Compliance- und Risiko-Management-Systemen vor. Allerdings lassen sich dem Kodex keine Hinweise zur konkreten Ausgestaltung der einzelnen Systeme und erst recht nicht zu einem integrierten Ansatz entnehmen. Dementsprechend unzureichend ist eine isolierte Bezugnahme auf den DCKG. Um die durch den DCKG gelieferten Oberbegriffe auszufüllen, ist vielmehr eine vertiefte Analyse dieser Systeme erforderlich.

1. Was ist „GRC"?

„GRC", also „*Governance, Risk & Compliance*" wird regelmäßig definiert als „*die integrierte Sammlung von Fähigkeiten, die eine Organisation in die Lage versetzen, Ziele zuverlässig zu erreichen, Unsicherheiten zu bewältigen und integer zu handeln.*"[15] Das entscheidende Stichwort in der Definition ist „integriert", denn es kommt darauf an, die Prinzipien, Strukturen und Prozesse von Governance, Risiko(-management) und Compliance(-management) so miteinander zu verknüpfen, dass die Unternehmensführung effektiv und effizient ihre „Ziele zuverlässig erreicht".

Abb. 2 – GRC als Rahmen für die Unternehmensplanung

Dabei richtet sich die Unternehmensführung – konkret jede „unternehmerische Entscheidung" – an der „Verfassung" des Unternehmens, also insbesondere dem Leitbild und der Strategie, aus und setzt diese wiederum durch das Herunterbrechen auf operative Ziele um. GRC dient damit dazu, die Unternehmensführung in die Lage zu versetzen, anstehende unternehmerische Entscheidungen effektiv und effizient zu treffen.[16] Damit bildet die Corporate Governance den Rahmen für die Entscheidungsfindung, das Risikomanagement fokussiert sich (in diesem Kontext)[17] auf die Identifizierung, Analyse und Abschwächung potenzieller Bedrohungen und die Compliance gewährleistet die Einhaltung von Satzungen, internen Richtlinien, externen Vorschriften und Branchenstandards. Während das Risikomanagement damit die Grenzen des (wirtschaftlichen) *Könnens* des Unternehmens definiert, gibt die Compliance die Grenzen des rechtlichen *Dürfens* (und reputationsbedingten *Wollens*) vor. Innerhalb dieser Grenzen muss sich die (informierte) unternehmerische Entscheidung bewegen. Flankiert werden diese Systeme durch die Kontrollinstanzen der Internen Kontrollsysteme (IKS) und Internen Revision (IR).

Schon dieser kurze Abriss zeigt, dass die häufig singulär betrachteten Themenstellungen holistisch betrachtet werden müssen – die Überbetonung eines der drei Bereiche zulasten der jeweils anderen führt zu einem Ungleichgewicht, welches sich negativ auf die unternehmerische Entscheidung auswirkt.

2. Historische Entwicklung

(1) Corporate Governance: Für ein besseres Verständnis der Prinzipien der Corporate Governance lohnt sich ein Blick in die historische Entwicklung.[18] So motivierten etliche Skandale, wie z.B. der sog. *Maxwell-Skandal* in England Ende der 1980er Jahre,[19] den englischen Gesetzgeber zur Einsetzung zahlreicher Untersuchungskommissionen[20] und schließlich zur Implemen-

12 S. dazu nur *Frank/Reischitz*, NWB Sanieren 2023, 364; *Hilmer*, ZInsO 2024, 1633.

13 Roland Berger, „Restrukturierung in der Transformation", Studie 2024, abrufbar unter: *https://content.rolandberger.com/hubfs/07_presse/Roland%20Berger%20Studie%20Restrukturierung%20in%20der%20Transformation_FINAL.pdf*.

14 Aktueller Stand abrufbar unter: *https://www.dcgk.de/de/kodex.html*.

15 Nach Open Compliance and Ethics Group (OCEG), 2002, „*GRC is the integrated collection of capabilities that enable an organization to achieve Principled Performance – the ability to reliably achieve objectives, address uncertainty, and act with integrity*.", abrufbar unter *https://www.oceg.org/ideas/what-is-grc/*, s. für eine weitergehende Definition *Otremba*, „GRC-Management als interdisziplinäre Corporate Governance", S. 150.

16 S. nachfolgend und vertiefend auch zur sog. „Business Judgement Rule", vgl. *Bea/Dressler*, NZI 2021, 67; *Gleißner*, GRC 2019, 148, abrufbar unter: *https://www.werner-gleissner.de/site/publikationen/WernerGleissner-offiziell-Nr-1784-Business-Judgement-Rule-Das-neue-Paradigma.pdf*.

17 Zum Aspekt des „Chancenmanagements" beim Risiko-Management, s.u.

18 An dieser Stelle wird auf die Beleuchtung der klassischen Begründungen für die Corporate Governance, wie etwa die Neue Institutionenökonomik, verzichtet, s. dazu aber z.B. *Otremba* (Fn. 15), S. 11 ff.

19 S. dazu nur *New York Times* v. 20.12.1991, „Maxwell's Empire: How It Grew, How It Fell", abrufbar unter: *https://www.nytimes.com/1991/12/20/business/maxwell-s-empire-it-grew-it-fell-special-report-charming-big-bankers-billions.html*.

20 Im Maxwell-Fall konkret: „Report of the Commission on the Financial Aspects of Corporate Governance" („The Cadbury Report"), abrufbar unter: *https://www.icaew.com/technical/corporate-governance/codes-and-reports/cadbury-report*.

tierung von zunächst „*Soft Law*" in Form von *Corporate Governance* Kodizes.[21] Auslöser für die spätere deutsche Corporate Governance-, aber auch der Compliance-Diskussion war u.a. der durch schwere Management-Fehler ausgelöste (Insolvenz-)Fall der *Philipp Holzmann AG* Anfang der 2000er Jahre,[22] der zur Berufung der Regierungskommission „Corporate Governance" führte (näher sogleich unten 3. a) (1)).

(2) Risiko: Zwar hat der deutsche Gesetzgeber mit dem KonTraG (s. dazu näher unten 3. b) (1)) bereits im Jahr 1998 – ebenfalls im Zuge skandalumwitterter Unternehmenszusammenbrüche[23] – zumindest für größere Agen die Pflicht zur Einführung eines Risikofrüherkennungssystems geschaffen. Jenseits dieser und weiterer einzelner Regulierungen im Finanzbereich nach der Finanzkrise hat das „R" in GRC bislang aber nicht nur in empirischen Untersuchungen eher einen Dornröschenschlaf gehalten.[24] Der Grund dafür ist relativ einfach: Denn trotz der Erforderlichkeit, sich dem technischen und gesellschaftlichen Wandel anzupassen, also die Notwendigkeit zur „Transformation" zu akzeptieren, und jenseits rechtlicher Pflichten, konnten viele Unternehmen dank guter Exportfähigkeit der deutschen Wirtschaft und niedriger Refinanzierungskosten bis 2020 zahlreiche Risiken schlicht ausblenden. Entgegen des vielfach deklarierten „*VUCA*"[25] herrschte in deutschen Unternehmen somit eher „*ceteris paribus*" – auch wenn die Krisenanzeichen schon weit vor 2020 klar zu erkennen waren.[26] Erst die Betriebsunterbrechungen, das Reißen zahlreicher Lieferketten und die Disruptionen der Corona-Pandemie (s. nur die Etablierung des Home-Office als regulärer Arbeitsplatz) haben zum Einzug eines (gewissen) Risiko-Bewusstseins in kleineren und mittleren deutschen Unternehmen geführt, das vor dem Hintergrund der aktuellen Polykrise[27] wohl auch nicht mehr so schnell abebben dürfte.

(3) Compliance: Der Begriff der „Compliance" entstammt ursprünglich der Medizin und bezeichnet dort die Einhaltung der vom Arzt verordneten Therapieformen.[28] Gegen Ende der 90er Jahre des vorigen Jahrhunderts fand der Begriff im Zuge der Diskussion über verschiedene Wirtschaftsskandale Einzug in das deutsche Wirtschaftsrecht und bedeutet zunächst nichts anderes als die „Einhaltung bestimmter Gebote". Damit verlangt (Corporate) Compliance, dass sich Unternehmen und Organe im Einklang mit dem geltenden Recht zu bewegen haben.[29] Der Deutsche Corporate Governance Kodex enthält in Nr. 4.1.3. mittlerweile eine Art Legaldefinition der Compliance: „*Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).*"

Auch wenn die Ursprünge der Corporate Compliance in (den oben angedeuteten) wirtschaftskriminellen Handlungen lagen und bis heute als sog. „*Criminal Compliance*" den Kern jedes Compliance-Management-Systems bilden, so hat sich der Umfang der Compliance über die Jahre immer weiter ausgedehnt. Zudem verschwimmen die Grenzen zur (nachfolgend kurz skizzierten) sog. „*Corporate Social Responsibility*" immer mehr, häufig, weil aus sog. „*Soft Law*", also Selbstverpflichtungen von Unternehmen, mit der Zeit „*Hard Law*", also allgemein verpflichtende Gesetze werden.[30] Prägnantes Beispiel hierfür ist das Lieferkettensorgfaltspflichtengesetz (LkSG).[31]

Entgegen landläufiger Ansicht[32] besteht durchaus ein prinzipieller Unterschied zwischen Compliance-Risiken und anderen Unternehmensrisiken, beide Bereiche sind – wie schon oben zu „(rechtlichem) Dürfen und (wirtschaftlichem) Können" ausgeführt – inhaltlich voneinander abzugrenzen. Compliance hat lediglich sicherzustellen, dass die rechtlich geforderten Standards eines Risikomanagement-Systems im Unternehmen tatsächlich etabliert und gelebt werden. (Zukünftige) Rechtsregeln können demgegenüber Risiken für den wirtschaftlichen Fortbestand des Unternehmens darstellen; man denke nur an das sog. „Verbrennerverbot",[33] das die EU für das Jahr 2035 festgelegt hat und das das Geschäftsmodell aller OEMs zumindest im Hinblick auf ihr bisheriges Kerngeschäft – die Produktion von Kfz mit Verbrennermotoren – konkret gefährdet.

(4) Der Ansatz, die v.g. Teilbereiche zu integrieren, ist nicht neu. Bereits im Jahr 2002 gründete *Scott L. Mitchell* in Folge des Zusammenbruchs der „New Economy" die *OCEG* („*Open Compliance and Ethics Group*") mit dem erklärten Ziel, die Compliance in Unternehmen zu verbessern. In der Folge wurde die Zielstellung u.a. um Risk-Management ergänzt und im Jahr 2004 zum GRC-Konzept weiter entwickelt.[34] In den Anfangsjahren wurde die Integration von G, R und C vorwiegend von Softwarehäusern in Bezug auf SAP-Anwendungen beschrie-

21 Eben z.B. den „Cadbury Code of Best Practice".

22 S. vertiefend bei Wikipedia, „Philipp Holzmann AG", abrufbar unter: *https://de.wikipedia.org/wiki/Philipp_Holzmann*.

23 *Laue*, „Integration der Corporate-Governance-Systeme", S. 14, verweist auf die Fälle *Vulkan*, *Klöckner* und *Metallgesellschaft*.

24 So auch *Laue* (Fn. 23), S. 85; *Otremba* (Fn. 15), S. 104.

25 „*Volatility, Uncertainty, Complexity, Ambiguity*", Der Begriff wurde bereits im Jahr 1987 im U.S. Army War College geprägt, s. Army Heritage and Education Center, „Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity", abrufbar unter: *https://usawc.libanswers.com/faq/84869*.

26 S. nur *Beissenhirtz*, „2018 – Cassandras Blick in die Glaskugel, ZInsO 2018", 281, abrufbar unter *https://www.beissenhirtz.com/wp-content/uploads/2021/08/Beissenhirtz_ZinsO-Glaskugel_2018.pdf*.

27 So zuerst im aktuellen Kontext *Tooze*, in: Die Zeit, 15.7.2022, „Kawumm!", abrufbar unter: *https://www.zeit.de/2022/29/krisenzeiten-krieg-ukraine-oel-polykrise*.

28 S. nur *Otremba* (Fn. 15), S. 121 m.w.N.

29 *Hauschka/Moosmayer/Lösler*, Corporate Compliance, S. 2; nach *Schneider*, ZIP 2003, 646, tatsächlich eine Binsenweisheit; s. auch vertiefend *Otremba* (Fn. 15), S. 122 ff.

30 S. dazu nur *Behringer*, ZRFC 2022, 149; *Hauschka*, in: Hauschka/Moosmayer/Lösler (Fn. 29), S. 3, will die Themenfelder (noch) voneinander abgrenzen.

31 S. zu den Hintergründen vertiefend Grabosch/*Grabosch*, Lieferkettensorgfaltspflichtengesetz, S. 15 ff.

32 Z.B. *Hauschka* (Fn. 30), S. 3.

33 S. näher dazu Bundesregierung, „EU-Umweltrat: Nur noch CO2-frei fahren", abrufbar unter: *https://www.bundesregierung.de/breg-de/schwerpunkte/europa/verbrennermotoren-2058450*.

