Herausragende Masterarbeiten

Autor*in

Lars Holger Tilgner

Studiengang

Wirtschaftsrecht für die Unternehmenspraxis, LL.M.

Masterarbeitstitel

**Compliance Managementsysteme: Pflicht oder Kür für den Mittelstand?
Ein Überblick aus Handels-, Steuer- und Insolvenzrecht**

RPTU
Distance and Independent Studies Center
DISC

Gliederungsverzeichnis

Erklärung über selbständige Bearbeitung

1. Einleitung

1.1 Einführung in die Thematik „Compliance“ und „Mittelstand“

„Compliance“ wurde zunächst als Regeleinhaltung interner Vorgaben in Unternehmen angesehen. Übersetzt man „Compliance“ wörtlich, so wird dies als „Einhaltung“ oder „Befolgung“ übersetzt.[1] Der Begriff wird heute als die ordnungsgemäße, systematische Einhaltung von Gesetzen, Vorgaben und freiwilligen Anforderungen verstanden[2]. Die entsprechenden Regularien sollen das Unternehmen vor finanziellen und rechtlichen Risiken, aber auch den allgemeinen Wirtschaftsverkehr vor finanziellen und tatsächlichen Schäden schützen. Allerdings sollen auch die Unternehmen unter Anwendung ihres systematischen Rahmenwerks vor straf- und ordnungsrechtlichen sowie anderseits zivilrechtlichen Haftungsszenarien geschützt werden. Schädigungen anderer und die des Unternehmens sollen im besten Falle verhindert werden.

Jedoch stellt sich zunächst die Frage: Wer ist Adressat? Wer ist überhaupt „der Mittelstand“?

Gesetzliche Regelungen ab wann ein Unternehmen zum Mittelstand gehört, gibt es nicht. Interessanterweise fühlen sich sowohl Unternehmen im MDAX als auch der „kleine“ Handwerker mit 5 Mitarbeitern dem Mittelstand zugehörig. Versucht man anhand von gesetzlichen Regelungen festzustellen, den Mittelstand zu objektivieren, stellt man sehr schnell fest, dass es dazu keine gesetzlichen Definitionen gibt.

Unabhängig von der Größe des Unternehmens gibt es einzuhaltende Vorschriften und Risiken, fehlerhafte Bilanzierung, Angriffe auf die IT-Infrastruktur, eine extreme Entwicklung bei der Beschaffung von Warenmaterial oder Fertigungsmaterial belasten die Firmen. Diesen Risiken sollten Unternehmen durch entsprechende Systeme entgegenwirken, so dass es für sie keine überraschenden Ereignisse gibt. Haben sie keine internen Kontroll- oder Risikomanagementsysteme wird nicht rechtzeitig Alarm geschlagen. Hätten diese Unternehmen eine Verpflichtung, Compliance-Managementsysteme und Risikomanagementsysteme einzurichten, dann würde auch die Überwachung nicht fehlen. Besonders fallen die großen börsennotierten Unternehmen, wie Wirecard, auf. Bei diesem Unternehmen wurden 1,9 Milliarden Euro als Treuhandkonten in der Bilanz ausgewiesen, die überhaupt nicht vorhanden waren, damit wurden viele Anleger geschädigt und stehen vor einem Totalverlust. Die Untersuchungen haben ergebenen, dass keine internen Kontrollsysteme

[1] Nestler/Modi, Leitfaden IT-Compliance, S. 19
[2] ebenda

vorhanden waren, die für einen Dax-Konzern angemessen gewesen wären. Hätte das Unternehmen, wie es für börsennotierte Unternehmen vorgeschrieben ist, ein internes Kontrollsystem gehabt und wäre ein funktionierendes angemessenes CMS und RMS installiert gewesen, wäre der Aufsichtsrat auch rechtzeitig informiert worden. Liest man die Wirtschaftspresse aufmerksam, so geraten immer wieder Firmen in den Fokus. Der Immobilienriese Adler, Leasingunternehmen wie Grenke, u. v. a. werden immer wieder mit Bilanzfälschungen oder der Nichteinhaltung von Gesetzen konfrontiert. Zuletzt musste der verantwortliche Vorstand für Compliance der Grenke AG gehen.

Der Gesetzgeber hat aufgrund dieser Bilanzskandale, wie Wirecard bei Gesetzesänderungen vorgegeben, dass entsprechende Überwachungsvorkehrungen getroffen werden müssen und bei Verstoß erhebliche Strafen nach sich ziehen. Durch die Verabschiedung des Gesetzes zur Stärkung der Finanzmarktintegrität (FISG) ist jedes börsennotierte Unternehmen verpflichtet, „angemessene und wirksame“ interne Kontrollsysteme (IKS) und Risikomanagementsysteme (RMS) einzurichten.

Aber was hat das mit dem Mittelstand zu tun? Das sind doch alles große börsennotierte Unternehmen. Im Mittelstand kommen doch Bilanzskandale gar nicht vor bzw. wer wird denn davon überhaupt geschädigt?

Der Gesetzgeber hat zahlreiche neue Gesetze und Regularien verabschiedet, die aufgrund dieser Missstände entstanden sind. Diese Regelungen gelten nicht nur für die Großunternehmen, sondern für alle Unternehmen. Die Corona-Pandemie brachte ebenfalls neue Gesetze hervor, die auch kleine und mittlere Unternehmen faktisch zwingen, entsprechende Regelungen im Unternehmen zu etablieren. Genannt sei an dieser Stelle das Gesetz zur Fortentwicklung des Sanierungs- und Insolvenzrechts (SanInsFoG), der Kern des Gesetzes, das Stabilisierungs- und Restrukturierungsgesetz (StaRUG). In § 1 StaRUG heißt es, „Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können.“ Genau durch solche Regelungen wird deutlich, dass der Gesetzgeber von **allen** Unternehmen verlangt, dass entsprechende Systeme im Unternehmen zur Überwachung und Steuerung eingeführt werden sollen, auch wenn es sich nicht um ein großes Unternehmen handelt. Die Regelungen in § 1 StaRUG gelten für alle Unternehmen, auch wenn sie nicht in der Krise sind.

Aber auch Rechtsgebiete wie Wettbewerbs- und Kartellrecht, Produkthaftungsgesetze, straf- und bußgeldrechtliche Regelungen für Unternehmen, Kapitalmarktrecht wie MARISK, Geldwäschegesetze,

Verrechnungspreisregelungen, Umwelt-, Sozial- und Arbeitsrechte, etc. diese Auflistung könnte man beliebig erweitern, führen zu Risiken, die der einzelne Unternehmer im Mittelstand kaum noch überblickt. Der Mittelstand hat meist keine eigene Rechts-, Steuer- oder gar Compliance-Abteilung, die auf die Einhaltung der Gesetze achten.

Da der Gesetzgeber zwar Fälle wie Wirecard vor Augen hat und daher Vorschriften für Unternehmen erlässt, hat dies jedoch auch Auswirkungen auf den Mittelstand.

Zwar betreffen die bisher aufgeführten Beispiele große börsennotierte Unternehmen, die sowieso verpflichtet sind, Compliance Managementsysteme zu unterhalten, jedoch ziehen immer wieder Formulierungen in die verschiedenen Gesetze ein, die alle Unternehmen verpflichten, entsprechende Systeme zu etablieren, die die Mitarbeiter zur Einhaltung von Regelungen verpflichten und gleichzeitig die Geschäftsführung verpflichtet wird, auf die Einhaltung zu achten.

Die allgemeinen Geschäftsrisiken von kleinen und mittelständischen Unternehmen haben ebenfalls mit Regelungen zur Einhaltung von Gesetzen und Vorschriften für eben diese zu tun. Das bekannteste Recht dürfte wohl dabei die DSG-VO (Datenschutzgrundverordnung) sein. Erstmals in der Diskussion über die Anpassung der DSG-VO und deren Verschärfungen machte auch kleinen Unternehmen bewusst, dass auch sie organisatorische Maßnahmen ergreifen müssen. Der „Musterschüler Deutschland“ hat bei dem Gesetzgebungsverfahren entschieden, dass bereits Unternehmen mit einer Mitarbeiterzahl von mehr als 20 Mitarbeitern, die ständig automatisiert Daten verarbeiten, einen Datenschutzbeauftragten bestimmen müssen.

„Nur wo Risiken bestehen, müssen Gesetze, Vorgaben und freiwillige Anforderungen eine Struktur schaffen, um die Folgen dieser Risiken zu vermeiden oder einzudämmen“[3]

Compliance als Oberbegriff umfasst daher nicht nur förmliche Rahmenbedingungen, die den unternehmerischen Tätigkeiten unterliegen, sondern auch die allgemeinen Wertevorstellungen bspw. Arbeitssicherheit, Umweltschutz oder Mitarbeiter- und Kundenumgang.

1.2 Zielsetzung

Bisher wurde die Auffassung vertreten, dass es eine gesetzliche Pflicht zur Einführung eines Compliance-Management-Systems in Deutschland explizit nur für bestimmte Branchen, so bspw. für die Finanz- und Versicherungsbranche[4]

[3] Fissenewert (2018), S. 1 f.
[4] Schwab, Dissertation, S. 2

gibt. Es wird spätestens mit der Entscheidung des OLG Nürnberg[5] deutlich, dass die Diskussion über die faktische Verpflichtung zur Einrichtung von CMS, RMS und IKS für kleine und mittelständische Unternehmen weitergeführt werden muss. Bemerkenswert an der Entscheidung ist, dass selbst bei einer mittelständischen Gesellschaft - hier waren in der Verwaltung neben dem Geschäftsführer lediglich 13 Mitarbeiter beschäftigt - ein Früherkennungssystem für bestandsgefährdende Entwicklungen (heute: § 1 Abs. 1 StaRUG) bzw. ein Compliance Management System einzurichten und zu dokumentieren ist.[6] Es ist daher fraglich, ob die Auffassung, dass eine ausdrückliche, wenn auch nicht allgemeine Verpflichtung der Unternehmensleitung, Compliance-Maßnahmen zu ergreifen im deutschen Recht wirklich nicht vorgesehen ist[7]. Für den Vorstand einer Aktiengesellschaft ergibt sich die Verpflichtung aus den §§ 76 Abs. 1 und 93 Abs. 1 AktG. Bekanntermaßen wurde sie vom Deutschen Corporate Governance Kodex aufgenommen – der Zusammenhang mit der Legalitätspflicht wird hier noch einmal deutlich. Als ebenfalls bekannt dürfte die Entscheidung des LG München I gelten, welches bereits 2013[8] die Pflicht zur Einrichtung eines Compliance-Management-Systems dem Vorstand zugewiesen und spiegelbildlich dem verantwortlichen Manager vorgeworfen hatte, kein ausreichendes und funktionsfähiges Compliance–Management–System eingerichtet zu haben. Dies könne automatisch eine Pflichtverletzung des Vorstands bedeuten[9]. Das Gericht stellte fest, die Sicherstellung des tatsächlichen Funktionierens eines Compliance-Systems sei „originäre, nicht delegierbare Aufgabe eines jeden Vorstands“[10]. Geläufig ist weiterhin, dass bei (irgend-)einer Verbandsgeldbuße Compliance-Maßnahmen bußgeldmindernd berücksichtigt werden können[11]. Diskutiert wurde in der Vergangenheit, ob die für die AG geltenden Grundsätze unmittelbar auf die GmbH übertragen werden können. So wurde die Meinung vertreten, der Maßstab und die Anforderungen an ein Compliance-Management-System seien grundsätzlich bei (kleinen) GmbHs weniger streng; es müsse durch den Geschäftsführer nicht einmal zwingend eine Organisationsstruktur vorgehalten werden. Etwas anderes galt lediglich, wenn die entsprechende GmbH über ein gewisses Gefahrpotential verfügt,[12]. Hingegen

[5] OLG Nürnberg, Endurteil vom 30.3.2022 - 12 U 1520/19
[6] Dachner, ZWH 2022, S.161
[7] Schieffer in: Minkoff/Sahan/Wittig, Konzernstrafrecht, 4. Teil, § 28 Rn. 1 mit dem Hinweis, dass sich aus ausländischen Normen eine derartige Verpflichtung auch für deutsche Unternehmen ergeben, kann
[8] LG München I, Urt. v. 10.12.2013 - 5 HK O 1387/10 - NZG 2014, 345
[9] Dohrn, Newsdienst Compliance 2014, 22101, beck-online
[10] Flick in: GWR 2014, 151
[11] vgl. BGH, Urt. v. 09.05.2017 - 1 StR 265/16 - NZG 2018, 36
[12] Noack/Servatius/Haas/Beurskens, 23. Aufl. 2022, GmbHG § 43 Rn. 11

wies exemplarisch Acker[13] in seiner Urteilskommentierung der genannten Entscheidung des LG München I bereits darauf hin, dass eine Verpflichtung zur Einrichtung eines Compliance-Systems für die GmbH regelmäßig aus § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG abzuleiten sei. In dem vorliegenden Urteil hat das OLG Nürnberg diese Compliancepflicht auch für den Geschäftsführer einer GmbH nochmals zugespitzt und ausgeführt, dass „aus der Legalitätspflicht [...] die Verpflichtung des Geschäftsführers zur Einrichtung eines Compliance Management Systems, also zu organisatorischen Vorkehrungen, die die Begehung von Rechtsverstößen durch die Gesellschaft oder deren Mitarbeiter verhindern“ folge[14], obwohl bereits der BGH im Urteil vom 27.04.1994[15] die Auffassung vertreten hat, dass § 130 OWIG keine Schutzzwecknorm ist, die eine Haftung nach § 823 II i. V. m. § 130 OWIG begründet.

Das OLG Nürnberg[16] sieht es in seiner Entscheidung anders, es erkennt in § 130 OWIG eine Schutzzwecknorm und erkennt daher Schadenersatzansprüche nach § 823 II BGB i. V. m. § 130 OWIG an. Hierdurch wird die rechtsform- und branchenunabhängige Pflicht zur Einführung eines Compliance-Management-Systems[17] faktisch bereits durch § 130 OWIG verankert.[18] Es bleibt daher abzuwarten, ob der BGH, der bis dahin durchaus die Auffassung vertreten hat, dass es zu weit ginge, die bußgeldbewehrte Pflicht, Aufsichtsmaßnahmen zur Verhinderung von Straftaten und Ordnungswidrigkeiten zu treffen (§§ 130, 9 I Nr. 1 OWiG), als Schutzgesetz zugunsten der Gläubiger iSv § 823 II BGB zu qualifizieren.[19]

Der bis dahin geführten akademischen Diskussion über die rechtliche Verankerung der Compliance Management-Systeme und der Ausstrahlungswirkung des § 91 Abs. 2 AktG bzw. die Beachtung der allgemeinen Sorgfaltspflichten von Unternehmensleitern in § 93 AktG und § 43 GmbHG hat das OLG Nürnberg mit dieser Entscheidung eine Absage erteilt und die Auffassung vertreten, dass bereits § 43 Abs. 1 GmbHG i. V. m. § 130 OWIG die Unternehmensleiter verpflichtet, ihre Überwachungsaufgaben ernst zu nehmen und systematisch wahrzunehmen. Die Diskussion von Compliance für alle Unternehmen hat damit neue Bedeutung bekommen und die sog. Standards

[13] Acker in IBR 2014, 309, beck-online
[14] OLG Nürnberg 12. Zivilsenat, Urteil vom 30.03.2022 - 12 U 1520/19, Rn. 102
[15] BGH | VIII ZR 223/93 27.04.1994 Urteil
[16] OLG Nürnberg vom 30.03.2022 (12 U 1520/19 - NZG 2022, 1058 ff.)
[17] Schwab, Dissertation, S. 2
[18] Uwe H. Schneider, ZIP 2003, 645; dazu Hauschka, ZIP 2004, 877 in Hauschka/Moosmayer/Lösler, Corporate Compliance, 1. Abschnitt. Einführung und rechtliche Rahmenbedingungen 1. Kapitel. Einführung § 1. Einführung Rn. 30, beck-online
[19] Noack/Servatius/Haas/Beurskens, 23. Aufl. 2022, GmbHG § 43 Rn. 134

werden gestärkt, so der Deutsche Corporate Governance Kodex[20] , der IDW PS 980 n. F. oder die ISO 1960012.

Jedoch hat das OLG Nürnberg nicht nur Compliance-Management-Systeme, sondern auch explizit die erforderlichen Überwachungs- und Kontrollmaßnahmen gefordert, da das Vier-Augen-Prinzip in den kritischen Arbeitsprozessen des Unternehmens nicht beachtet wurden. Damit erfährt auch die Einführung von internen Kontrollsystemen eine besondere Bedeutung bei kleinen und mittelständischen Unternehmen und nicht nur bei den mittelgroßen und großen Kapitalgesellschaften, die bereits durch die allgemeinen Sorgfaltspflichten rechtlich dazu verpflichtet sind. Das Gericht rügt auf der Grundlage des § 130 OWIG als einen wesentlichen Verstoß gegen die Pflichten des Geschäftsführers das Fehlen des VIER-AUGEN-PRINZIP und fordert dieses branchenübergreifend als erforderlich ein[21].

Doch die meisten Mittelständlern sind sich dessen gar nicht bewusst. Sie erkennen schlicht und ergreifend gar nicht, welche Compliance-Risiken sie Tag täglich eingehen. Meist sind sie bereits mit dem Alltagsgeschäft und der damit verbundenen Problematiken, wie Personalbeschaffung, Materialbeschaffung, etc.., so beschäftigt, dass ihnen kaum noch Zeit bleibt, sich über Risiken, die aus ihrer Sicht nur theoretisch bestehen, Gedanken zu machen. Sie sind schließlich ihr eigener Herr, meist selbst der Gesellschafter und Geschäftsführer. Wer soll denn da den Geschäftsführer in die Haftung nehmen? Solange kein Schaden entsteht, besteht das Risiko doch nur theoretisch. Doch gerade diese Denkweise ist gefährlich. Es soll aufgezeigt werden, wann für den Geschäftsführer das Risiko entsteht und wann die unterlassene systematische Überwachung zu einem nicht mehr zu behebenden Problem wird.