34 S. näher dazu OCEG, Celebrating 20+ years of OCEG, abrufbar unter: *https://www.oceg.org/20-years/*; *Scott L. Mitchell* (2007-10-01), „GRC360: A framework to help organisations drive principled performance", International Journal of Disclosure and Governance, (4): 279 – 296.

ben, teilweise wurde nicht einmal der der Terminus „GRC" als solcher verwandt, obwohl sich bereits im Jahr 2010 auf dem Netzwerk Linked-In ca. 4.000 Personen als „GRC Professionals" bezeichneten.[35] In Deutschland treibt seit einiger Zeit das IDW e.V. eine Integration der Bereiche voran und hat, beginnend ab 2017, mit den sog. „IDW PS 98x" eine Sammlung von Standards für die Prüfung einzelner Bereiche geschaffen, die zusammengenommen ein GRC-System darstellen können.[36]

3. Entwicklung der (rechtlichen) Rahmenbedingungen

GRC ist aber nicht nur aufgrund der v.g. historischen Entwicklung Teil der Lösung für eine gute Unternehmensführung. Zumindest die Einrichtung der einzelnen GRC-Disziplinen in Unternehmen jeder Größe und fast jeder Rechtsform entspricht zudem den Anforderungen der aktuellen Rechtslage. Dabei herrscht im Bereich GRC kein Erkenntnis- sondern – wie in anderen Rechtsbereichen auch – eher ein Umsetzungsproblem. Denn auf die zuvor erläuterten Skandale hat der deutsche Gesetzgeber zunächst zwar eher zögerlich reagiert, überschlägt sich aber mittlerweile in der Konkretisierung der Pflichten des Managements. Dazu tritt eine ebenfalls stetig anschwellende Rechtsprechung zu diversen Pflichten der Unternehmensführung. Verschiedene Organisationen versuchen zudem diesen an sich schon nur schwer überschaubaren juristischen Flickenteppich durch Standards praktisch umsetzbar zu gestalten – nicht selten getrieben von eigenen ökonomischen Interessen. Dementsprechend schwer fällt einem rechtlich nicht versierten Unternehmenslenker der Überblick über die Rechtslage, zu der er sich (neu-deutsch) *compliant* verhalten soll. Deswegen wird im Folgenden ein erster Überblick zur rechtlichen Situation und etablierten Standards gegeben, der bei der nachfolgenden Betrachtung der Mindeststandards sodann weiter vertieft wird.

a) Gesetzgeberische Entwicklung[37]

(1) Governance: Die v.g. Regierungskommission „Corporate Governance" legte ihren Bericht im Sommer 2001 vor[38] und empfahl die Schaffung eines Deutschen Corporate Governance Kodex (DCGK). Der entsprechende erste Kodex wurde am 26.2.2002 verabschiedet[39] und wird seitdem von der nunmehr ständigen Regierungskommission „Corporate Governance Kodex" stetig überarbeitet.[40] Vorstand und Aufsichtsrat einer börsennotierten AG müssen jährlich gem. § 161 Akt in einer sog. „Entsprechenserklärung" ausführen, inwieweit sie den DCGK befolgen. Ferner wurde im Jahr 2005 durch das sog. UMAG[41] mit der Regelung des § 93 Abs. 1 Satz 2 AktG (neu) die sog. „*Business Judgement Rule*" (BJR) ins deutsche Recht eingeführt.[42] Mit dem BilMoG wurde schließlich 2009 für börsennotierte Gesellschaften die Pflicht zur Abgabe einer Erklärung zur Unternehmensführung (Corporate Governance Erklärung) in § 289a HGB a.F. (nunmehr in § 289f HGB) eingefügt.[43]

Zwischenzeitlich hat die EU diese Thematik ebenfalls aufgegriffen, zur bereits benannten „*Corporate Social Responsibility*"[44] erweitert und mit der CSR-Richtlinie[45] eine (weitere) Berichtspflicht zunächst für größere Kapitalgesellschaften etabliert. Die entsprechenden Regelungen sind mittlerweile in §§ 289b ff. HGB verankert.[46] Seit einiger Zeit erhöhen die Institutionen der EU die Regulierungsdichte im Rahmen der Durchsetzung des sog. „*Green Deals*"[47] – was absehbar zu einer weiteren Verschärfung der Berichtspflichten führen wird, hinsichtlich derer sich die Unternehmen *compliant* verhalten müssen.[48] Ziel dieser Berichtspflichten ist natürlich die Einwirkung auf die Governance des jeweiligen Unternehmens.

(2) Risiko: Bereits vor den konzertierten Aktivitäten zur Corporate Governance, nämlich im Jahr 1998, hatte der Gesetzgeber mit der Verabschiedung des „Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich" (KonTraG)[49] erste zaghafte

35 S. für einen historischen Abriss zu GRC auch *Otremba* (Fn. 15), ab S. 143 ff., *Racz/Weippl/Seufert*, „A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)", Konferenz-Dokumentation, Linz, 2010, abrufbar unter: *https://www.researchgate.net/publication/221521336_A_Frame_of_Reference_for_Research_of_Integrated_Governance_Risk_and_Compliance_GRC*.

36 S. näher dazu unten, aber auch *Brühl/Hiendlmeier*, ZRFC 2013, 24.

37 Es würde den Rahmen dieses Artikels bei Weitem sprengen, an dieser Stelle vertieft auf Gesetze anderer Staaten oder Institutionen einzugehen, die z.T. weltweite Geltung beanspruchen, wie etwa der *UK Bribery Act* oder der (US) *Foreign Corruption Practices Act*. Gerade für exportorientierte deutsche Mittelständler ist die Kenntnis dieser Regelungen (oder etwa auch der Auswirkungen der *US Sentencing Guidelines*) allerdings unabdingbar.

38 Bericht der Regierungskommission „Corporate Governance", BT-Drucks.: 14/7515, abrufbar unter: *https://dip.bundestag.de/vorgang/bericht-der-regierungskommission-corporate-governance-unternehmensführung-unternehmenskontrolle-modernisierung/103137*.

39 Deutscher Corporate Governance Kodex, 26.2.2002, abrufbar unter: *https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/D_CorGov_Endfassung_2002_02_23.pdf*.

40 Aktueller Stand abrufbar unter: *https://www.dcgk.de/de/kodex.html*.

41 „Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts", BGBl. I 2005, S. 2802, Dokumentation abrufbar unter: *https://dip.bundestag.de/vorgang/gesetz-zur-unternehmensintegrit%C3%A4t-und-modernisierung-des-anfechtungsrechts-umag-g-sig-15019590/97767?f.deskriptor=Vorstand&start=275&rows=25&pos=279&ctx=d*.

42 S. dazu grundlegend *Lutter*, ZIP 2007, 841.

43 Vertiefend unter: *https://dip.bundestag.de/vorgang/gesetz-zur-modernisierung-des-bilanzrechts-bilanzrechtsmodernisierungsgesetz-bilmog/14158*.

44 S. näher dazu und zum Verhältnis zu „ESG" („*Environmental, Social & Governance*") bei *Pollman*, „Corporate Social Responsibility, ESG, and Compliance", in: Penn Carey Law: Legal Scholarship Repository, abrufbar unter: *https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3571&context=faculty_scholarship*.

45 „Richtlinie 2014/95/EU des Europäischen Parlaments und des Rates vom 22.10.2014 zur Änderung der Richtlinie 2013/34/EU im Hinblick auf die Angabe nichtfinanzieller und die Diversität betreffender Informationen durch bestimmte große Unternehmen und Gruppen", ABl. L 330 v. 15.11.2014, p. 1 – 9, abrufbar unter: *https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32014L0095*.

46 „Gesetz zur Stärkung der nichtfinanziellen Berichterstattung der Unternehmen in ihren Lage- und Konzernlageberichten (CSR-Richtlinie-Umsetzungsgesetz)", abrufbar unter: *https://dip.bundestag.de/vorgang/gesetz-zur-st%C3%A4rkung-der-nichtfinanziellen-berichterstattung-der-unternehmen-in-ihren/76955*.

47 EU-Kommission, „Der europäische Grüne Deal", abrufbar unter: *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_de*.

48 Konkret: RL (EU) 2022/2464 (CSRD), abrufbar unter: *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2464*.

49 S. vertiefend dazu bei Deutscher Bundestag, KonTraG, BT-Drucks.: 872/97, S. 25, abrufbar unter: *https://dip.bundestag.de/vorgang/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-kontrag-g-sig-13020839/136069*.

Schritte zur Einführung von Risikofrüherkennungssystemen in Unternehmen unternommen und mit § 91 Abs. 2 AktG zumindest für AGen die Pflicht statuiert, ein Krisenfrüherkennungssystem vorzuhalten. Diese Pflicht ist seit 2022 durch § 1 StaRUG für haftungsbeschränkte Unternehmensträger ausgestaltet und wesentlich erweitert worden (s. vertiefend dazu unten). Für börsennotierte AGen wurde im Jahr 2021 zudem durch das Finanzmarktintegritätsstärkungsgesetz (FISG) u.a. die Pflicht zur Errichtung eines angemessenen und wirksamen internen Kontrollsystems (IKS) sowie eines entsprechenden Risikomanagementsystems (RMS) und für Unternehmen von öffentlichem Interesse eines Prüfungsausschusses eingeführt.[50]

(3) Compliance: Spätestens seit dem beeindruckenden Bußgeld gegen Siemens i.H.v. 395 Mio. € wegen Verletzung der Aufsichtspflicht des Gesamtvorstands durch eine mangelhafte Compliance-Struktur des Konzerns im Jahr 2008[51] gelten die §§ 30, 130 OWiG als haftungsrechtliche Grundlage für die Haftung von Gesellschaftsorganen im Falle mangelhafter Compliance-Strukturen in Unternehmen. Dies dürfte bis zu einer etwaigen Verabschiedung des sog. „Verbandssanktionengesetzes" auch so bleiben.[52] Dementsprechend kann das Unterlassen der Einrichtung eines Compliance-Management-Systems (CMS) an sich bereits nachteilige Folgen für das Unternehmen zeitigen. Darüber hinaus verdeutlichen z.B. die regelmäßig nach § 83 Abs. 5 DSGVO für Verstöße gegen Datenschutzvorschriften verhängten Bußgelder im Millionenbereich,[53] dass die Vernachlässigung einzelner Compliance-Themen Unternehmen ebenfalls teuer zu stehen kommen kann.

b) Rechtsprechung

(1) Governcance: Während ausdrückliche (deutsche) Rechtsprechung zur Corporate Governance so nicht auszumachen ist, schon weil der DCGK – mit Ausnahme der Berichtspflichten – als „*Soft Law*" nicht gerichtlich durchsetzbar ist,[54] existiert bereits eine längere Rechtsprechungshistorie zum Kern der Governance, nämlich der unternehmerischen Entscheidung, der bereits o.g. „*Business Judgement Rule*". So urteilte der BGH im Jahr 1997 in Sachen *ARAG/Garmenbeck*, dass „*dem Vorstand bei der Leitung der Geschäfte des Gesellschaftsunternehmens ein weiter Handlungsspielraum zugebilligt werden muß, ohne den eine unternehmerische Tätigkeit schlechterdings nicht denkbar ist.*"[55]

(2) Risiko: Für die Bereiche des Risiko-Managements existiert eine historisch gewachsene und durchaus differenzierte Rechtsprechungslage. So verlangt die Rechtsprechung von Geschäftsführern und Vorständen grds. sog. Maximialrisiken zu vermeiden und darüber hinaus, dass die zu erwartenden Erträge eines vorzunehmenden Geschäfts in einem ausgewogenen Verhältnis zu dessen Risiken stehen.[56] Bereits Mitte der 90er Jahre des vorigen Jahrhunderts konstatierte der BGH zudem, dass der „*Geschäftsführer einer Gesellschaft mit beschränkter Haftung (GmbH) für eine Organisation sorgen [muss], die ihm die […] erforderliche Übersicht über die wirtschaftliche und finanzielle Situation der Gesellschaft jederzeit ermöglicht. Dabei hat er die wirtschaftliche Lage des Unternehmens laufend zu beobachten und sich bei Anzeichen einer krisenhaften Entwicklung durch Aufstellung einer Zwischenbilanz oder eines Vermögensstatus einen Überblick über den Vermögensstand zu verschaffen.*"[57] Nachdem eine Verletzung der Insolvenzantragspflicht nach einer Entscheidung des BGH grds. nicht mehr zu einem Haftungsausschluss der D&O-Versicherung führt,[58] könnten Versicherer die Verletzung der Pflicht, ein RMS einzurichten, möglicherweise nutzen, um auf diesem Wege den Verlust des Versicherungsschutzes im Fall der Insolvenz zu begründen.[59]

(3) Compliance: Für den Bereich der Compliance urteilte zunächst das LG München im sog. „*Neubürger-Urteil*" aus dem Jahr 2013 im Zusammenhang mit dem v.g. Siemens-Fall, dass die „*Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance-Systems zur Gesamtverantwortung des Vorstands*" gehört.[60] Seitdem wird die Verpflichtung zur Einrichtung eines CMS zumindest bei börsennotierten AGen als verpflichtend angesehen. Nachdem der BGH diese Pflicht in seiner sog. „*Panzerhaubitzen-Entscheidung*" im Jahr 2017[61] scheinbar etwas abschwächte, indem er dem Faktor eines etablierten CMS und dessen Fortentwicklung (z.B. nach einem Fall der Non-Compliance) eine bußgeldmindernde Wirkung zusprach, verpflichtete das OLG Nürnberg in einer Entscheidung aus dem Jahr 2023 Geschäftsführer selbst von Klein-GmbH,[62] ein CMS und ein System der internen Kontrolle (IKS, dazu sogleich) einzurichten.[63]

c) Standards

Zahlreiche Institutionen versuchen durch von ihnen entwickelte Standards den oben skizzierten Rechtsrahmen auszu-

50 „Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG)", BGBl. I, 10.6.2021, 1534, abrufbar unter: *https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl121s1534.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1534.pdf%27%5D__1721806803785*.

51 Der Entwurf des Bußgeldbescheides ist auf den Seiten von Siemens nach wie vor abrufbar, vgl. *https://assets.new.siemens.com/siemens/assets/api/uuid:0d6eee47-5b44-4ad6-bd5d-34de580085ae/MucStaats.pdf*; s. auch die Meldung bei Beck-Online, „Nochmals Schmiergeldaffaire: Staatsanwaltschaft München I erlässt Bußgeldbescheid in Höhe von 395 Millionen € gegen Siemens", abrufbar unter: *https://community.beck.de/2008/12/16/nochmals-schmiergeldaffaire-staatsanwaltschaft-munchen-i-erlasst-busgeldbescheid-in-hohe-von-395-millionen-e-gegen-si*.

52 S. zur damaligen Diskussion nur *Weidenauer*, CCZ 2021, 53.

53 S. dazu die Übersicht über aktuelle Bußgelder unter: *https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/*.

54 S. aber die theoretischen Erwägungen bei *Brugger*, NZG 2020, 281.

55 BGH, Urt. v. 21.4.1997 – II ZR 175/95, BGHZ 135, 244 Rn. 22.

56 Vgl. OLG Thüringen, Urt. v. 8.8.2000 – 8 U 1387/98, NZG 2001, 86.

57 BGH, Urt. v. 20.2.1995 – II ZR 9/94.

58 BGH, Urt. v. 18.11.2020 – IV ZR 217/19, ZInsO 2021, 47.

59 So *Weiß*, „Tod der D&O-Versicherung?", Handelsblatt Live, 25.1.2024, abrufbar unter: *https://live.handelsblatt.com/tod-der-do-versicherung/*.

60 LG München I v. 10.12.2013 – 5 HK O 1387/10, abrufbar unter: *https://openjur.de/u/682814.html*.

61 BGH, Urt. v. 9.5.2017 – 1 StR 265/16.

62 Das betroffene Unternehmen beschäftigte zum Zeitpunkt der beurteilten Taten 13 Mitarbeiter.

63 OLG Nürnberg v. 30.3.2022 – 12 U 1520/19, Kommentierung dazu bei *Bartz/Bitter*, CCZ 2022, 319.

füllen. Auf internationaler Ebene ist das neben der *OECD*[64] z.B. das *Institute of Internal Auditors* (IIA), das mit seinem mittlerweile als „*Three Lines Model*" bezeichneten Standard[65] sozusagen den Rahmen für die Diskussion „integrativer Konzepte" setzt.[66]

Daneben haben sich insbesondere US-Institutionen durch verschiedene Standards hervorgetan, so z.B. das „*Committee of Sponsoring Organizations of the Treadway Commission*" (*COSO*),[67] welches mit dem „*COSO ERM – Enterprise Risk Management Framework*" einen Standard für die Implementierung von RMS gesetzt hat.[68] Die *Internationale Organisation für Normung* (ISO) hat mit dem Standard „ISO 31000"[69] einen weiteren weltweiten Standard für RMS entwickelt, genauso wie mit dem Standard ISO 37301:2021 für Compliance, der ebenfalls weltweite Geltung beansprucht.[70]

Neben dem bereits o.g. DCGK setzt die *Bundesanstalt für Finanzaufsicht*, BaFin, mit den sog. „MA-Risk"[71] (Mindestanforderungen-Risk) in Deutschland den Standard für das Risikomanagement bei Finanzinstituten. Die Kenntnis dieser Mindestanforderungen sind für den Mittelständler nicht uninteressant, zumal, wenn er sich um Kredite bemüht. Daneben hat das *IDW e.V.* zunächst mit dem IDW PS 340 einen Prüfungsstandard für die nach § 317 Abs. 4 HGB erforderliche Prüfung von Risikofrüherkennungssystemen nach § 91 Abs. 2 AktG geschaffen.[72] In der Folge hat das IDW ab 2017 mit den sog. „IDW PS 98x" eine Sammlung von Standards – IDW PS 980 für CMS, 981 für RMS, 982 für IKS sowie 983 für Interne Revisionssysteme – für die Prüfung einzelner Bereiche veröffentlicht, die zusammengenommen ein GRC-System darstellen (können).[73] Das *Deutsche Institut für Interne Revision* (DIIR) hat mit seinem Standard Nr. 2 Grundsätze für die Prüfung des Risikomanagementsystems durch die Interne Revision festgelegt.[74] Daneben veröffentlicht die (deutsche) *Risk Management & Rating Association e.V.* (RMA e.V.) laufend Leitfäden zur Risikofrüherkennung und zum Risikomanagement.[75] Schließlich setzt das *Deutsche Institut für Compliance* (DICO) seit Jahren verschiedene Standards für die Entwicklung von CMS.[76]

Zusammenfassend lässt sich zu diesem Abschnitt feststellen, dass die Einrichtung und der Betrieb der einzelnen Elemente von GRC von Gesetzgebung und Rechtsprechung mittlerweile verpflichtend festgelegt sind und ein Verstoß gegen diese grundsätzlichen Pflichten Haftungsgefahren nach sich ziehen kann. Gleichzeitig geben internationale und nationale Standards eine z.T. nicht mehr überschaubare Anzahl an Definitionen, Strukturen und Hinweisen zur „*Best Practice*". Die unternehmerische Leistung liegt nunmehr also auch darin, unternehmensadäquate Strukturen und Prozesse zu schaffen, die diese Vorgaben erfüllen, das Unternehmen dabei aber nicht überfordern, sondern es möglichst sogar wettbewerbsfähiger aufstellen.

4. Nicht nur der deutsche Mittelstand ziert sich – aus Gründen

Trotz der empirisch untermauerten Erkenntnisse über die Ursachen von Unternehmenskrisen und den zahlreichen rechtlichen Verpflichtungen zur Etablierung zumindest der Einzelkomponenten von GRC sind augenscheinlich weder die Einzelkomponenten und erst recht nicht ein holistischer GRC-Ansatz[77] Selbstläufer im deutschen Mittelstand. Das belegen etliche Studien zur Implementierung von Compliance-Management-Systemen: So bewerteten zwar 80 % der in einer Studie aus dem Jahr 2018 befragten Vertreter mittelständischer Unternehmen Compliance-Risiken als wesentlich, allerdings verfügten zum damaligen Zeitpunkt nur 45 % über eine eigene Compliance-Abteilung und lediglich 27 % über ein unternehmensweites CMS.[78] Häufig sehen die Mittelständler den tatsächlichen Nutzen eines CMS nicht, weil sie die Regeltreue von Mitarbeitern bereits über andere Wege oder Abteilungen zu sichern glauben.[79] Zudem befürchten mittelständische Unternehmer häufig, dass ein CMS als Fremdkörper die Vertrauenskultur im Unternehmen untergrabe.[80] Die fehlende Verbreitung von und bestehende Skepsis gegenüber CMS mag auch darin begründet liegen, dass die Kosten für die Einführung und das Betreiben von entsprechenden Systemen bei Mittelständlern häufig als nicht in einem akzeptablen Verhältnis zum Nutzen angesehen wird.[81] Der Kostenfaktor ist tatsächlich nicht zu unterschätzen: So gaben mittelständische Unternehmen laut einer Umfrage aus dem Jahr 2011 im Durchschnitt 37.300 €/Jahr für Compliance

64 Mit ihrem „Leitfaden zur Erfüllung der Sorgfaltspflicht für verantwortungsvolles unternehmerisches Handeln", abrufbar unter: *https://mneguidelines.oecd.org/OECD-leitfaden-fur-die-erfullung-der-sorgfaltspflicht-fur-verantwortungsvolles-unternehmerisches-handeln.pdf*.

65 Abrufbar unter: *https://www.theiia.org/globalassets/site/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/glob-three-lines-model-paper_layout-rebuild.pdf*.

66 So zu Recht *Gleißner*, Controlling 2020, 23, 24, abrufbar unter: *https://futurevalue.de/wp-content/uploads/2022/03/FA-1813-Integratives-Risikomanagement-Schnittstellen-2020.pdf*.

67 Näheres unter: *https://www.coso.org/*.

68 Aktueller Stand 2017, nähere Informationen abrufbar unter: *https://www.coso.org/guidance-erm*; s. zur Implementierung des COSO-Standards im Mittelstand bei *Schulte/Balk*, ZRFC 2011, 62.

69 S. zur ISO 3100:2018 und zur Übernahme als DIN: *Herdmann/Henschel*, ZRFC 2018, 111.

70 Nähere Informationen unter: *https://www.iso.org/obp/ui/#iso:std:iso:37301:ed-1:v1:en*.

71 Abrufbar unter: *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html*.

72 S. dazu näher bei *Gleißner*, WPg 2017, 158, abrufbar unter: *https://futurevalue.de/wp-content/dokumente/offiziell_Nr._1413b_Risikomanagement_KonTraG_und_IDW_PS340.pdf*.

73 Sehr informativ, *Wermelt*, Die Prüfung von Corporate Governance Systemen", abrufbar unter: *https://www.wiwi.uni-muenster.de/mgk/sites/mgk/files/downloads/abendvortrag/mgk_-_einfuehrung_ps98x_-_dezember_2017_-_versand.pdf*; s. auch unter: *https://shop.idw-verlag.de/Praxisleitfaden-Governance-Risk-und-Compliance/11769*.

74 Abrufbar unter: *https://www.diir.de/fachwissen/standards/diir-standards/*.

75 Abrufbar unter: *https://rma-ev.org/news-publikationen/publikationen-rma-spezial*.

76 Nähere Informationen abrufbar unter: *https://www.dico-ev.de/publikationen/*.

77 Zum GRC-Konzept s. die empirische Studie von *Brühl/Hiendlmeier* ZRFC 2013, 24.

78 FAZ-Institut/*Ebner Stolz*, „Compliance – Brennpunkt Mittelstand", S. 12 f., abrufbar unter: *https://www.ebnerstolz.de/de/9/7/7/3/8/Ebner_Stolz_Compliance-Studie-2018.pdf*.

79 So *Mittendorf*, „Compliance in mittelständischen Unternehmen", 2020, S. 13; *Lindemann/Menke*, CCZ 2022, 85, 88.

80 So *Lindemann/Menke*, CCZ 2022, 85, 88.

81 *Mittendorf* (Fn. 79), S. 14.

aus.[82] Eine Erhebung der *Hochschule Konstanz Technik, Wirtschaft und Gestaltung* (HTWG) aus dem Jahr 2012 ergab eine relativ große Spreizung der tatsächlichen Ausgaben: So zahlten demnach 23 % der mittelständischen Unternehmen unter 10.000 € für Compliance im Jahr, nur 10 % dagegen über 200.000 €.[83] Die Kosten für Compliance dürften in den letzten Jahren allerdings über die gesamte Bandbreite nicht unerheblich gestiegen sein.[84]

Vor der Einführung der Pflicht zur Risikofrüherkennung für (als juristische Personen verfasste) Unternehmen durch § 1 StaRUG bestand eine gesetzliche Pflicht zur Etablierung derartiger Systeme nur für AGen (mit erhoffter, aber wohl tatsächlich nie eingetretener Ausstrahlungswirkung auf GmbH).[85] Dementsprechend liegen empirische Untersuchungen zu RMS vor 2021 eigentlich nur für (börsennotierte) AGen, nicht jedoch für mittelständische Unternehmen, vor.[86] Nach einer von *Deloitte* im Jahr 2023 durchgeführten Benchmark-Studie ist zwar das Risikobewusstsein bei den befragten zumeist großen Unternehmen vorhanden, aber die konkrete Ausgestaltung des jeweiligen RMS noch ausbaufähig.[87] *Eulerich/Gleißner* weisen in einer Untersuchung von 2021 nach, dass die meisten Risikomanagement-Systeme noch nicht einmal die gesetzlichen Mindestanforderungen erfüllen.[88]

Die (teilweise nicht immer ganz aktuellen) empirischen Einzelbetrachtungen zu Compliance- und Risiko-Management werden nur durch wenige empirische Untersuchungen zum Erfolg von (holistischen) GRC-Strukturen in Unternehmen ergänzt, insbesondere auch aktuelleren Datums.[89] *Racz*, *Weippl* und *Seufert* haben in einer im Jahr 2010 veröffentlichten Studie die bis dahin zu integrierten Ansätzen vorliegenden Veröffentlichungen untersucht, aber auch eine Befragung von 99 Personen durchgeführt, die zum damaligen Zeitpunkt im Bereich GRC aktiv waren.[90] *Brühl* und *Hiendlmeier* haben im Jahr 2013 eine Befragung von 29 großen und mittelständischen Unternehmen zum Stand von GRC durchgeführt.[91] Die Ergebnisse dieser Untersuchungen sind allerdings ebenfalls eher ernüchternd. Zwar vertrat die Mehrheit der 2010 befragten Personen die Ansicht, dass die Vorteile eines integrierten Ansatzes den Aufwand überwiegen, letztendlich ließ aber nach den sowohl 2010 als auch 2013 durchgeführten Untersuchungen die Integration der Systeme noch zu wünschen übrig.[92]

Bislang sind zudem erfolgreiche Praxisbeispiele zu in Unternehmen tatsächlich integrierten GRC-Konzepten, die zumindest als anekdotische Evidenz dienen könnten, eher rar gesät. So verfügen *Volkswagen*,[93] die *FraPort AG*, *EnBw*[94] und *Würth*[95] über integrierte GRC-Systeme. Mit *Würth* findet sich zudem ein eigentümergeführtes Unternehmen auf der Liste, allerdings ist es nur schwerlich noch als mittelständisch zu bezeichnen. Sprich, für Großunternehmen gibt es bereits einige „Best Practice"-Beispiele, für den typischen deutschen Mittelstand sind diese jedenfalls noch nicht bekannt.