Die Sicherstellung der Einhaltung der gesetzlichen Vorschriften gehört zu den Organisations- und Sorgfaltspflichten der gesetzlichen Vertreter[22], egal ob man dies mit § 91 AktG begründet und der Ausstrahlungswirkung auf § 43 Abs. 1 GmbHG oder mit der originären und bußgeldverpflichteten Verpflichtung nach § 130 OWIG. Nach der bisherigen Rechtsprechung besteht die Legalitätspflicht darin, dafür Sorge zu tragen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass Gesetzesverstöße verhindert werden.[23] Der gesetzliche Vertreter hat die Pflicht, das Unternehmen so zu organisieren, dass bei

[20] Der Deutsche Corporate Governance Kodex ist ein im Jahr 2002 entstandenes Regelwerk, das mittels Empfehlungen und Anregungen auf eine gute Corporate Governance hinwirkt. Weitere Ausführungen zum Entstehungshintergrund des Deutschen Corporate Governance Kodex, v. Werder, in: Kremer/Bachmann/Lutter/v. Werder, DCGK-Komm, S. 17 ff. Im Folgenden DCGK genannt.

[21] OLG Nürnberg 12. Zivilsenat, Urteil vom 30.03.2022 - 12 U 1520/19, (Rn. 96, 103 ff., 108, 137).

[22] Vgl. IDW Praxishinweis 1-2022

[23] ebenda

entsprechender Gefährdungslage das Risiko kontrolliert und der Schaden verhindert werden kann. Die Organisationspflicht ist so zu organisieren, dass eine entsprechende Compliance-Organisation eingerichtet wird. Die Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance Management Systems gehört zur Gesamtverantwortung der gesetzlichen Vertreter.[24]

1.3 Aufbau der Arbeit

Die Arbeit setzt sich kritisch mit den gesetzlichen Verpflichtungen zur Einführung von CMS, RMS und IKS auseinander und zeigt auf, welche Auswirkungen die verschiedenen gesetzlichen Regelungen, wie dem § 4 GWG, § 1 StaRUG oder durch die Entscheidung des OLG Nürnberg auf Gesellschafter-Geschäftsführer haben. Es soll weiter dem Mittelstand aufgezeigt werden, welche Maßnahmen ergriffen werden müssen und wie ein wirksames und angemessenes CMS ausgestaltet werden kann und wie es ganz pragmatisch am Beispiel des GWG umgesetzt werden kann. Dazu hat der sich Verfasser an den Standards des IDW orientiert und hat diese auf Anwendbarkeit auf den Mittelstand dargestellt.
Es soll aufgezeigt werden, warum hohe Haftungsrisiken entstehen, wenn nicht auf die Einhaltung der Regelungen und Gesetze geachtet wird.
Es wird anhand von praktischen und tatsächlichen Fällen gezeigt, welche organisatorischen Maßnahmen der Unternehmensleiter auch in kleineren Unternehmen einführen kann.
Auf ein angemessenes und wirksames Compliance Management System nach IDW PS 980 kommt aus Sicht des Unternehmens nicht nur präventive Wirkung zu, sondern ein Compliance Management System kann im Falle eines eingetretenen Compliance-Regelverstoßes auch eine bußgeldmindernde Wirkung entfalten.[25]

Da in der unternehmerischen Realität auch das beste Compliance-Management-System nicht in der Lage ist, Rechtsverstöße durch Mitarbeiter und Beauftragte des Unternehmens zu 100 % zu verhindern, sind Unternehmen neben der Prävention auch zur korrespondierenden Repression verpflichtet:[26]
Nachdem sich das LG München I in der vielbeachteten „Siemens/Neubürger"-Entscheidung mit der Organhaftung und der konkreten Ausgestaltung eines

[24] Vgl. sogenanntes „Neubürger-Urteil" (LG München I, Urteil vom 10.12.2013 – 5HK O 1387/10).
[25] Vgl. BGH, 09.05.2017 – 1 StR 265/16.
[26] Reichert in FS Hoffmann-Becking, 2013, 943 (947); Reichert/Ott NZG 2014, 241 f.; Seibt/Cziupka, DB 2014, 1598 (1599)

Compliance-Systems befasst hat, hat sich der 1. Strafsenat des BGH[27] im Rahmen des Ordnungswidrigkeitenrechts zur Berücksichtigung von Compliance-Management-Systemen bei der Bemessung von Bußgeldern gegen Unternehmen nach § 30 OWiG in einem obiter dictum geäußert.[28] Der Senat wies darauf hin, dass für die Bemessung der Geldbuße gegen das Unternehmen von Bedeutung sei, inwieweit es seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management-System installiert hat.[29]

Die Arbeit soll ein Leitfaden speziell für kleine und mittelständische Unternehmen sein, *daher wird auf den Aspekt der Bußgeld Reduzierung nicht näher eingegangen*. Es wird zu den Verhältnissen und die in der Praxis immer wieder auftretenden Problematiken hingewiesen und wie damit umgegangen werden kann. Zur besseren Verständlichkeit wird zu Beginn der Arbeit dargestellt, in welchem Verhältnis Compliance-Management-Systeme (CMS, IDW PS 980), Risiko-Management-Systeme (RMS, IDW PS 981), und Interne-Kontroll-Systeme (IKS, IDW PS 983) sowie Tax-Compliance-Management-Systeme (TCMS Stellungnahme 1/2016 des IDWs) zueinanderstehen und wie diese ineinandergreifen.

Des Weiteren wird anhand eines Beispiels eines Pfandleihhauses aufgezeigt, wie auch schon bei kleinen Unternehmen eine rechtliche Komplexität entstehen kann und wie dieser entgegengewirkt werden kann. Grundsätzlich ist bei jedweder unternehmerischen Betätigung die allgemeinen von den spezifischen rechtlichen Betreiberrisiken zu unterscheiden.

So wird bspw. der im GwG (Geldwäsche-Gesetz) verwendete Begriff „Risikomanagement“ unter Berücksichtigung von rechtlichen und betriebswirtschaftlichen Grundsätzen als ein auf die Einhaltung der geldwäscherechtlichen Vorschriften gerichteter Teilbereich eines Compliance Management Systems angesehen[30]. Daher ist es wichtig, eine klare Abgrenzung und Definition der vom Gesetzgeber verwendeten Begriffe und der in der Betriebswirtschaft und dem Institut der Wirtschaftsprüfer verwendeten Begriffe zu definieren.

[27] Vgl. BGH vom 9.5.2017 – 1 StR 265/16

[28] Vgl. die (zumeist kritischen) Besprechungen von Bachmann ZIP 2014, 579 ff.; Bürkle CCZ 2015, 52 ff.; Fleischer NZG 2014, 321 ff.; Kuhlen NZWiSt 2015, 121 (124 ff.); Meyer DB 2014, 1063 ff.; Oppenheim DStR 2014, 1063 ff.; Paefgen WM 2016, 433 ff.; Seibt/Czuipka DB 2014, 1598 ff.; Simon/Merkelbach AG 2014, 328 ff.

[29] Jenne/Martens: Compliance-Management-Systeme sind bei der Bußgeldbemessung nach § 30 OWiG zu berücksichtigen – Anmerkung zu BGH, Urteil vom 9.5.2017 – 1 StR 265/16

[30] IDW Praxishinweis 1-2022

1.4 Methodik

Es wird anhand der Standards des IDWs zu CMS, RMS und IKS die Anforderungen an diese Systeme dargestellt und mit der täglichen Arbeit von mittelständischen Unternehmen verglichen. Zudem sollen die tatsächlichen, rechtlichen und wirtschaftlichen Risiken von Gesellschafter-Geschäftsführern dargestellt werden. Die letzten verabschiedeten Gesetze zeigen auf, welche Bedeutung die systematische Organisation von Unternehmen bekommen hat. Zur besseren Lesbarkeit und dem besseren Verständnis wird anhand von praktischen Fällen des Verfassers anhand eines Pfandleihhauses aufgezeigt, wie auch bei kleinen und mittelständischen Unternehmen bereits komplexe Situationen und Haftungsgefahren entstehen. Aufgrund eines normenübergreifenden Regulativs von Pfandleihhäusern stellt dies den Unternehmensleiter und seine Berater vor einem sehr komplexe Herausforderung. Gerade dies soll aufzeigen, wie Vorschriften, die jeden Unternehmer betreffen und Branchenspezifische Regularien in einem Compliance-Management-System einzuarbeiten gilt. Einfache tägliche und in der Praxis häufig auftretende Problematiken werden dargestellt und anhand diesen meist unproblematischen Situationen aufgezeigt, wie schnell persönliche Haftungsgefahren für den Geschäftsführer entstehen. Dabei wird insbesondere auf handelsrechtliche, steuerrechtliche und insolvenzrechtliche Problematiken eingegangen.

2. Der Dreiklang aus Governance, Risikomanagement und Compliance

Der Dreiklang Governance, Risk und Compliance gilt es im Mittelstand zu implementieren. Effektive und haftungsminimierende Unternehmenssteuerung muss diesen Dreiklang beherrschen. Im Folgenden werden aus Sicht eines Pfandleihhauses insbesondere die Bereiche Compliance-Management, das Risikomanagement und interne Kontrollen dargestellt. Weitere zentrale Handlungsebenen sind die Umsetzung und die Haftungsrisiken, die entstehen, wenn keine angemessenen Systeme eingeführt werden.

Ein Pfandleihhauses kann grundsätzlich jeder unbescholtene Bürger betreiben.