Aufgrund der eher dünnen empirischen Datenlage und der wenigen Praxisbeispiele wird man als Beleg für den Nutzen einer holistischen GRC-Struktur dementsprechend zunächst nur – eher theoretisch – auf die offensichtliche Korrelation zwischen dem Scheitern des Unternehmens und schlechter Unternehmensführung zurückgreifen können. Die Insolvenzhäufigkeit von KMU, die höher liegt als die von Großunternehmen,[96] korreliert zumindest mit der häufig bei gerade jenen KMU konstatierten „schlechten Führungskompetenz".[97] Letztlich dürfte das Scheitern von Transformations- und Sanierungsprojekten auf ähnlichen Ursachen beruhen wie die Insolvenz – eben einer nicht „guten" Unternehmensführung.

5. GRC ist nicht DIE, kann aber ein Teil der Lösung sein – unter Bedingungen

Trotz der ernüchternden Analyse des Ist-Zustandes zur Implementierung schon der Einzelbereiche, erst recht aber eines holistischen Ansatzes, wird sich der deutsche Mittelstand der Implementierung der Einzelbestandteile von GRC zukünftig nicht entziehen können und aus Effizienz- und Effektivitätsgründen wird die Entwicklung hin zu integrierten Konzepten gehen. Warum?

Zum einen steigen – wie zuvor gezeigt – die rechtlichen Anforderungen in den hier diskutierten Bereichen in den letzten Jah-

82 *Westhausen*, ZRFC 2021, 199, 200.

83 Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG), „Compliance im Mittelstand", 2014, S. 46 f., abrufbar unter: *https://opus.htwg-konstanz.de/frontdoor/deliver/index/docId/859/file/CBCI_Studie_Compliance_im_Mittelstand.pdf*.

84 S. dazu nur Thompson Reuter, „2023 Cost of Compliance", abrufbar unter: *https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-report-final-web.pdf*.

85 RegE KonTraG v. 28.1.1998 – BT-Drucks. 13/9712, S. 15, abrufbar unter: *https://dserver.bundestag.de/btd/13/097/1309712.pdf*.

86 Vgl. nur die Übersicht bei *Köhlbrandt/Gleißner/Günther*, Corporate Finance 2020, 248, abrufbar unter: *https://www.werner-gleissner.de/site/publikationen/WernerGleissner-offiziell-Nr-1514-Umsetzung-gesetzlicher-Anforderungen-an-das-RM.pdf*; s. auch *P. Ulrich/J. Barth/S. Lehmann*, KSI 2018, 154.

87 Deloitte, „Benchmarkstudie Risikomanagement 2023", Zehn Kernaussagen, abrufbar unter: *https://www2.deloitte.com/de/de/pages/audit/articles/benchmarkstudie-risikomanagement.html*.

88 *Eulerich/Gleißner*, ZCG 2021, 266, abrufbar unter: *https://futurevalue.de/wp-content/dokumente/FA_1904_Lines_of_Defense_und_ihre_Probleme_2021.pdf*.

89 S. etwa *Kembaren/Endro/Pendrian*, „Effect of governance, risk management and compliance on a firm's value (healthcare industry)", Enrichment: Journal of Management, 12 (5) (2022), 4076, abrufbar unter: *https://enrichment.iocspublisher.org/index.php/enrichment/article/download/947/746/&ved=2ahUKEwjqxo3gw66HAxUuRfEDHawrDeUQFnoECD4QAQ&usg=AOvVaw16uJA79rWpd_ZWMyE44gAL*, wonach der Unternehmenswert von 33,8 % der an der indonesischen Börse gelisteten Unternehmen aus dem Bereich der Gesundheitsvorsorge positiv mit einem vorhandenen GRC-System korreliert.

90 *Racz/Weippl/Seufert* (Fn. 35).

91 *Brühl/Hiendlmeier*, ZRFC 2013, 24.

92 Die Ergebnisse der Studien werden bei *Otremba* (Fn. 15), S. 146 f. gut zusammengefasst.

93 *Jäkel*, in: Compliance Manager, 2015, „Im GRC-Nirvana", abrufbar unter: *https://www.compliance-manager.net/artikel/im-grc-nirvana/*.

94 *Laue* (Fn. 23), S. 141 ff.

95 *Glaser*, ZRFC 2015, 56.

96 S. näher bei Institut für Mittelstandsforschung (Ifm), „Gründungen und Unternehmensschließungen", (2023), abrufbar unter: *https://www.ifm-bonn.org/statistiken/gruendungen-und-unternehmensschliessungen/unternehmensinsolvenzen*.

97 S. Meritus-Studie, a.a.O., S. 7.

ren stetig. So wird im Rahmen der aktuellen Fälle, wie die der bereits oben zitierten *Meyer-Werft* oder der *BayWa*, dem Management bereits jetzt die Frage gestellt, wie es denn um ihr Risikomanagement bestellt war, wenn die jeweilige Unternehmenskrise angeblich so „plötzlich" auftreten konnte.[98] Es erscheint nicht fernliegend, dass die Erkenntnisse aus diesen und weiteren Fällen, die im Zuge der sich aktuell verschärfenden Wirtschaftskrise „hochgespült"[99] werden, die Grundlage für weitere Verschärfungen der Rechtslage bilden – wie in den Zyklen zuvor Fälle wie *Vulkan* oder *Philipp Holzmann*. Angesichts der aktuellen „Rückfälle" in die Insolvenz dürften zudem Insolvenzverwalter vermehrt mit der Frage konfrontiert werden, warum die Sanierung im jeweiligen Insolvenzverfahren eben doch nicht „nachhaltig" war. In den bekannten Fällen erscheint es nicht fernliegend, dass schon in der zeitlich vorgelagerten Sanierungsplanung das Risikomanagement zu schwach ausgebildet war und/oder Unternehmensführung/Insolvenzverwalter sich etwas zu sehr in die eigene Sanierung verliebt hatten, ohne die Risiken angemessen zu gewichten. Dementsprechend werden es – ganz im Sinn der Maxime von Churchill, „*Never let a good crisis go to waste*" – gerade Restrukturierer und Insolvenzverwalter sein, die die sich derzeit mannigfaltig bietende „Chance" von Unternehmenskrisen nutzen und spätestens im Rahmen einer (insolvenzbedingten) Sanierung zielgerichtet entsprechende Strukturen und Prozesse aufbauen müssen, um die erforderliche operative Transformation sicherzustellen, schon um ihre eigenen Haftungsrisiken zu minimieren. Nicht ohne Grund wird bereits jetzt eine Risikofrüherkennung in der Insolvenz gefordert[100] und ein Plädoyer für die Einführung von Compliance-Standards in der Insolvenzverwaltung gehalten.[101] Zwar muss man berücksichtigen, dass eine Sanierung in der Insolvenz sich eigentlich nur auf die Stabilisierung der Liquiditätslage, eine Bilanzbereinigung (etwa durch einen Schuldenschnitt) und erste operative Eingriffe beschränken kann. Die erforderliche „nachhaltige Wettbewerbsfähigkeit" wird man erst in der Folge durch weitere operative und auch strategische Maßnahmen erreichen.[102] Dementsprechend werden Verwalter nur die ersten Schritte gehen können. Ein Sanierungscontrolling nach Aufhebung der Insolvenz oder im Rahmen einer außergerichtlichen Sanierung wird in der Folgezeit den effektiven Kulturwandel im Unternehmen überwachen müssen. Das Fehlen jeglicher Aktivitäten zur Implementierung der Einzelkomponenten von GRC, wenn nicht gar eines integrierten Ansatzes, dürften dagegen das Risiko einer potenziellen Haftung von Insolvenzverwaltern in Folgeverfahren zukünftig nicht unwesentlich erhöhen.

Zum anderen, weil nicht nur internationale Organisationen, wie IIA oder COSO, sondern auch nationale, wie der IDW e.V., mittlerweile in Richtung integrierter Systeme tendieren: Wie schon o.a., hat das IDW e.V. ab 2017 mit den sog. „IDW PS 98x" eine Sammlung von Standards für die Prüfung einzelner Bereiche geschaffen, die zusammengenommen ein GRC-System darstellen (können). Auch vormals eher kritische Stimmen nähern sich integrierten Systemen immer mehr an (s. dazu näher unten).

Schließlich darf man die frühen Wurzeln von GRC in der Software-Entwicklung nicht vergessen. Die zunehmende Digitalisierung aller Unternehmensbereiche und die fortschreitende Nutzung von Künstlicher Intelligenz (KI) dürfte integrierten (und damit zunächst einmal komplexeren) Systemen zu einer verbesserten Anwendbarkeit verhelfen. Schon heute werden zahlreiche „elektrische Helferlein" eingesetzt, um bei den Kernanliegen von Risk und Compliance zu unterstützen – von webbasierten Tools zur Liquiditätsplanung bis hin zu automatisierten Hotlines für Hinweisgeber-Systeme. Obwohl bereits jetzt beeindruckend, dürften diese Techniken[103] noch am Anfang stehen. Zukünftig wird die zunehmende Digitalisierung damit nicht nur eine kostengünstige Etablierung holistischer Governance-Systeme ermöglichen, sondern selbst zum Treiber von besseren (integrierten) Governance-Systemen werden.

Die Implementierung eines integrierten GRC-Konzeptes bietet zudem etliche Vorteile: Zum einen wird über durch die Interne Revision (IR) und das Internen-Kontroll-System (IKS) überwachten „Kontrollschleifen" (s. dazu näher unten III. 3.) die Um- und Durchsetzung unternehmerischer Entscheidungen erleichtert. Die so gesteigerte Professionalisierung führt zu einer Verbesserung der Wettbewerbsfähigkeit.[104] Eine gelebte GRC-Risikostruktur dürfte zudem helfen, Management-Fehler zu vermeiden und damit Haftungsrisiken reduzieren. Dementsprechend achten D&O-Versicherer verstärkt auf entsprechende Strukturen.[105] Ein etabliertes oder optimiertes GRC-System dürfte – so es nicht schon bereits den Eintritt von Krisenstadien zu verhindern hilft – zumindest zu milderen Krisenverläufen führen und etwaige Transformationsprozesse erleichtern. Darüber hinaus bildet es die Grundlage für *Business Continuity Management* und damit für ein „resilientes" Unternehmen.[106] Auch dürfte es bei der Unternehmensnachfolge eine nicht unwesentliche Rolle spielen.[107] Insgesamt ermöglicht GRC damit, die „Resilienz-Rendite" des Unternehmens zu kassieren.[108] Leider führt die Etablierung von GRC-Strukturen zumindest bislang nicht zu einem verbesserten Kredit-Rating bei Banken. Das dürfte sich aber bereits mit-

98 S. dazu vertiefend *Eulerich/Gleißner*, ZCG 2021, 266, abrufbar unter: *https://futurevalue.de/wp-content/dokumente/FA_1904_Lines_of_Defense_und_ihre_Probleme_2021.pdf*.

99 Frei nach Warren Buffet, „Man sieht erst, wenn die Ebbe kommt, wer die ganze Zeit über ohne Badehose geschwommen ist".

100 So *Nickert*, ZInsO 2023, 1797; *Spiekermann*, ZInsO 2024, 1517.

101 *Albrecht/Schütz/Taheri*, ZInsO 2022, 793.