Die Pfandleihe ist grundsätzlich ein Kreditgeschäft im Sinne von § 1 Abs. 1 Satz 2 Nr. 2 Alt. 1 des Gesetzes über das Kreditwesen (Kreditwesengesetz – KWG). Ein Pfandleihinstitut ist ein Kreditinstitut im Sinne von § 1 Abs. 1 Satz 1 KWG und

sein Geschäft würde damit unter Erlaubnisvorbehalt nach § 32 Abs. 1 KWG stehen, gäbe es nicht den § 2 Abs. 1 Nr. 5 KWG.[31]

Nach § 2 Abs. 1 Nr. 5 KWG gelten jedoch Unternehmen des Pfandleihgewerbes, soweit sie dieses durch Gewährung von Darlehen gegen Faustpfand betreiben, nicht als Kreditinstitute und benötigen somit keine Erlaubnis nach § 32 Abs. 1 Satz 1 KWG.[32]

Die Gründung einer GmbH stellt ebenfalls keinen erlaubnispflichtigen Vorgang dar. Der im GmbHG geregelte Gründungsvorgang beginnt mit dem notariellen beurkundeten Abschluss des Gesellschaftsvertrages gem. § 2 GmbHG. Da jedoch die GmbH allein nicht handlungsfähig ist, sondern nur durch ihr Organ der Geschäftsführung gem. § 35 GmbHG, ist es erforderlich, dass der Geschäftsführer ein unbescholtener Bürger ist, der versichern muss, keine Vermögens- und Insolvenzstraftaten begangen zu haben. Der formale Akt beim Notar führt zur Errichtung der Gesellschaft. Die Gesellschaft entsteht jedoch erst mit Eintragung. Der Geschäftsführer wird durch Gesellschafterbeschluss gem. §§ 6 III 2, 46 Nr. 5 GmbHG bestellt. Der Geschäftsführer hat die Einlage gem. § 7 II, III GmbHG entgegenzunehmen und meldet die Gesellschaft zum Handelsregister an (§§7 I, 8, 78 GmbHG, § 13 GmbHG i. V. m. §§ 6 I, 12 HGB). Ist, wie es in der Praxis häufig vorkommt, der Gesellschafter und der erste Geschäftsführer personengleich, so richtet der Gesellschafter-Geschäftsführer nach dem Termin beim Notar ein Bankkonto auf den Namen der GmbH in Gründung ein und zahlt das erforderliche Stammkapital gem. § 5 I GmbHG in Höhe von 25.000 Euro ein. Der Geschäftsführer muss bei der Anmeldung der GmbH versichern, dass er nicht wegen der in § 6 II GmbHG aufgeführten Straftaten in den letzten fünf Jahren verurteilt worden ist.

Doch allein mit der Gründung der Gesellschaft ist es nicht getan. Der Betreiber eines Pfandleihhauses muss die Allgemeinen Gesetze für gewerbliche Unternehmen, die jeder Gewerbebetreibende und auch jede Kapitalgesellschaft zu beachten haben, einhalten. Als GmbH unterliegt unser Pfandleihhaus dem GmbHG und dem HGB, steuerrechtlichen Vorschriften (AO, KStG, GewStG, UStG, etc…), der GewO sowie allgemeinen Schutzgesetzen, wie das Ladenschlussgesetz (LadSchlG), Unfallverhütungsvorschriften, Arbeitsschutzrechten der Arbeitnehmer, sofern er beabsichtigt Angestellte zu beschäftigen, dem Geldwäschegesetz (GWG) und Datenschutzrechten (DSG-VO). Neben den allgemeinen Rechtsvorschriften hat er jedoch auch spezifische

---

31 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_101209_ausnahme_pfandleihgewerbe.html

32 ebenda

Gesetze wie die Pfandleiherverordnung (PfandlV) und, wenn die Pfandgüter verwertet werden, so hat dies durch eine öffentliche Versteigerung unter Beachtung der dafür vorgesehen Verordnungen und Gesetze zu erfolgen.
Der Pfandleiher darf das Pfand nur annehmen, wenn er mit dem Verpfänder vereinbart, sich wegen der Rückzahlung der Forderung, Zinsen, Kosten und sonstigen Vergütungen nur aus dem Faustpfand zu befriedigen (vgl. § 5 Abs. 1 Satz 1 Nr. 1 PfandlV); die Einschränkung folgt aus dem Schutzgedanken der Norm. Der Schuldner soll nur das riskieren, was er zum Pfand gibt und damit offenbar in der Not entbehren kann. Er soll nicht, wenn sich seine finanzielle Situation nicht zeitig bessert, auch noch mit gerichtlichen Mahnbescheiden bedrückt werden. Der Darlehensnehmer hat die Option, nicht die Pflicht, das Pfand nach Ablauf des Darlehensvertrages wieder auszulösen. Die Pfandleiherverordnung hält eine entsprechende Verpflichtung ausdrücklich fest (§ 5 Abs. 1 Satz 1 Nr. 1 PfandlV); entsprechend sind auch die Verträge der durch die Gewerbeaufsichtsämter der Länder zugelassenen Pfandleihinstitute zu gestalten.
Nun möchte der Betreiber eines Pfandleihhauses mit dem Ankauf von Edelmetallen und der Gewährung von Darlehen Gewinne erwirtschaften, so dass er das Personal schulen muss, Wertgegenstände zu bewerten und einen möglichen Auszahlungsbetrag zu ermitteln. Da der Schuldner eine realistische Chance haben soll, sein verpfändetes Gut wieder zu erhalten, ist gem. § 5 I PfandlV eine Mindestvertragslaufzeit von 3 Monaten einzuhalten. Endet die Vertragslaufzeit, darf der Pfandleiher das Pfand erst einen Monat nach Ende der Vertragslaufzeit verwerten.
Daher muss bei dem Beleihungswert des Pfands bereits berücksichtigt werden, dass mit dem möglichen Erlös in vier Monaten Kosten, Gebühren und Zinsen sowie das ausgereichte Darlehen zurückgezahlt werden können. Das Personal muss so geschult sein, dass durch die Vergabe von Pfandkrediten auf jeden Fall Gewinn erwirtschaftet wird und das geltende Recht eingehalten wird. Zudem muss erkannt werden, ob der Einlieferer des Pfandguts auch wirklich der rechtliche und wirtschaftliche Eigentümer ist. Das Personal ist daher auch dahingehend zu schulen, dass es erkennt, ob sie möglicherweise Diebesgut, Fälschungen oder Güter, die der Terrorismusfinanzierung dienen sollen, vorliegen.
Der Betreiber des Pfandleihhauses muss also Ziele formulieren, die alle Mitarbeiter des Unternehmens einzuhalten haben.
Der Geschäftsführer hat nach § 43 GmbHG die Geschäfte mit der Sorgfalt eines ordentlichen Geschäftsmannes zu führen. Andernfalls haftet er nach § 43 II

GmbHG dafür der Gesellschaft obligatorisch und solidarisch. Nach § 6 HGB ist das Pfandleihhaus Kaufmann i. S. d. § 1 HGB und daher verpflichtet, nach § 238ff. HGB Bücher zu führen und nach § 242 ff. HGB Bilanzen aufzustellen. Je nach Größenklassen nach §§ 267a, 267 HGB sind ggf. ergänzend Anhang und Lagebericht aufzustellen. Der Jahresabschluss ist nach § 264 I HGB in der dafür je nach Größenklasse vorgesehen Frist aufzustellen. Bei kleinen Kapitalgesellschaften spätestens innerhalb von 6 Monaten nach Abschluss des Geschäftsjahres. Befindet sich die Kapitalgesellschaft in der Krise, sind andere Maßstäbe anzuwenden. Spätestens mit dem Urteil des BGH vom 26.01.2017[33] wird für den Geschäftsleiter eines haftungsbegrenzen Unternehmens deutlich, dass die Frist nicht vorbehaltlos ausgeschöpft werden kann, sondern ggf. innerhalb von 6 Wochen der Jahresabschluss aufzustellen ist.

Doch wo kein Kläger da kein Richter, wer soll denn die Interessen der Gesellschaft geltend machen, wenn doch der Gesellschafter mit dem Geschäftsführer identisch ist?

Im Urteil des OLG Nürnbergs[34] wurde der Geschäftsführer aufgrund der fehlenden Überwachung und der Verletzung des Vier-Augen-Prinzips wegen der Verletzung seiner Sorgfaltspflicht zu Schadenersatz verurteilt. Kläger waren die Gesellschafter. In dem gewählten Beispiel, wird jedoch der Gesellschafter kaum sich selbst verklagen. Doch was viele Ein-Mann-GmbH-Gesellschafter vergessen, dass sie auch gegenüber den Gläubigern ihrer Gesellschaft eine Treuepflicht haben. Meist treten im Insolvenzfalle dann die Probleme bzw. die Mängel ans Tageslicht. Der Staat in der Gestalt des Finanzamtes fordert gem. § 149 Abs. 3 AO die Abgabe von Steuererklärungen. Die Steuererklärungen der GmbH sind, wenn sich die GmbH steuerlich vertreten lässt, bis zum 31.08. des übernächsten Jahres abzugeben. Als GmbH ist das Pfandhaus nach § 1 KStG körperschaftssteuerpflichtig, nach § 1 GewStG gewerbesteuerpflichtig und ggf. je nach Umsatzerzielung auch nach § 2 UStG Unternehmer im umsatzsteuerrechtlichen Sinne und daher verpflichtet, eine Körperschafts-, Gewerbesteuer und Umsatzsteuerjahreserklärung abzugeben. Je nach zahlungspflichtiger Umsatzsteuer ist er nach § 18 UStG verpflichtet, monatlich oder quartalsweise Umsatzsteuervoranmeldungen abzugeben. Des Weiteren verlangt der Staat in der Gestalt des Bundesjustizamt die Offenlegung von Jahresabschlüssen nach § 325 HGB oder zumindest je nach Größe der Kapitalgesellschaft die Hinterlegung beim Betreiber des Bundesanzeigers auf elektronischen Wegen.