102 S. dazu vertiefend schon *Beissenhirtz*, ZInsO 2016, 1778, 1789 ff.

103 S. zum Einsatz der IT allgemein, *Johannsen/Kant,* „IT-Governance, Risiko- und Compliance-Management (IT GRC)", in: HMD Praxis der Wirtschaftsinformatik, 2020, 1058, abrufbar unter: *https://link.springer.com/article/10.1365/s40702-020-00625-8*; zur Digitalisierung der Compliance, s. *Haselmeyer/Wockel*, in: ComplianceBusiness (2023), „Digitalisierung der Compliance", abrufbar unter: *https://www.deutscheranwaltspiegel.de/compliancebusiness/compliancepraxis/digitalisierung-der-compliance-31445/*.

104 Ausführlich: *Fissenewert*, „Compliance im Mittelstand", S. 31 f.

105 *Fissenewert*, ZCG 2023, 121; s. auch *Beissenhirtz*, „Pflicht zur Krisenfrüherkennung – eine tickende Zeitbombe?", Post (2023), abrufbar unter: *https://gunnercookede.com/pflicht-zur-krisenfruherkennung-eine-tickende-zeitbombe/*.

106 S. dazu näher etwa bei *Seibt*, DB 2016, 1978.

107 S. zum Letzteren nur *Fissenewert* (Fn. 104), S. 24.

108 So *Großehagenbrock*, „Die Resilienz-Rendite", Deutscher Anwaltsspiegel (2024), abrufbar unter: *https://www.deutscheranwaltspiegel.de/compliancebusiness/compliancepraxis/compliance-und-krisenmanagement-35760/*.

telfristig ändern,[109] denn die Banken werden sich in ihrem Wettbewerb mit anderen Banken auch mithilfe zinsgünstiger Kredite durchsetzen, die aber gleichwohl noch risikoadäquat bepreist sein sollten. Durch holistische Governance geführte Unternehmen dürften dabei besser abschneiden als Unternehmen ohne solche Systeme.

Allerdings kann selbst ein integriertes GRC-System nur ein Teil der Lösung sein, denn es bildet lediglich den Rahmen für die eigentliche unternehmerische Tätigkeit, es kann sie nie ersetzen.[110] Darüber hinaus besteht die Gefahr, die Themenstellung zu überfrachten, indem immer weitere Unterthemen auf dieselbe Hierarchie-Ebene gehoben werden. Schließlich kursiert eine schier unendliche Zahl von Ansätzen, wie die „richtige" Struktur auszusehen hat. Gerade für den Mittelstand ist allerdings eine einfache Struktur unerlässlich, um ihn vom Nutzen eines GRC-Systems zu überzeugen. Deswegen soll nachfolgend anhand der Mindeststandards eine erste einfache GRC-Struktur skizziert werden.

III. GRC – die Mindeststandards

Als konzeptionelle Grundlage für die erforderlichen Strukturen und Prozesse zur unternehmerischen Entscheidungsfindung und -durchsetzung bietet sich ein (modifizierter) „GRC"-Ansatz an, der die wesentlichen (Grenz-)Bereiche der unternehmerischen Tätigkeit abdeckt. Dieser integrierte Ansatz sollte zudem die in den o.g. Umfragen identifizierte Schwachstelle der bisherigen Bestrebungen zumindest mindern, nämlich in Bezug auf die eingesetzten Ressourcen einen messbaren Mehrwert für das Unternehmen genieren.[111] Auch aus Kosten-Nutzen-Erwägungen heraus sollte die Geschäftsleitung konzeptionell eine „GRC-Ziel-Pyramide" entwickeln, die zunächst die zu erfüllenden Mindeststandards erfasst, worauf in späteren Zyklen weitere Komponenten, wie etwa branchenweite Standards („*Best Practices*") oder „*Soft Law*" der *Corporate Social Responsibility*, aufgesetzt werden können.

Dementsprechend sollen nachfolgend die von der Geschäftsleitung zu beachtenden – branchen- und größenunabhängigen – Mindeststandards näher vorgestellt werden.

1. (Corporate) Governance

„Corporate Governance" ist „*der rechtliche und faktische Ordnungsrahmen für die Leitung und Überwachung von Unternehmen.*" Zumeist wird diese Definition heutzutage ergänzt um die Wendung „*zum Wohl aller relevanten Anspruchsgruppen (= Stakeholder)*", und demnach eben nicht nur der Anteilsinhaber (= *Shareholder*).[112] So wird aus der eher technischen Definition ein Anspruch, eben die „*Good Corporate Governance*". Der Ordnungsrahmen wird maßgeblich durch Gesetzgeber und Eigentümer bestimmt. Die konkrete Ausgestaltung dieses Rahmens obliegt dann den Aufsichtsorganen und der Unternehmensführung. Das unternehmensspezifische Corporate-Governance-System besteht somit aus der Gesamtheit relevanter Gesetze, Richtlinien, Kodizes, Absichtserklärungen, dem Unternehmensleitbild und Gewohnheiten der Unternehmensleitung und -überwachung.

Grundlegend sollte ein Unternehmen also über eine „Verfassung" verfügen – dies ist zumeist der Gesellschaftsvertrag bzw. die Satzung. Daneben treten dann die in Abb. 2 genannten Dokumente zur strategischen und operativen Aufstellung, Entwicklung und Zielrichtung des Unternehmens. Aus dem Blickwinkel des Risikomanagements ist von diesen die Strategieentwicklung hervorzuheben. Im Rahmen der dabei regelmäßig durchgeführten *SWOT*-Analyse[113] werden die sich aus der Risiko-Analyse ergebenden Chancen („*Opportunities*") und Risiken („*Threats*") ausgewertet und der Umgang damit festgelegt.[114] Aus dieser Dokumentation müssen sich die Unternehmensorganisation – Geschäftsleitung, etwaige Aufsichtsorgane, Abteilungsstrukturen etc. – sowie grundlegende Prozesse des Unternehmens ableiten lassen (was sich auch in grafischen Darstellungen und Organigrammen niederschlagen sollte). Zusammen mit den daraus abgeleiteten Geschäftsordnungen bilden sie die verschriftlichte Grundlage der Governance im Unternehmen.

2. Risikofrüherkennung und -management

Zunächst ist für diese „Säule" des GRC-Konzepts eine Klärung der in diesem Bereich vorherrschenden Begrifflichkeiten vorzunehmen, da häufig „Krise" und „Risiko" sowie „Erkennung" und „Management" synonym verwandt werden. Während ein „Risiko" allgemein als Möglichkeit eines Schadens oder Verlustes als Konsequenz eines bestimmten Verhaltens oder Geschehens definiert wird,[115] entstammt der Begriff „Krise" dem Griechischen und bezeichnet ursprünglich den Bruch einer bis dahin kontinuierlichen Entwicklung. Die Unternehmenskrise, als spezielle Form der Krise, weist zumeist folgende Merkmale auf: Das Unternehmen befindet sich in einer – nachhaltig, ungewollt sowie ungeplant – existenzbedrohenden Situation, deren Ausgang ungewiss ist. Die Unternehmenskrise ist durch ihren Prozesscharakter gekennzeichnet, wobei der Prozess autonom abläuft. Der Prozess lässt sich zwar beeinflussen, der tatsächliche Einfluss stellt allerdings besondere Anforderungen an die Qualität des Managements.[116] Während Risiken eher generell-abstrakt sind, ist eine (Unternehmens-) Krise spezifisch und konkret. Die (Früh-)Erkennung beschäftigt sich mit der Frage, wie man ein Risiko oder eine zukünftige Krise erkennen kann, während das (Risiko- und Krisen-)-Management den Umgang mit erkannten Risiken/ Krisen regeln soll. Dabei umfasst das Risiko-Management im weiteren Sinne auch die Risiko-Früherkennung.

---

109 So auch *Fissenewert* (Fn. 104), S. 24.

110 So auch *Gleißner*, „Integratives Risikomanagement", Controlling 2020, 23, abrufbar unter *https://futurevalue.de/wp-content/uploads/2022/03/FA-1813-Integratives-Risikomanagement-Schnittstellen-2020.pdf*.

111 So auch *Otremba* (Fn. 15), S. 143.

112 Zum aktuellen Stand der Diskussion zur Durchsetzung des Stakeholder Value, s. nur *Lotz*, „Das Ende des Shareholder Value?" (2021), abrufbar unter: *https://www.ghst.de/fileadmin/images/02_Formulare_und_Dokumente/Essaypreis_2021_Carsten_Lotz_-_Das_Ende_des_Shareholder_Value.pdf*.

113 S. zum Prozess der Unternehmensplanung näher bei *Ihlau/Duscha*, BB 2013, 2346, 2349.

114 S. auch *Scherer*, CCZ 2012, 201, 205.

115 S. nur RiskNet, Glossar & Definitionen, „Risiko", abrufbar unter: *https://www.risknet.de/wissen/glossar/?tx_a21glossary_pi1%5Bchar%5D=Risiko%20%28Definition%29&cHash=6fa138b3794c9cd4af5ea30367c6fad1*.

116 Nach *Krystek*, Die Unternehmenskrise, S. 9.

Zwar ist die Regelung des § 1 StaRUG mit „Krisenfrüherkennung und Krisenmanagement" überschrieben,[117] in der Regelung selbst, wie auch bei § 91 Abs. 1 AktG, wird allerdings der Terminus der „bestandsgefährdenden Entwicklungen" verwandt. Der IDW PS 340 definiert solche bestandsgefährdenden Entwicklungen als „*Risiken, die einzeln oder im Zusammenwirken mit anderen Risiken dem Ziel der Unternehmensfortführung entgegenstehen können*".[118] Somit setzen die v.g. Regelungen bereits bei abstrakten Risiken und nicht erst bei einem bestimmten Krisenstadium an.[119]

Bei der Implementierung des RMS ist auch kritischen Stimmen Rechnung zu tragen, die vor dem Hintergrund der oftmals bereits in Unternehmen etablierten Compliance-Regelungen davor warnen, Risiko lediglich als Gefahr zu verstehen, welche es zu vermeiden bzw. zu minimieren gelte.[120] So bezeichnet etwa *Otremba* das Risikomanagement als „*systematische Identifikation, Analyse und Bewertung, Bewältigung sowie Dokumentation und Berichterstattung von internen und externen Ereignissen, die das Potential aufweisen, ein definiertes Ziel zu verfehlen (Gefahr) oder zu übertreffen (Chance).*"[121] Auch *Gleißner* fordert ein „entscheidungsorientiertes Risikomanagement", bei dem die Chancen, die sich dem Unternehmen bieten, gleichwertig neben den Risiken abgebildet werden.[122] Wie bereits oben zur Governance ausgeführt, ist dieser Aspekt des „Chancenmanagements" im Rahmen der Strategieentwicklung des Unternehmens zu berücksichtigen. Tatsächlich ist jegliches RMS somit auch als „Chancenmanagement" zu begreifen und muss dementsprechend im Rahmen der „*Opportunities*" im Rahmen einer *SWOT*-Analyse Eingang in die Unternehmensplanung finden. Auch sind CMS und RMS nicht um ihrer selbst willen zu betreiben, sondern konsequent im Sinne der unternehmerischen Entscheidungsfindung („Governance") auszurichten.[123]

Die gesetzlichen Regelungen selbst enthalten keinerlei Vorgaben für die Ausgestaltung eines Risiko-Management-Systems (RMS), genau so wenig wie bislang die Rechtsprechung. Sowohl die internationalen wie auch die nationalen Standards überspannen regelmäßig die Anforderungen an mittelständische Unternehmen.[124] Gleichwohl können diese Standards als Handreichung bei der Planung eines RMS gute Dienste erweisen. So enthält der IDW PS 981 neben einer Definition des RMS („*Gesamtheit der Regelungen, die einen strukturierten Umgang mit Risiken (i.S.v. positiven und negativen Zielabweichungen) im Unternehmen sicherstellt*", vgl. IDW PS 981 Rn. 18.) auch acht sog. „Grundelemente" eines RMS, die miteinander in Wechselbeziehung stehen (vgl. näher bei IDW PS 981 Rn. 31 ff.). Nämlich die Festlegung der Risikokultur sowie der Ziele und der Organisation des RMS, die Risikoidentifikation und -bewertung, die Risikosteuerung und -kommunikation sowie die Organisation der Überwachung und Verbesserung des RMS.[125] Schließlich hat das Deutsche Institut für interne Revision (DIIR) bereits 2018 einen „Revisionsstandard Nr. 2 – Prüfung des Risikomanagementsystems durch die interne Revision" entwickelt, der zuletzt 2022 unter Berücksichtigung der Vorgaben des StaRUG überarbeitet wurde.[126]

Als (größenunabhängige) Mindestanforderung an ein gesetzeskonformes RMS dürfte eine integrierte rollierende Finanzplanung mit einer monatsbasierten Liquiditätsplanung gelten, die regelmäßig einen Zeitraum von 24 Monaten abzudecken hat (und damit zugleich auch der zeitliche Anwendungsbereich der drohenden Zahlungsunfähigkeit nach § 18 InsO ist)[127], sowie die Berücksichtigung der nach § 101 StaRUG vom BMJ veröffentlichten „Informationen zu Frühwarnsystemen".[128] Derartige Planungen werden regelmäßig sowieso im Rahmen eines Controlling-Prozesses erstellt. Das Controlling ist damit Teil des GRC (s. dazu auch unten).[129] Bestimmte, vorab festgelegte Unternehmenskennzahlen, wie etwa die Eigenkapitalquote oder Liquiditätskennziffern, bilden als sog. „Frühwarn-System" den Mindeststandard für ein Risikofrüherkennungssystem in Unternehmen. Darüber hinaus sollte eine schriftliche Dokumentation der Strategie im Umgang mit Risiken (Kultur, Ziele und Organisation), der Risikoanalyse und -steuerung (Festlegung der zu beobachtenden Risiken,[130] Maßnahmen bei erkannten Risiken bzw. Krisen), der Risikokommunikation sowie der entsprechenden Kontrollsysteme zumindest in Anlehnung an IDW PS 981 erfolgen. Die aus diesen Instrumenten gewonnen Erkenntnisse sind zu aggregieren, es sollte also das oben bereits genannte „Zusammenwirken" erkannter Risiken simuliert werden. Dazu sind Sensitivitätsanalysen bzw. Szenariorechnungen durchzuführen.[131] Je nach Größe des Unternehmens und (aus der Risikostrategie abgeleitetem) Risikoappetit sollte darüber hinaus eine Aggre-

117 S. grundlegend zu § 1 StaRUG nur *Gleißner/Haarmeyer*, ZInsO 2024, 173.

118 So auch *Steffan/Poppe/Roller*, KSI 2022, 53, 54 m.w.N., s. auch *Seibt*, BB 2019, 2563.

119 So aber noch *Haghani*, NZI-Beilage 2019, 20, 21.

120 So *Gleißner*, Risknet, „GRC-Konzepte führen in die Sackgasse", abrufbar unter: *https://www.risknet.de/themen/risknews/grc-konzepte-fuehren-in-die-sackgasse/*.

121 *Otremba* (Fn. 15), S. 106.

122 *Gleißner*, DB 2018, 2769.

123 So zu Recht *Gleißner*, Controlling 2020, 23, abrufbar unter *https://futurevalue.de/wp-content/uploads/2022/03/FA-1813-Integratives-Risikomanagement-Schnittstellen-2020.pdf*.

124 So auch *Steffan/Poppe/Roller*, KSI 2022, 53, 55.

125 S. für eine einfache Darstellung RiskNet, „Der Prozess des Risikomanagements", abrufbar unter: *https://www.risknet.de/wissen/risk-management-prozess/*; s. zur potenziellen Nutzung des ISO 31000 im Mittelstand *Herdmann/Henschel*, ZRFC 2018, 111, zur Vorgängerregelung des ISO 19600 s. bereits *Fissenewert* (Fn. 104), S. 51 ff.

126 Der Standard ist abrufbar unter: *https://www.diir.de/content/uploads/2023/09/DIIR_Revisionsstandard_Nr._2_Version_2.1.pdf*; s. dazu auch *Gleißner*, ZIR 2022, 112.

127 *Jacoby/Thole*, StaRUG, § 1 Rn. 16; *Pannen/Riedemann/Smid*, StaRuG, Rn. 50; *Bea/Dressler*, NZI 2021, 67, 70.

128 *Jacoby/Thole* (Fn. 127), § 1 Rn. 16.

129 Liste abrufbar unter: *https://www.bmj.de/DE/themen/wirtschaft_finanzen/schulden_insolvenz/fruehwarnsysteme/fruehwarnsysteme.html*; s. dazu auch RMA, „Integriertes Risikomanagement: von GRC zu GRC²", abrufbar unter: *https://rma-ev.org/news-publikationen/news-risk-blog/einzelansicht-blog/integriertes-risikomanagement-von-grc-zu-grc2*; *Gleißner/Ulrich*, ZfRM 4/2024, 88; *Gleißner*, Controlling 2020, 23, 26; s. auch *Beissenhirtz*, ZInsO 2020, 1673, 1681 ff., mit weiteren Hinweisen zur Integration des Controlling in die Gesamtstruktur.

130 S. hierzu *Gleißner*, BC 2022, 217; *Beissenhirtz*, ZInsO 2020, 1673; für ein Beispiel eines einfachen Risiko-Handbuchs, s. die entsprechende Mustervorlage bei RiskNET, abrufbar unter: *https://www.risknet.de/fileadmin/risknetwork/download/RM-Handbuch.rtf*.

131 *Ihlau/Duscha*, BB 2013, 2346, 2349.

gation nach der sog. „Monte-Carlo-Methode" erfolgen.[132] Schließlich ist die Überwachung des RMS zu regeln und der gesamte Prozess als Kreislauf anzulegen, der in von der Geschäftsleitung festzulegenden Zyklen (die mit der übrigen Unternehmensplanung synchronisiert werden müssen!) immer wieder durchlaufen wird.

3. Compliance-Management

Wie im Bereich der Governance und des Risiko-Managements, so existieren auch bei der Planung und Implementierung eines Compliance-Management-Systems (CMS) keine gesetzlichen Vorgaben und das oben zitierte Urteil des OLG Nürnberg legt lediglich die Pflicht für Unternehmen jeglicher Größe fest, ein CMS zu etablieren. In dem ebenfalls bereits oben zitierten „*Neubürger-Urteil*" hatte das LG München zudem vorgegeben, dass „*entscheidend für den Umfang [des CMS] im Einzelnen […] Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit [sind].*" Sprich, die Unternehmensgröße spielt bei der konkreten Ausgestaltung eines CMS durchaus eine Rolle. Daneben werden das Betätigungs- und Geschäftsfeld sowie die Art der Tätigkeiten des Unternehmens Anhaltspunkte für die konkrete Ausgestaltung des CMS geben.[133] Damit sind inhaltliche Mindestvorgaben an ein CMS – wie etwa bei RMS die Liquiditätsplanung – grds. nicht möglich.[134] Die strukturellen Mindestvorgaben lassen sich aber wieder aus den einschlägigen Standards ableiten. So enthält der IDW PS 980 ab Rn. 27 eine in weiten Teilen strukturell analog zum IDW PS 981 für RMS angelegte Darstellung von „Grundelementen eines CMS", die als Ausgangspunkt für die Planung und Implementierung der Organisation und Prozesse eines CMS dienen können. Die DICO hat zudem mit dem „Arbeitspapier A12 – Compliance-Baukasten für den Mittelstand"[135] eine Arbeitshilfe entwickelt, die strukturell dem IDW PS 980 folgt. Bei der Identifizierung der für das jeweilige Unternehmen spezifischen compliance-relevanten Themenstellungen kann die darin entwickelte generische Übersicht[136] helfen. So werden sich nur die wenigsten Unternehmen einer Auseinandersetzung mit den Themen Steuern, Arbeitsrecht und Datenschutz entziehen können. Diese und weitere Kernthemenstellungen wird die Unternehmensleitung durch die Compliance-Risikoanalyse identifizieren und in einem CMS berücksichtigen müssen.

4. Integration der Einzelsysteme in „GRC²+"

So wenig es verbindliche Vorgaben für die Ausgestaltung der einzelnen Elemente von GRC gibt, so existiert erst recht kein Standard zum Aufbau eines integrierten Systems. Gleichwohl legt bereits der prozessuale Gleichlauf von RMS und CMS eine Integration der Systeme nah.

„Mentale" Grundlage jeglicher Integration ist zunächst die Änderung gerade der Denkweise (des „*Mindsets*") der Compliance. Wie bereits o.a., definiert Compliance eher die Grenzen des rechtlichen (oder reputationsbedingt sinnvollen) *Dürfens*, während das Risikomanagement eher die Grenzen des wirtschaftlichen *Könnens* bestimmt. Beide Aspekte müssen im Rahmen der unternehmerischen Entscheidungsfindung grds. gleichwertig in die Betrachtungen mit einbezogen werden. Während die Denkweise des Risikomanagements davon geprägt ist, dass es nicht möglich ist, unternehmerische Risiken vollständig auszuschließen, sondern der unternehmerische Erfolg gerade durch einen geschickten Chancen-Risiko-Mix erreicht wird, liegt dem – eher legalistisch geprägten – Compliance-Management häufig eine „Null-Risiko-Denkweise" zugrunde. Im Hinblick auf den angestrebten entscheidungsorientierten Ansatz des GRC-Systems muss die Compliance-Risikoanalyse somit aus dem grundlegenden Verständnis der Risikoanalyse lernen, damit die Systeme kompatibel werden und ein integriertes System entsteht.[137] Dabei wird man bereits auf Ebene der Compliance-Risiko-Analyse an den (durchaus anschaulichen) Matrix- bzw. „Ampel"-Systemen[138] ansetzen und rechtliche (oder gar Reputations-)Risiken konkret „bepreisen" müssen. Dies kann gut z.B. durch den Ansatz von Kosten für etwaige Sanktionen bei Verstößen (etwa Bußgelder bei Verstößen gegen die Datenschutz-Compliance) geschehen, denen die Kosten für die Compliance mit den entsprechenden Vorschriften als „*mitigating factor*" gegenüber gestellt werden. Durch diesen zahlenbasierten Ansatz lässt sich auch eine Risikoaggregation wesentlich besser gestalten und die Szenarioanalyse oder gar eine Monte-Carlo-Analyse können dann auch realistisch Compliance-Risiken abbilden.

Die *prozessuale* Grundlage eines integrierten Systems bildet das GRC-Rahmenwerk. Ausgangspunkt ist dabei der „GRC-Regelkreis", bestehend aus der (GRC-)Risikostrategie/-identifikation, der Risikobewertung und der Risikosteuerung.[139] Zur wechselseitigen Integration dient neben der oben skizzierten Änderung des Denkansatzes bei der Compliance-Risikoanalyse die ebenfalls bereits oben angesprochene „Überkreuzprüfung" durch die Compliance-Abteilung im Hinblick auf das gesetzeskonforme Vorhandensein eines RMS sowie durch die Risiko-Abteilung im Hinblick auf die vom CMS aufgezeigten Compliance-Risiken. Dieses wird, wie bereits in Abb. 2 oben gezeigt, aus dem Zusammenspiel zwischen den Grundlagen der Unternehmensstrategie und den Grundlagendokumenten der einzelnen Bereiche zusammengestellt, und bildet selbst den oben beschriebenen GRC-Regelkreis ab. Zusätzlich werden auf dieser Stufe bereits die

---

132 S. dazu näher bei *Gleißner*, „Grundlagen des Risikomanagements", S. 309 ff.; grundlegend auch *Kühne/Nickert*, „Wann ist eine insolvenzrechtliche Prognose positiv?", ZInsO 2014, 2297, abrufbar unter: *https://www.schrittmacher-kanzlei.de/wp-content/uploads/2023/06/ZinsO_Wann_ist_eine_insolvenzrechtl._Prognose_positiv.pdf*; *Steffan/Poppe/Roller*, KSI 2022, 53, 59.

133 S. vertiefend dazu bei *Bock*, ZIS 2009, 68, 75, abrufbar unter: *https://www.zis-online.com/dat/artikel/2009_2_293.pdf*.

134 So auch *Wilhelm*, ZRFC 2013, 133.

135 Abrufbar unter: *https://www.dico-ev.de/wp-content/uploads/2021/04/A12_ComplianceBaukasten_Mittelstand.pdf*.

136 S. DICO, a.a.O. (Fn. 135), S. 13.

137 S. auch *Gleißner*, Controlling 2020, 23, 25.

138 S. dazu *Haberhauer*, CCZ 2017, 78, 80; *Ozip-Philippsen*, ZRFC 2013, 203, 207.

139 Vgl. dazu *Otremba* (Fn. 15), S. 152, *Laue* (Fn. 23), S. 120.

GRC-Organisation (nachfolgend näher erläutert), GRC-Technologie und GRC-Kommunikation beschrieben.

In Bezug auf die *Organisation* des integrierten GRC-Managements kann die Unternehmensführung positiv gesehen aus einer Vielzahl von Modellen auswählen. Neben dem eher aus Governance-Sicht stammenden „House of Corporate Governance"[140] oder dem eher aus Risiko-Sicht konzipierten (bereits o.g.) „*Three-Lines-Model*" und dem „*COSO-ERM*"-Ansatz existieren auch individuelle Vorschläge zur Integration.[141] Aus Sicht mittelständischer Unternehmen bietet sich eine an das (eher noch einfach ausgestaltete) sog. „*House of Governance*" angelehnte, allerdings modifizierte, Struktur für die Organisation der Systemintegration an. Wie bereits o.a. ist das Controlling des Unternehmens nämlich sozusagen als Fundament eines integrierten GRC-Ansatzes („GRC²") anzusehen[142] und ist deswegen als weiteres Element in das „Haus" aufzunehmen.

Neben der Schnittstelle zum Controlling ist aber auch die Schnittstelle sowohl zur (soweit vorhanden) Internen Revision (IR) als auch zum Internen-Kontroll-System (IKS) herzustellen. Diese Systeme bilden die bereits oben genannte „Kontrollschleife" und dienen damit dem Monitoring von CMS und RMS.