[33] BGH, Urteil v. 26.01.2017 - IX ZR 285/14
[34] siehe Fn. 15.

Das Bundesamt der Justiz hat mitgeteilt, dass es in Abstimmung mit dem Bundesministerium der Justiz gegen Unternehmen, deren gesetzliche Frist zur Offenlegung von Rechnungslegungsunterlagen für das Geschäftsjahr mit dem Bilanzstichtag 31. Dezember 2021 am 31. Dezember 2022 endet, vor dem 11. April 2023 kein Ordnungsgeldverfahren nach § 335 des Handelsgesetzbuchs einleiten.[35]

Diese Ankündigung kann nun den Anschein erwecken, dass eine verspätete Aufstellung des Jahresabschlusses 2021 und der damit scheinbar verlängerten Offenlegungsfrist eine faktische Fristverlängerung bis zum 11. April 2023 gegeben ist. Jedoch stellt § 283b III StGB eine verspätete Aufstellung unter Strafe und eröffnet damit auch zivilrechtliche Ansprüche nach § 823 II BGB.

Kommt die GmbH in Zahlungsschwierigkeiten, droht also die Zahlungsunfähigkeit, so muss der Geschäftsführer nach § 15a i. V. m. § 18 InsO einen Antrag auf Insolvenzeröffnung stellen. Ab diesem Zeitpunkt ist der bisherige Gesellschafter-Geschäftsführer nicht mehr „Herr“ des Verfahrens, sondern der Insolvenzverwalter. Der Insolvenzverwalter bzw. oft zunächst der vorläufige Insolvenzverwalter wird vom Gericht bestellt und hat zu prüfen, inwieweit die Insolvenzmasse (Vermögen der Gesellschaft) so erhöht werden kann, dass damit die Verfahrenskosten, sein Honorar und die Gläubiger bedient werden können. Er wird genau prüfen, ob in der Vergangenheit die Jahresabschlüsse fristgerecht aufgestellt worden sind und erforderliche Maßnahmen, wie Risikomanagementsysteme wie es § 1 StaRUG vorsieht, installiert wurden. Aber auch, wenn der Geschäftsführer frühzeitig erkennt, dass eine Krise droht, so hat er nach § 1 StaRuG ein geeignetes Frühwarnsystem zu etablieren, damit er in den Genuss der außergerichtlichen Sanierung kommt. Weitere Voraussetzung ist, dass er seine bisherigen Verpflichtungen ordnungsgemäß und fristgerecht erfüllt hat und ihnen nachgekommen ist.

Der Vorstand einer Aktiengesellschaft ist nach § 91 II AktG verpflichtet, ein Überwachungssystem einzurichten, damit der Fortbestand des Unternehmens nicht gefährdet wird. Dies wird häufig als Risikomanagementsystem (RMS) bezeichnet. Sowohl in der Rechtsprechung als auch in der Literatur werden gerne RMS, CMS und IKS als synonyme bezeichnet. Allerdings soll das RMS ein mögliches Ereignis oder eine mögliche bestandsgefährdende Entwicklung, die dem Unternehmen oder dessen Kunden schaden könnte, davon erfassen. Inwieweit die Begriffe abgegrenzt werden können, wird am Ende der Arbeit

---

35 https://www.bundesjustizamt.de/DE/Themen/OrdnungsgeldVollstreckung/Jahresabschluesse/Jahresabschluesse_node.html

dargestellt. Diese Vorschrift, obwohl sie ins AktG explizit geschrieben wurde und keine entsprechende Regelung ins GmbHG aufgenommen worden ist, hat nach dem Willen des Gesetzgebers eine Ausstrahlungswirkung auf GmbHs, je nach Größe, Komplexität und ihrer Struktur.[36] Durch die explizite Neuregelung des § 1 StaRUG gehört es zu den Pflichtenkanon der Geschäftsleiter einer AG oder GmbH.[37]

Insgesamt zählen zum Risikomanagement alle organisatorischen Regelungen und Maßnahmen sowohl zur Risikoerkennung als auch zum Umgang mit den aus der unternehmerischen Betätigung entstehenden Risiken.[38] Das Risikomanagementsystem strukturiert das Risikomanagement und somit den Umgang mit Risiken im Unternehmen. Es handelt sich hierbei um einen Prozess aus mehreren Einzelschritten, die zwar nacheinander ablaufen, trotzdem aber auch miteinander zusammenhängen.[39]

Nicht nur durch die richterliche Rechtsfortentwicklung gehört es zu den Pflichten eines GmbH-Geschäftsführers, sondern nun auch explizit durch gesetzliche Regelungen wird bei unterlassener Einrichtung eines Frühwarnsystems dies als Sorgfaltspflichtverletzung angesehen. Das im März gefällte Urteil des OLG-Nürnbergs[40] hat den Pflichtenkanon durch ihre Auslegung zum § 130 OWIG und der Verpflichtung zur Überwachung des Unternehmens im Vier-Augen-Prinzips erweitert.

Das Vier-Augen-Prinzip ist ein wichtiger Bestandteil des Internen-Kontroll-Systems (IKS). Eine Begriffsbestimmung für das IKS findet sich bei den Prüfungsstandards des IDW unter PS 261, Tz. 19 ff. Demnach umfasst dieses System „die von dem Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) [...], die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen), zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften."

Der Geschäftsführer ist also nicht nur verpflichtet, darauf zu achten, ein Überwachungssystem zu etablieren, das den Fortbestand des Unternehmens sichert, sondern er hat auch neben dem Frühwarnsystem, welches Bestandteil

[36] Vgl. BT-Drs 13/9712, S. 15 zu Ziff. 7
[37] Flöther/Goetker, 1. Aufl. 2021, StaRUG § 1 Rn. 31
[38] Vgl. Boecker/Zwirner, IRZ 2014, 135 f.
[39] Vgl. ausführlich auch Boecker, Accounting Fraud aufdecken und vorbeugen, Berlin 2010, 312 ff.
[40] Fn. 15.

eines Risikomanagementsystems ist, ein funktionierendes und angemessenes IKS einzurichten. Dass er auf die Einhaltung sämtlicher Rechtsvorschriften achten muss, ergibt sich schon aus den originären Pflichten eines Geschäftsführers, so dass er durch die Einführung eines angemesseneren und wirksamen Compliance-Management-Systems sorgen soll, dass auch alle anderen Unternehmensmitarbeiter sämtliche Vorschriften befolgen.

Die zur Überwachung dienenden Corporate Governance Systeme sind

- Compliance Management System (CMS)
- Risikomanagementsystem (RMS),
- internes Kontrollsystem (IKS), und
- Internes Revisionssystem (IRS)

diese sind weder im Gesetz noch in der Literatur eindeutig definiert[41]. Im Mittelstand haben interne Revisionssysteme in der Regel keine Relevanz. Interne Revisionssysteme sind so einzurichten, dass ein unabhängiger Mitarbeiter im Unternehmen kontrolliert, ob die Mittelverwendungen so stattfinden, wie vorgesehen. Es ist vorgesehen, dass diese an der Geschäftsführung vorbei an die Gesellschafter bzw. für die für ein Unternehmen Verantwortlichen wie bei der Aktiengesellschaft der Aufsichtsrat berichten, wenn zu erwarten ist, dass die Organe, Geschäftsführung und Vorstand keine Abhilfe schaffen werden. Da im Mittelstand der Geschäftsführer meist mit dem Gesellschafter identisch ist und daher keine interne Revision eingesetzt wird, wird auf Ausführungen zur internen Revision verzichtet.

2.1 Compliance-Management-Systeme (IDW PS 980)

Die Entscheidung hinsichtlich Qualität und Ausmaß einer individuell angemessen ausgestalteten Compliance-Organisation obliegt jedenfalls bislang – und unter Ausnahmen – der unternehmerischen Entscheidung der Geschäftsleiter.[42] Compliance Management Systeme sind daher auf der Grundlage der von den Organen der Gesellschaft festgelegten Ziele[43] einzuführen. Diese müssen grundsätzlich festgelegt werden und angemessene Maßnahmen im Unternehmen entwickelt werden. Compliance umfasst die Einhaltung von internen und externen Vorgaben und soll sicherstellen, dass die gesetzlichen Vertreter, Geschäftsführer bei GmbHs und Vorstände bei Aktiengesellschaften und deren Mitarbeiter bestimmte Regeln einhalten und damit wesentliche Verstöße (Regelverstöße)[44] verhindert werden. Ein CMS iSd. IDW

[41] IDW EPS 982 aus 04-2017
[42] DStR 2021, 1238, beck-online
[43] vgl. IDW PS 980 Tz. 23
[44] vgl. IDW PS 980 Tz. A5

Prüfungsstandards 980 kann sich insb. auf Geschäftsbereiche, auf Unternehmensprozesse (z.B. Einkauf oder Beleihung) oder auf bestimmte Rechtsgebiete (z.B. Steuerrecht, Geldwäschegesetze, PfandIV, etc..) beziehen.[45] Das Unternehmen hat bei der Beschreibung ihres CMS Erklärungen zur Konzeption des CMS, die Grundelementen des CMS, die Angemessenheit sowie die Implementierung und die Wirksamkeit des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen zu einem bestimmten Zeitpunkt bzw. in einem bestimmten Zeitraum festzulegen und zu dokumentieren.[46]

2.1.1 CMS-Ziele

Damit das Unternehmen jedoch ein Compliance-Management-System einrichten kann, muss das Unternehmen zunächst überhaupt das Ziel definieren. Damit das Unternehmen das Ziel definieren kann, benötigt es einen Überblick, welche Rechtsgrundlagen einzuhalten sind und wodurch Regel- oder Rechtsverstöße entstehen können. Erst wenn das Unternehmen sich über die einzuhaltenden Gesetze, Verordnungen und Richtlinien und Regelungen bewusst ist, kann es im Unternehmen eine günstige Compliance-Kultur schaffen.
Aber wie formuliere ich die erforderlichen Ziele? Am besten das Unternehmen macht sich beginnend bei den allgemeinen gesetzlichen Verpflichtungen bis hin zu den spezielle gesetzlichen Regelungen Gedanken.
In der Regel fängt es mit der Aufstellung der Eröffnungsbilanz, der Einrichtung der Buchhaltung an und geht weiter bis hin zu den zur Ausübung der gewinnwirtschaftlichen Tätigkeit einzuhaltenden Spezialnormen. Nach § 242 I HGB hat jeder Kaufmann zu Beginn seines Handelsgewerbes eine Eröffnungsbilanz aufzustellen. Nach § 238 HGB ist er verpflichtet, Bücher zu führen und somit jeden Geschäftsvorfall aufzuzeichnen. § 239 HGB schreibt vor, wie die Handelsbücher zu führen sind. Diese gesetzliche Verpflichtung ist in den Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern konkretisiert. Aufgrund der zunehmenden Digitalisierung sind diese durch das Bundesamt der Finanzen (BMF) überarbeitet und erweitert worden. Bei den Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[47] handelt es sich um ein BMF-Schreiben vom 14. November 2014. Es ist

[45] vgl. IDW PS 980 Tz. A3
[46] Vgl. IDW PS 980.Tz 7
[47] Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (BMF-Schreiben vom 28.11.2019)

seit dem 01. Januar 2015 in Kraft und löste die Vorgängerschreiben GoBS[48] und GDPdU[49] ab. Die GoBD werden flankiert von den sog. „ergänzenden Informationen zur Datenträgerüberlassung“. Hierbei handelt es sich um eine Hilfestellung, die insbesondere an kleinere und mittlere Unternehmen gerichtet ist und Hinweise bezüglich der zu überlassenden Daten im Rahmen einer steuerlichen Außenprüfung enthält. Diese grundlegende Verpflichtung betrifft jeden Kaufmann, der ein Handelsgewerbe betreibt.

Der Unternehmer muss Regeln aufstellen, wie mit Belegen, Erfassung von Einnahmen, Dokumentation von Geschäftsvorfällen umzugehen ist. Wer veranlasst Zahlungen, wer überprüft die Rechnungen, etc…

Wer sorgt dafür, dass die erforderlichen Steueranmeldungen ggf. Umsatzsteuervoranmeldungen und Lohnsteueranmeldungen fristgerecht und ordnungsgemäß abgegeben werden. Ziel ist also die Einhaltung von handelsrechtlichen und steuerrechtlichen Vorschriften. Es ist wichtig, dem verantwortlichen Mitarbeiter die Rechtsnormen klarzumachen und ggf. welche Folgen, die Nichtbeachtung haben kann.

2.1.2 CMS-Kultur

Zur CMS-Kultur gehört es, dass die Unternehmensleitung Mitarbeiter sensibilisiert, diese zur Einhaltung von Gesetzen, Regeln, Vorgaben „erzieht“ und selbst darauf achtet mit gutem Beispiel voranzugehen. Die Compliance Kultur soll als Werte des Unternehmens, quasi als die Verfassung, verstanden werden.[50] Nur wenn ein werteorientiertes kommunikatives Ziel gemeinsam erarbeitet und gelebt wird, kommt es zu einer Compliance-Kultur.[51]

„Der Mensch ist von Natur aus böse, wenn er dennoch gut ist, so ist dies die Frucht der Kultur.“ —Xunzi[52]

Bereits im 17. Jahrhundert fand man in den USA heraus, dass Versicherungsnehmer von Feuerversicherungen fahrlässiger handelten als Unversicherte. Daraus entstand der Begriff Moral Hazard, Moral Hazard heißt auf Deutsch so viel wie moralisches Risiko. Versicherungsnehmer von Feuerversicherungen handelten fahrlässiger als Unversicherte und somit wurde durch die Versicherungsverträge risikofreudiges Verhalten begünstigt. Konkret

[48] Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (BMF-Schreiben vom 07.11.1995)
[49] Grundsätze zum Datenzugriff und zur Prüfbarkeit distaler Unterlagen (BMF-Schreiben vom 16. Juli 2001)
[50] Fissenewert, E-Book Seite 11
[51] Fissenewert, ebenda
[52] Xunzi, auch Hsün-Tse oder, in Wade-Giles Umschrift, Hsün-Tzu, war ein chinesischer Philosoph gegen Ende der Zeit der Streitenden Reiche. Seine Lehren werden dem Konfuzianismus zugerechnet. Gleichzeitig ist Xunzi auch der Name seines Werkes.- https://gutezitate.com/zitat/210255

wurde beobachtet, dass im Falle einer Feuerversicherung beispielsweise weniger Feuerlöscher installiert wurden. Der Menschen muss ständig Verlockungen und Versuchungen widerstehen. Moral Hazard erklärt, warum Menschen sich oft unmoralisch verhalten, wenn ihnen die Gelegenheit geboten wird. Moral und Ethik geben Verhaltensnormen in einer Gesellschaft oder einem Unternehmen vor. Wird der Vorgesetzte als moralisch integer bezeichnet und lebt er einen gewissen Verhaltenskodex vor, so wird dies auch eher von anderen Mitarbeitern übernommen und gelebt. Interaktionen werden innerhalb einer sozialen Gruppe reguliert. So gibt die Moral vor, was in Ordnung ist und welche Grenzen nicht überschritten werden dürfen.[53]

Derjenige, der die Gelegenheit hat, wird diese ergreifen, wenn er für sich eine Rechtfertigung hat, und er unterstellt, dass eigentlich keinem einen Schaden entsteht. Dies ist oft bei Versicherungsbetrugsversuchen zu sehen, da hier meist kein Unrechtsbewusstsein besteht. Man zahle ja schließlich Beiträge und letztlich hat ja keiner einen Schaden. Es wird schlicht übersehen, dass der Schaden ja von allen, der Allgemeinheit, letztlich durch die steigenden Versicherungsbeiträge gezahlt wird. Wird dies jedoch in das Bewusstsein genommen, so reduziert sich bei der Mehrheit unrechtmäßiges Verhalten.

In der Wirtschaftsprüfung spricht man vom sog. FRAUD-Dreieck:

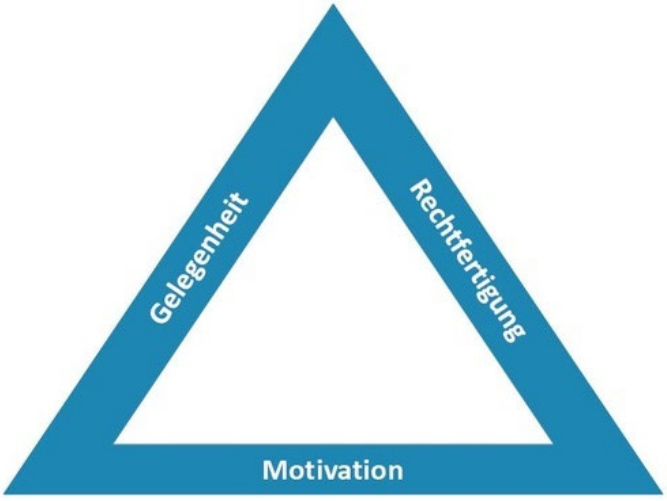

Abbildung 1: Fraud Triangel[54]

Übertragen auf unser Pfandhaus und dessen Buchführung bedeutet es, die korrekte Erfassung von Einnahmen und Ausgaben sowie der fristgemäßen Abgabe von Steueranmeldungen oder -erklärungen stellt die Finanzierung des Staates sicher, sichert den eigenen Arbeitsplatz und der Allgemeinheit öffentliche

[53] Fissenewert, E-Book. 7

[54] https://www.compliance-praxis.at/Themen/Management_Organisation/Archiv/Risk_Assessment_aus_forensischer_Sicht.html

Ausgaben für Schulen und Kindergärten. Darüber hinaus steigt das Ansehen des Unternehmens. Alles ist letztlich der Unternehmenskultur geschuldet. Damit es auch tatsächlich eine Unternehmenskultur wird, sind zunächst die Mitarbeiter zu charakterisieren. Unterschiedliche Charaktere müssen unterschiedlich „angepackt“ werden. Schulungen der Mitarbeiter sind so zu gestalten, dass diese die Werte des Unternehmens nicht nur vorgestellt bekommen, sondern aktiv leben. Bei einer deutschen Ländergesellschaft eines amerikanischen Konzerns konnte beobachtet werden, dass die Mitarbeiter zwar alle brav das Compliance-Handbuch gelesen haben und die Multiple-Choice Fragen anschließend richtig beantwortet haben, dennoch war überhaupt kein Bewusstsein vorhanden, welche Regelungen den Mitarbeiter nun selbst im Unternehmen betreffen. Die Wirtschaftsprüfer stellten fest, dass zahlreiche innerdeutsche Vorschriften verletzt wurden, da sich darüber von Seiten des Konzerns keiner Gedanken machte. Erst ein Wechsel der Geschäftsführung der deutschen Gesellschaft veränderte das Bewusstsein der Mitarbeiter.