Ein Internes Kontrollsystem (IKS) besteht aus systematisch gestalteten technischen und organisatorischen Regeln des methodischen Steuerns von Kontrollen im Unternehmen zum Einhalten von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können.[143] Die „Interne Revision" (IR) dagegen ist eine Institution, die unabhängige Prüfungs- und Beratungsleistungen (für die Unternehmensleitung) erbringt. Sie soll die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewerten und verbessern.[144]

Die IR ist eine betriebsinterne Organisation, während das IKS betriebsinterne (Prüfungs-)Prozesse beschreibt. Die Organisationseinheit IR überwacht auch die Tätigkeit der Compliance- und Risiko-Management-Abteilungen. Nach der bereits oben zitierten Entscheidung des OLG Nürnberg ist als IKS zumindest die Einführung des Vier-Augen-Prinzips bei wichtigen Transaktionen als rechtlich verpflichtend anzusehen. Zwar werden beide Bereiche organisatorisch regelmäßig direkt im Risikomanagement verortet.[145] Eine zu enge Verknüpfung des Risikomanagements mit der IR wird allerdings als problematisch angesehen, weil sie für die unabhängige Überprüfung des Risikomanagements verantwortlich ist. Im *Three-Lines-Model* werden die Funktionen deswegen getrennt.[146]

Das hier verfolgte „GRC²+"-Modell basiert also auf einem entsprechend strukturierten Controlling (deswegen „²") und verfügt zusätzlich über definierte Schnittstellen zum IKS und (soweit existent) zur IR (deswegen „+"; insgesamt also „GRC²+).[147] Diese Organisationen sind in den Ablauf des GRC-Regelkreises mit einzubeziehen und haben ihrerseits ihre jeweilige Organisation im Sinne eines entscheidungsorientierten Ansatzes anzupassen.

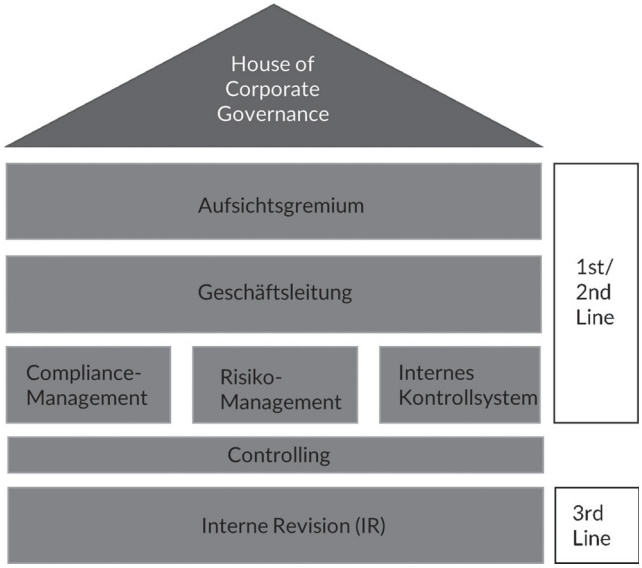

Abb. 3 – „GRC²+ – House of Corporate Governance" (nach *Gnändiger*, 2013).

IV. Praktische Hinweise zur Implementierung von GRC in KMU

Nach diesen Ausführungen zu den Mindeststandards eines integrierten Systems sollen dem mittelständischen Unternehmer/Geschäftsführer zum Abschluss noch einige übergreifende Denkanstöße zum effektiven und effizienten Aufbau eines integrierten Systems an die Hand gegeben werden.

1. „Erst verloren wir das Ziel aus den Augen, dann verdoppelten wir unsere Anstrengungen"

Nicht zufällig wurde in Abb. 2 der „GRC-Dreiklang"[148] als Rahmen für die Dokumentation der Unternehmenskultur und -strategie gesetzt.[149] Denn nur wenn das Ziel des Unternehmens klar

140 *Gnändiger*, StuB 2013, 182.

141 So *Otremba* (Fn. 15), S. 151 ff.; *Henschel/Heinze*, Governance, Risk und Compliance im Mittelstand, 2016, S. 62 ff.

142 S. dazu nur die Darstellung bei *Gleißner*, Controlling 2020, 23, 24.

143 Zitiert nach Wikipedia, abrufbar unter: *https://de.wikipedia.org/wiki/Internes_Kontrollsystem*; s. aber auch IDW PS 261 Rn. 19; zur Diskussion um die Begrifflichkeiten, *Koch*, AktG, § 91 Rn. 17 ff.; *Fischer/Schuck*, NZG 2021, 534, 537.

144 Nach *Otremba* (Fn. 15), S. 91; s. auch *Fischer/Schuck*, NZG 2021, 534, 537.

145 S. nur die Übersicht bei *Glaser*, ZRFC 2015, 56, 58.

146 S. dazu das Schaubild bei *Gleißner*, Controlling 2020, 23, 28; dabei soll nicht verkannt werden, dass ein derartiges „Trennungsmodell" genau der Systemintegration zuwiderläuft und (erneut) zum Silodenken einlädt, s. nur *Laue* (Fn. 23), S. 19. Dieses Risiko ist bei der konkreten Wahl der Organisationsform mit den Erfordernissen einer effektiven Überwachung abzuwägen. Lösungen können hier bislang nur individuell gefunden werden.

147 S. auch *Brühl/Hiendlmeier*, ZRFC 2013, 24.

148 So *Glaser*, ZRFC 2015, 56.

149 Zur Entwicklung einer Unternehmensstrategie s. schon *Schwab/Kroos*: „Moderne Unternehmensführung im Maschinenbau", VDMA, 1971, abrufbar unter: *https://www3.weforum.org/docs/WEF_KSC_CompanyStrategy_Presentation_2014_DE.pdf*.

definiert ist, kann ein GRC-System sich danach ausrichten und überhaupt wirksam werden. Die Entwicklung der Unternehmensstrategie gleicht in Relation zu Compliance und Risiko der berühmten Huhn-Ei-Diskussion. Denn um eine wettbewerbsfähige Strategie zu entwickeln, muss man die rechtlichen und wirtschaftlichen Rahmenbedingungen – und damit Chancen und Risiken – des Unternehmensumfeldes ebenfalls ausleuchten.[150] Allerdings folgt auch die Entwicklung einer Unternehmensstrategie einem Zyklus – das Ende der Entwicklung ist der erneute Anfang des Kreislaufs.[151] So gesehen wird sich die Entwicklung der Strategie auch immer wieder am jeweils aktuellen Stand des RMS und CMS orientieren.

2. GRC-Rahmenwerk, (Unter-)Ziele und erste Strukturen setzen

Um eben nicht ziellos durch die GRC-Welt zu segeln, ist es erforderlich, aus der Unternehmensplanung heraus das GRC-Rahmenwerk zu erstellen. Dies wird regelmäßig auch im Hinblick auf – oftmals schon vorhandene (s.u.) – Komponenten in einem iterativen Prozess erfolgen. Dabei wird man z.B. bei Erstellen der Compliance-Strategie zunächst auch rein plakative Ziele akzeptieren (etwa: „Korruptionsrisiken minimieren"). Danach ist ein weiteres Herunterbrechen dieser Ziele auf die jeweiligen Hierarchieebenen des Unternehmens erforderlich.[152] Bei der Zielfindung ist zunächst zu klären, was die Geschäftsleitung aus GRC-Sicht tun *muss*, wo sie also keinen Ermessensspielraum hat. Die weiteren Ziele sind an der gelebten Praxis des Unternehmens („Kultur"), etwaigen Branchenstandards und „*Soft Law*" im Sinne einer „*Best Practice*" auszurichten. Dabei muss ein GRC-System in einer „*high-trust organisation*" anders aussehen als in einer „*low-trust organisation*".[153] Auf diese unternehmensspezifischen Mindeststandards und *Best Practices* können dann weitere Ziele – etwa im Rahmen von CSR/ESG – aufgesetzt werden, sodass sich eine „GRC-Ziel-Pyramide" herausbildet.[154]

3. „Culture Eats Strategy for Breakfast"

Dieses dem Management-Vordenker *Peter Drucker* zugeschriebene Zitat sollte nicht nur die oberste Leitlinie bei der Implementierung eines GRC-Konzeptes sein, sondern auch als Mahnung an jeden Unternehmer, Geschäftsleiter oder Sanierer/Restrukturierer gelten. Nicht umsonst betonen alle einschlägigen Standards immer wieder die Erforderlichkeit einer „Compliance-" oder „Risiko-Kultur" und dass der „*tone from the top*" entscheidend sei für die Erreichung der Compliance-, bzw. Risiko-Ziele sei. Freilich folgt gerade die Entwicklung einer Unternehmenskultur ganz anderen Zeitläuften und Bedingungen („Vertrauen gewinnt man in Tröpfchen und verliert es in Litern.") als die eines Strategiepapiers. Jeder Sanierer kann davon ein Lied singen. Dementsprechend sollte bei jeglicher Planung von GRC-Strukturen auch die – in den o.g. empirischen Untersuchungen immer wieder betonte – Vertrauenskultur in mittelständischen Unternehmen berücksichtigt werden.[155]

4. Ansetzen beim schon Vorhandenen

Es wird nur wenige Fälle geben, in denen Unternehmen auch heute noch überhaupt keine Prozesse und Organisationsstrukturen etabliert haben, die auch GRC (oder IKS/IR) dienen. Vielmehr dürften häufig zumindest einzelne Aspekte der Compliance oder des Risikomanagements etabliert sein, etwa zum Datenschutz – mitsamt entsprechenden Prozessen und einem verantwortlichen (externen) Datenschutzbeauftragten – oder eine Liquiditätsplanung.[156] Diese „GRC-Inseln" gilt es bereits in der Analyse-Phase zu identifizieren und in das zu schaffende System zu integrieren.

5. Anamnese – die (GRC-)Risiko-Analyse

Grundlage jeglicher Anamnese ist die o.g. Unternehmensplanung. Wie o.a. ist die (integrierte) Risiko-Analyse die Grundlage für die Etablierung eines GRC²+-Systems. Da sowohl der Einführung eines Compliance- als auch eines Risiko-Management-Systems eine Risikoanalyse – mit vielfachen Überschneidungen – zu Grunde liegt,[157] kann man sich dies zu Nutze machen. Viele Fragen aus den beiden Katalogen sind ähnlich bzw. identisch und umfassen die Corporate Governance.

6. Vom „pragmatischen" Start zum „eingeschwungenen" GRC-System

Nach diesem pragmatischen Start sollte erstmalig der Regelkreis der Systeme durchlaufen und damit ein Basis-GRC-System aufgestellt werden, das zumindest den oben skizzierten rechtlichen Mindestanforderungen genügt. Das mehrfache Durchlaufen der Regelkreise unter Abarbeitung der im jeweiligen vorherigen Durchgang aufgedeckten Schwachstellen führt nach einiger Zeit zu einem „eingeschwungenen"[158] GRC-System.

7. „*Checks and Balances*"

Jedes GRC-System wird nur so gut sein wie die Menschen, die es anwenden und durchsetzen. Und damit kommt erneut Corporate Governance ins Spiel, die durch die Besetzung der für GRC wichtigen Positionen[159] aber auch die Etablierung von Kontrollinstanzen (Beiräte, Aufsichtsräte, externe Compliance-Beauftragte) für eine Struktur von „*checks and balances*"

---

150 S. dazu bereits *Porter*, „Competitive Strategy", 1980.

151 „Pläne sind nichts, Planung ist alles", Dwight D. Eisenhower.

152 S. vertiefend zu Compliance-Zielen etwa *Schefold*, ZRFC 2012, 253.

153 S. dazu näher bei *Dobler*, KSI 2011, 64, abrufbar unter *https://ksidigital.de/ce/ausbau-des-risikomanagement-und-compliance-systems-in-besonders-schwierigem-unternehmensumfeld/detail.html*.

154 Vgl. *Boehringer*, Compliance kompakt, S. 36 f.; *Scherer*, CCZ 2012, 201, 202.

155 „Jede neue Regel reduziert die Übernahme von Verantwortung", Christoph Babendererde, abrufbar unter: *https://www.linkedin.com/posts/christoph-babendererde_m%C3%BCssen-wir-denn-wirklich-alles-vorschreiben-activity-7204731381824794626-oWf1/*.

156 So auch *Lindemann/Menke*, CCZ 2022, 85, 91, „Sie haben mehr, als Sie glauben".

157 S. näher zum „GRC-Regelprozess" aus „Risikoidentifikation, Risikobewertung und Risikosteuerung" nur *Laue* (Fn. 23), S. 119 f.