2.1.3 CMS-Risiken

Aufgrund von immerwährenden neuen wirtschaftlichen Herausforderungen ist auch der Gesetzgeber auf europäischer und nationaler Ebene aktiv neue verbraucherschützende Regelungen zu schaffen. Unternehmen müssen diese Änderungen fortlaufend bewerten. Dies hat Auswirkungen auf die tägliche Arbeit der Unternehmen. Daher sind die Compliance Ziele von den Verantwortlichen festzulegen und zu identifizieren. Die Identifizierung, Dokumentation und Bewertung dieser Risiken stellen den Verantwortlichen oft erst einmal vor eine schwierige Aufgabe. Denn er muss sich über die richtige Herangehensweise Gedanken machen. Die Methodik ist wichtig und ggf. mit einem vorhandenen Risikomanagement im Unternehmen abzustimmen. Viele Unternehmen würden gar nicht funktionieren, wenn sie nicht bereits die Risiken ermittelt hätten. Jedes Unternehmen muss für sich die Organisation so bestimmen, dass es leicht von der Hand geht und die tägliche Arbeit unterstützt. Daher empfiehlt es sich, die tägliche Arbeit zu analysieren und nicht am „grünen“ Tisch die Vorgaben aus Compliancesicht zu machen. Bei der Ermittlung der Risiken sollte die Geschäftsführung (top-down) ebenso wie einzelne Unternehmensbereiche (bottom-up) eingebunden werden. Zusammen mit den Mitarbeitern sollten Workshops abgehalten und die tägliche Arbeit dokumentiert werden. Die Mitarbeiter sollten in einer Diskussion eingebunden werden, damit sie Risiken im Unternehmen besser einschätzen lernen. Werden die Prozesse zu detailliert erfasst, kann sich dies dauerhaft als hinderlich herausstellen. Es sind zwei Arten

der Herangehensweisen zu empfehlen. Zum einen sollten Risikoszenarien vorgegeben werden und gemeinsam erarbeitet werden. Zum anderen sollte (zunächst) die Erarbeitung auf einzelne wichtige Rechtsgebiete beschränkt werden, damit eine Überforderung verhindert wird. Die Compliance-Risiken müssen beurteilt werden (zum Beispiel Aufzeichnungspflichten) und deren Ausmaß sowie Eintrittswahrscheinlichkeit bestimmt werden.

Damit keine Risiken im CMS vergessen werden, hilft es Checklisten zur Risikoidentifikation anzufertigen oder Arbeitsabläufe niederzuschreiben. Wenn eine Liste der Geschäftsprozesse in allen vorhandenen Unternehmensbereichen erstellt wird und dort die Arbeitsschritte dokumentiert werden, kann dies als Checkliste in den Unternehmensbereichen dienen, die der Compliancebeauftragte auf die Einhaltung von zutreffenden Vorschriften abgleicht. Allgemein zugängliche Risikokataloge der Branche können ebenso hilfreich sein und helfen eine gewissen Vollständigkeit zu erreichen.

So wäre bei dem Beispiel des mittelständischen Pfandhauses zunächst festzustellen, dass eine Verpflichtung zur vollständigen, zeitnahen, wahrheitsgemäßen und unveränderlichen Erfassung aller Geschäftsvorfälle vorzunehmen ist. Nach § 264 I S. 3 HGB besteht die Verpflichtung, zum Ende des Geschäftsjahres innerhalb von 6 Monaten den Jahresabschluss aufzustellen und innerhalb von 12 Monaten nach Abschluss des Geschäftsjahres diesen nach § 325 HGB offenzulegen. Wird dies nicht gemacht, so macht sich der für das Unternehmen Verantwortliche nach § 283b StGB strafbar und setzt sich damit auch etwaigen zivilrechtlichen Schadenersatzansprüchen ggf. nach § 823 II BGB i. V. m. § 283b StGB aus. Überträgt er nun diese Aufgabe auf Mitarbeiter, so hat er erforderliche organisatorische Maßnahmen zu ergreifen, damit sichergestellt ist, dass dieser seine Aufgaben erfüllt. Ist sich der Mitarbeiter über die Bedeutung seiner Tätigkeit im Klaren, so ist von innenheraus auch das Risikobewusstsein vorhanden.

2.1.4 CMS-Organisation

Erst wenn der Prozess zur Feststellung und Analyse der Compliance-Risiken durch das Unternehmen[55] abgeschlossen ist, kann ein sinnvolles Compliance-Programm zum Aufbau der Compliance Organisation (Aufbau- und Ablauforganisation) entwickelt werden.[56]

Hat man nun die Compliance-Risiken identifiziert, so hat man im nächsten Schritt, diese zu bewerten. Durch die Bewertung erfolgt eine Priorisierung, um die

[55] IDW PS 980 Tz. 10
[56] IDW PS 980, TZ 42

erforderlichen und angemessenen Maßnahmen daraus ableiten zu können. Die Bewertung erfolgt nach gleichen Maßstäben wie die des Risikomanagements. Letztendlich wird bei der Bewertung die potenzielle Schadenhöhe ermittelt sowie eine Eintrittswahrscheinlichkeit. Über eine Matrix stuft man die Risiken in gering, mittel, hoch und sehr hoch ein (siehe Abbildung 2 für ein Beispiel).

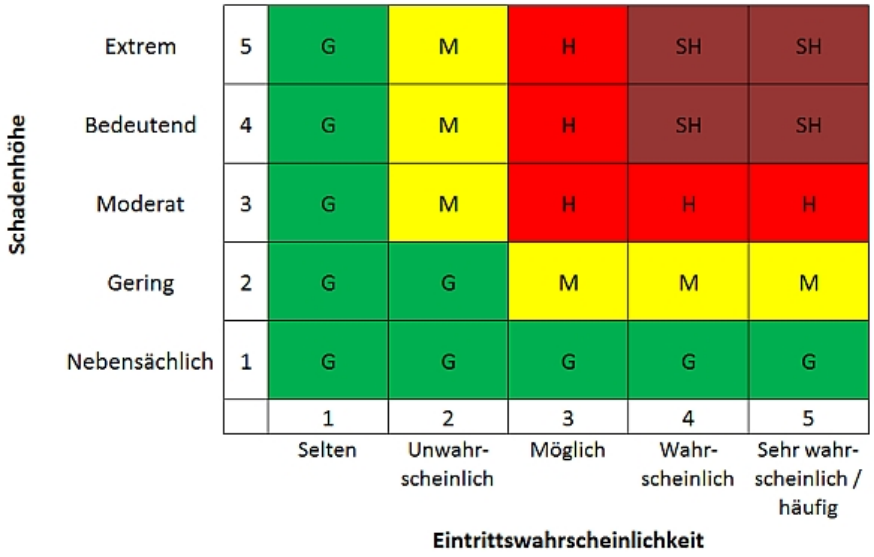

Abb. 2 [57]

Bei einem CMS kann meist die Schadenshöhe nicht ermittelt werden. Jedoch sollte auch bei Compliance-Risiken eine genaue quantitative Beurteilung dieser Schwierigkeit; beispielsweise, wenn der Schaden eine Rufschädigung mit sich bringen könnte, eingeordnet werden. Letztlich ist es immer eine Kombination von quantitativen und qualitativen Bewertungsrisiken bzw. Bewertungsmaßstäben. Die Risikobewertung erfolgt ohne Berücksichtigung eventueller Risikostrategien und -maßnahmen (= Bruttorisikobewertung). Mit der Bruttorisikobewertung schafft man die Grundlage zur Bestimmung der Risikostrategie. Auf dieser Grundlage kann entschieden werden, das Risiko zu reduzieren, es zu vermeiden, zu teilen (zum Beispiel durch eine Versicherung) oder weiter zu beobachten. Die Maßnahme hängt von der definierten Strategie ab und entscheidet welche Maßnahmen eingeleitet werden.

Nach der Bruttorisikobewertung erfolgt die Nettorisikobewertung. Nun betrachtet man die potenzielle Schadenshöhe und die Eintrittswahrscheinlichkeit des Risikos unter Berücksichtigung der Maßnahmen. Sie erlaubt die Beurteilung, ob das Restrisiko für das Unternehmen akzeptabel ist.