158 Nach *Kark*, „Plötzlich Compliance Officer", S. 25, 81.

159 S. nur *Jack Welch* zum Strategie-Team eines Unternehmens: „*Comprise a organization's best minds […]. And, importantly, people with a propensity for paranoia – not just what-if-ers, mind you, but worst-casers*", in: *Welch*, The Real Life MBA, S. 32; s. auch *Pohlmann*, in: Juve, „Das Management muss einen starken General Counsel aushalten", abrufbar unter: https://www.juve.de/markt-und-management/das-management-muss-einen-starken-general-counsel-aushalten/.

sorgen muss, bei der das Ziel einer effektiven und effizienten Entscheidungsfindung im Vordergrund steht und die o.g. Überbetonung eines Bereichs zulasten anderer möglichst ausgeschlossen wird.[160] Gerade die Etablierung eines Aufsichts- oder Beirates kann die unternehmerische Entscheidungsfindung, aber auch die Stabilität der Unternehmensführung in Krisenzeiten (z.B. bei Ausfall der Geschäftsführung)[161] absichern.[162]

8. *„Vertrauen ist gut…"*

… und Kontrolle nicht immer besser. Aber ganz ohne Aufsicht und Kontrolle (IKS!) wird es auch in den häufig vertrauensgetriebenen mittelständischen Unternehmen nicht gehen – schon die Rechtsprechung verlangt danach. Wie ein Mindestmaß an Kontrolle und Revision im jeweiligen Unternehmen jenseits des Vier-Augen-Prinzips auszugestalten ist, entscheidet sich im jeweiligen Unternehmen. Ansätze eines IKS und einer IR schon in die Governance-Systeme zu integrieren, erscheint – nicht nur vor dem Hintergrund der o.g. Entscheidung des OLG Nürnberg – allerdings immer ratsam.

9. Konsequenzen & Sanktionen

Verstöße gegen die festgelegten Regeln müssen zu Sanktionen führen, ansonsten werden die (neuen) Regeln das bestehende System (die „Kultur") nicht nachhaltig beeinflussen können.[163] Dementsprechend ist für Verstöße gegen Compliance-Regelungen ein abgestufter Sanktionskatalog erforderlich. Bei „falschen" unternehmerischen Entscheidungen, aus deren Blickwinkel dieser Artikel vornehmlich verfasst ist, existieren zudem mit § 43 Abs. 2 GmbHG oder § 93 Abs. 2 AktG dezidierte Haftungsnormen für Geschäftsleiter (die über Verweise auch die jeweiligen Aufsichtsorgane erfassen). Die Frage nach der Haftung impliziert aber bereits, dass „das Kind in den Brunnen gefallen ist," sprich sich eine Pflichtverletzung in einem Schaden niedergeschlagen hat. Zur Vermeidung derartiger Szenarien sollten die Organe der Geschäftsleitung bereits in ihren Zielvereinbarungen zur Implementierung und Beachtung von GRC-Systemen angehalten werden. Denn (neudeutsch) „*Incentives*" sind zumeist wesentlich motivierender als Haftungsrisiken. Auch sollte zwischen Konsequenzen und Sanktionen auf allen Ebenen unterschieden werden. So sollten die Konsequenzen aus erkanntem Fehlverhalten gezogen, aber ein „Pranger" für beteiligte Personen vermieden werden. Die richtige Balance in diesem Bereich ist wichtig, um die Vertrauenskultur im Unternehmen aufrechtzuerhalten.

10. Digitalisierung ja, aber *„bad processes make for bad digitization"*

Getreu des oben zitierten Mottos geht die (gute) Standardisierung jeglicher Digitalisierung vor – und die „Kunst des Weglassens" sollte zum Mantra der Verantwortlichen werden. Zudem muss die Überwachung der „elektronischen Helferlein" geregelt werden.[164]

11. Kommunikation und Schulung

Jedes System ist nur so gut wie ihr schwächstes Glied. Sind also die einzelnen Mitarbeiter sich des verfolgten Ansatzes und ihrer Rolle darin nicht bewusst, so ist nicht nur jegliches integrierte GRC-Konzept, sondern auch jede unternehmerische Strategie zum Scheitern verurteilt. Vor diesem Hintergrund ist die (wiederholte) Kommunikation der für die Umsetzung des GRC-Ansatzes erforderlichen Planungen, Maßnahmen und Ergebnisse (!) unerlässlich.[165] Regelmäßige Schulungen sollten deswegen im GRC-Regelkreis fest etabliert sein.

12. *„Kiss – Keep it simple, stupid"*

Sobald man sich nach mehreren Durchläufen des GRC-Zyklus einem „eingeschwungenen" integrierten System genähert hat, sollte man sich „in der Kunst des Weglassens"[166] üben, sprich: prüfen, welche Prozesse oder Regelungen zu vereinfachen sind.

13. *„Only what gets measured, gets managed"*[167]

Westhausen[168] versucht sich lobenswerter Weise mithilfe eines generischen Berechnungsmodells an einer Möglichkeit zur Quantifizierung des Mehrwerts eines CMS für Einzelunternehmen. Und zeigt damit einen wichtigen Punkt auf: Nur wenn das (integrierte) System einen Nutzen für das Unternehmen stiftet, wird es auf Dauer auch akzeptiert werden.[169] Für Unternehmen bedeutet das „GRC-relevante KPI-Systeme"[170] festzulegen, die sich möglichst auch in „harter Währung" ausdrücken, sprich auf die Ertragslage des Unternehmens, auswirken sollten.

V. Fazit

Die vorangegangene Untersuchung zeigt auf, dass trotz der empirisch unterlegten Erkenntnis, dass Unternehmen regelmäßig an Managementfehlern scheitern, sich gerade der deutsche Mittelstand bei der Einführung adäquater Governan-

160 S. dazu näher bei *Otremba* (Fn. 15), S. 167 f.; *Scherer*, CCZ 2012, 201, 203 f.; instruktiv zur Governance bereits *Malek*, „Die richtige Corporate Governance".

161 S. dazu nur *Dämon*, „Unfälle bei Managern – Plötzlich musste ich meine Rolle als CEO überdenken", in: WirtschaftsWoche (2017), abrufbar unter *https://www.wiwo.de/erfolg/management/unfaelle-von-managern-ploetzlich-musste-ich-meine-rolle-als-ceo-ueberdenken/20700032.html.* S.

162 S. dazu grundlegend *Vetter*, GmbHR 2011, 449; *Schilling*, „Gute Aufsicht scheitert am Menschen", FAZ v. 13.10.2014, 16, stellt gut die typischen Mängel in der Aufsichtsratsgestaltung dar.

163 S. näher bei *Schaupensteiner*, NZA-Beilage 2011, 8, 11.

164 S. nur *Romeike/Gleißner*, GRC aktuell 2021, 126, abrufbar unter: *https://futurevalue.de/wp-content/dokumente/FA_2019_StaRUG_-_Risikomanagement-Software_fuehrt_zu_Haftungsrisiken_2021.pdf.*

165 S. dazu näher erneut bei *Schaupensteiner*, NZA-Beilage 2011, 8, 11.

166 Entsprechend des zehnten Prinzips des Agilen Manifests (abrufbar hier: *https://digitaleneuordnung.de/blog/agiles-manifest/*), s. aber auch *Talib*, – „Skin in the Game", S. 15, zum Prinzip der „*via negativa*" bzw. „*systems learn by removing parts*".

167 Zitiert nach *Westhausen* ZRFC 2021, 199, 203.

168 In: ZRFC 2021, 199 ff.

169 Ähnlich auch *Otremba* (Fn. 15), S. 143.

170 Nach *Westhausen*, ZRFC 2021, 199, 203.

ce-Systeme ziert. Dabei legt bereits die aktuelle Rechtslage Geschäftsleitern – und damit in der Folge auch Beratern und Verwaltern in der Krise/Insolvenz des Unternehmens – die Pflicht auf, eine Unternehmensorganisation zu implementieren, die ihnen informierte unternehmerische Entscheidungen ermöglicht.

Aber auch unter betriebswirtschaftlichen Gesichtspunkten erfordert eine nachhaltige Transformation, Restrukturierung und Sanierung, die Prozesse und Organisation der Entscheidungsfindung im Unternehmen auf Effektivität und Effizienz zu überprüfen und ggf. nachzujustieren. Anstatt diese Systeme als Insellösungen im Unternehmen zu etablieren, sollte eine Integration der Systeme im Sinne eines (modifizierten) GRC-Modells („GRC²+“) angestrebt werden, um einer Silobildung im Unternehmen und damit einseitig beeinflussten unternehmerischen Entscheidungen entgegen zu wirken.

Gutes GRC ist dabei kein Selbstzweck, sondern lediglich ein Werkzeug, um die Sicherung oder Wiedererlangung einer nachhaltigen Wettbewerbsfähigkeit von (mittelständischen) Unternehmen zu unterstützen. Deswegen ist es stets entscheidungsorientiert auszurichten und muss einen messbaren Mehrwert für das Unternehmen liefern, ansonsten wird es sich nicht durchsetzen.

Der Aufbau bzw. die Re-Organisation bestehender Governance-Strukturen hin zu einem integrierten entscheidungsorientierten System ist gleichzeitig Grundlage und Schritt in der nachhaltigen Transformation des Unternehmens. Ohne den Nachweis ein solch integriertes System aufgestellt und betrieben zu haben, dürfte es Geschäftsleitern, Sanierern und Insolvenzverwaltern künftig schwerfallen, sich durch Berufung auf die *Business Judgement Rule* einer Haftung im Fall des Scheiterns des Unternehmens oder der (insolvenzbedingten) Sanierung zu entziehen.

Going Concern in der Unternehmenskrise – Gibt es eine „Erwartungslücke“ bei Abschlussprüfungen?

Eine Betrachtung aus dem Blickwinkel eines sanierungserfahrenen Wirtschaftsprüfers mit Praxisfällen

von Dipl.-Kfm./Steuerberater/Wirtschaftsprüfer Michael Hermanns, Düsseldorf*

Unternehmenskrisen entstehen typischerweise aus Strategiekrisen, also strategischen Fehlentscheidungen der Unternehmensleitung, die zunächst unerkannt bleiben. Manifestiert sich hieraus eine Ertrags- und im Folgenden sogar eine Liquiditätskrise ist die Unternehmensfortführung im Zweifel gefährdet. Werden im Zeitablauf keine unternehmerischen Gegenmaßnahmen eingeleitet und die Verlustquellen beseitigt, dann droht „unbehandelt“ die Insolvenz.

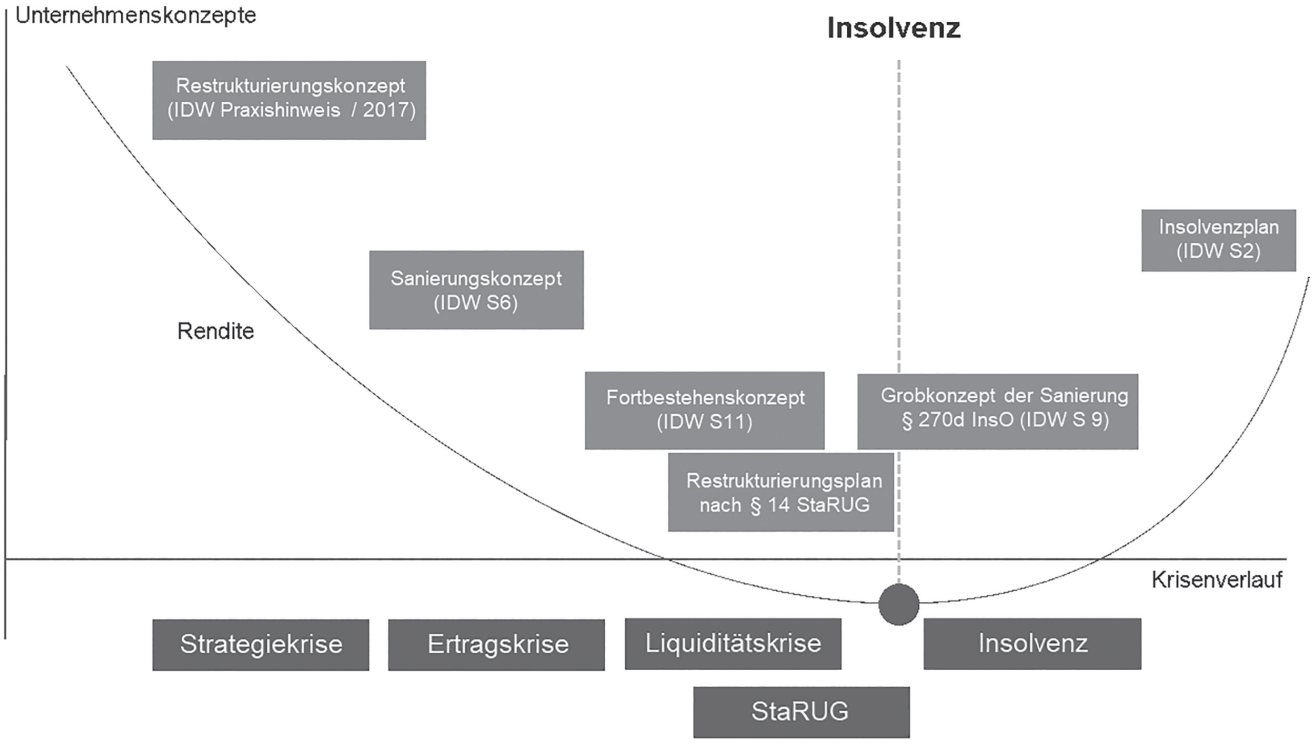

Abb.: Krisenstadien und Werkzeugbaukasten des IDW

* Der Verfasser ist Gründungspartner der BUTH&HERMANNS PartmbB WPG StBG, seit 2009 Mitglied und seit 2024 Vorsitzer im Fachausschuss Sanierung und Insolvenz (FAS) beim IDW e.V.