Es empfiehlt sich zur Dokumentation dieser Schritte ein Risikoregister einzurichten. Damit das CMS den ständigen Veränderungen angepasst werden kann, ist eine regelmäßige Aktualisierung beziehungsweise Wiederholung der

[57] https://www.compliance-manager.net/sites/default/files/abb1_0.jpg

Compliance-Risikoanalyse und -bewertung notwendig. Sofern das Unternehmen ein Risikomanagement hat, ist es erforderlich, dass sich beide Verantwortliche für CMS und RMS, sofern diese nicht sowieso ein und dieselbe Person sind, im Hinblick auf Methodik und Durchführung miteinander abstimmen. Es ist wenig zweckhaft, dass die Funktionen unterschiedliche Methoden zur Erfassung und Bewertung von Risiken verwenden. Sind sie nicht abgestimmt, besteht die Gefahr, dass die operativen Einheiten verwirrt werden, ebenso die Berichtsempfänger (zum Beispiel die Geschäftsführung/Vorstand). Es ist auch wenig förderlich für eine Abstimmung untereinander – schließlich muss das Compliance-Management zumindest die wesentlichen Compliance-Risiken an das Risikomanagement melden, damit dieses einen wirklichen Überblick über die Risikosituation des Unternehmens erlangen kann. Die weitere Gefahr ist, dass eine unterschiedliche Herangehensweise dazu führt, dass es keine Akzeptanz der Funktionen im Unternehmen gibt.

Zudem ist erforderlich, dass die Ermittlung und Aktualisierung der Risiken gemeinsam mit den verschiedenen Unternehmensbereichen durchgeführt werden. Regelmäßige Risikoaktualisierungstermine des Risikomanagements mit den Geschäftsbereichen, sollte ebenso stattfinden wie mit dem Compliance Management, in denen die Betrachtung der Compliance-relevanten Risiken abgestimmt werden.

Regelmäßige Kommunikation der Compliance-Risiken an das Risikomanagement, und idealerweise ein allgemeiner Austausch zur Risikosituation, ist nicht nur empfehlenswert, sondern auch notwendig.

Die Methodik zur Identifizierung, Bewertung und Dokumentation von Compliance-Risiken erlaubt es Unternehmen, diese strukturiert zu erfassen und zu priorisieren. Dies ermöglicht eine solide Basis zur Ableitung der Compliance-Maßnahmen im Rahmen des CMS. Idealerweise erfolgt das Compliance-Risikomanagement in enger Abstimmung beziehungsweise Zusammenarbeit mit dem Risikomanagement des Unternehmens.

Dies übertragen auf das Pfandhaus bedeutet, dass die Buchhaltung, der Geldwäschebeauftragte, ggf. der Datenschutzbeauftragte, der Mitarbeiter, der für die Versteigerungen bzw. der Bewertung und Begutachtung der Pfandgüter zuständig ist, regelmäßig in ihren Bereichen die Kommunikation mit der Geschäftsführung und den Kollegen suchen.

2.1.5 CMS-Kommunikation

Steht die Compliance-Organisation so folgt die Compliance Kommunikation. Ganz wichtig! Es muss miteinander gesprochen werden! Allen Mitarbeitern sind

die Rollen und die Verantwortlichkeiten der verschiedenen Abteilungen und Unternehmensbereichen darzustellen. Ebenso ist wichtig, festzulegen, wie mit Verstößen umgegangen werden soll und an wen zu berichten ist. Funktionsfähige Kommunikationsprozesse und -instrumente sind eine zentrale Voraussetzung für ein effizientes, effektives und nachhaltiges Compliance-Management-System (CMS).[58]

2.1.6 CMS-Weiterentwicklung

Doch auch wenn das System eingerichtet ist, hat die Unternehmensleitung weiterhin das System zu überwachen und bei Feststellung von Mängeln diese zu beheben und das System ständig zu verbessern.

In der Rechtsprechung werden die Compliance-Anforderungen ständig fortentwickelt. So wurde bereits im BGH-Urteil vom 09.05.2017 (1 StR 265/16) anerkannt, dass bei der Bemessung einer Geldbuße gegen ein Unternehmen zu berücksichtigen ist, ob zum Zeitpunkt von Gesetzesverstößen ein angemessenes und effektives Compliance Management System installiert gewesen ist. In die Bußgeldbemessung ist auch miteinzubeziehen, ob das Unternehmen im Zuge der Aufklärung der Non-Compliance zu Tage getretene Defizite des Compliance Management Systems behebt und Maßnahmen ergreift, um vergleichbare Normverletzungen in Zukunft zu verhindern oder zumindest wesentlich zu erschweren. Im Entwurf wird diesbezüglich hervorgehoben, dass zum Nachweis der jederzeitigen Angemessenheit des CMS im Zeitablauf und der kontinuierlichen Anwendung der Regelungen die Dokumentation unbeschadet von Aufbewahrungspflichten über einen ausreichend langen Zeitraum aufbewahrt werden sollte.

Meist ist sich der mittelständische Unternehmensleiter gar nicht bewusst, dass er bereits durch das tägliche „Doing“ zwar die Maßnahmen ergriffen hat, diese jedoch nicht dokumentiert hat.

Wie bereits unter 2 dargestellt hat ein Pfandleihhaus viele Rechtsvorschriften, die es bei der täglichen Arbeit berücksichtigen muss und die die Mitarbeiter im Umgang mit den Kunden beachten müssen.

2.2 Risikomanagementsytem nach IDW PS 981 (RMS)

Nach § 4 GWG ist ein angemessenes und wirksames Risikomanagementsystem in den Unternehmen einzurichten. Aber auch in anderen Gesetzen, wie § 91 II AktG hat ein Vorstand einer Aktiengesellschaft (AG) geeignete Maßnahmen zu ergreifen, um den Fortbestand eines Unternehmens zu sichern. Auch in der

[58] Vgl. IDW PS 980 Tz. 17

Gesetzesbegründung zu § 91 II AktG führte der Gesetzgeber aus, dass diese Regelungen eine Ausstrahlungswirkung auch auf GmbHs haben sollen.[59] Wie bereits dargestellt, ist in § 1 StaRUG verpflichtend für alle Unternehmen ein funktionierendes Risikofrühwarnsystem einzurichten. Das Frühwarnsystem ist ein wichtiger Bestandteil des Risikomanagementsystems. Geschäftsführer von UGs (haftungsbeschränkt), GmbHs oder auch GmbH & Co. KGs sind verpflichtet, rechtszeitig Krisenursachen zu erkennen (Krisenfrüherkennung). Es reicht jedoch nicht aus, die Krisenursache zu erkennen, sondern es sind auch geeignete Gegenmaßnahmen einzuleiten und dem entgegenzusteuern (Krisenmanagement). Der Gesetzgeber hat darauf verzichtet, diese Regelung auf bestimmte Unternehmen zu beschränken, so dass auch kleine und mittlere Unternehmen (KMU) ein angemessenes und wirksames Risikomanagement einrichten müssen. Dieses System ist der Größe und den Risiken des Unternehmens anzupassen und zu implementieren, so dass sie ihre individuellen Risiken einschätzen können. Egal, ob es sich um ein Krisenunternehmen handelt oder nicht, haben die Geschäftsleiter die Verpflichtung, das Frühwarnsystem einzurichten. Der Gesetzgeber geht davon aus, dass jeder Geschäftsführer fortlaufend über die Entwicklungen in seinem zu leitenden Unternehmen, welche den Fortbestand der juristischen Person gefährden könnte, informiert ist. Diese Vorgabe ist auch nicht neu. Bereits in § 49 III GmbHG ist der Geschäftsführer verpflichtet, eine Gesellschafterversammlung einzuberufen, wenn die Hälfte des Stammkapitals aufgezehrt ist. Daher ist es auch logisch, dass der Geschäftsführer verpflichtet ist, bestandsgefährdende Entwicklungen systematisch zu erkennen und verpflichtet ist, geeignete Gegenmaßnahmen zu ergreifen, um ggf. den Überwachungsorgangen (Gesellschaftern) unverzüglich Bericht zu erstatten. Da die Ausgestaltung eines Risikomanagementsystems von der Art des Unternehmens und der Größe stark abweichen kann, gibt das Gesetz keine Hinweise, wie es auszugestalten ist. In der Bundestagsdrucksache ist zur Gesetzesbegründung zu lesen, dass die „konkrete Ausformung und Reichweite … von der Größe, Branche, Struktur und auch der Rechtsform des jeweiligen Unternehmens“[60] abhängt. Des Weiteren stellt die Begründung klar, „dass es sich namentlich bei kleineren Unternehmen verbietet, übermäßige Organisationspflichten zu statuieren.“

Würde also nun ein Risikomanagementsystem nach der ISO 31000 eingerichtet werden, so wäre dies sicherlich für KMUs überspannt und kann daher deutlich einfacher gehalten werden. Als Mindestanforderung sollte für das zur

[59] BT-Drucks. 19/24181, S. 104
[60] A.a.O.

Krisenfrüherkennung eingerichtete RMS die Verhältnisse des Unternehmens und die Geschäftsentwicklungen, die für die Tätigkeit des Unternehmens relevant sind, laufend betrachtet werden und überprüft werden, ob sie das Potenzial haben, bei ungehindertem Fortgang den Fortbestand des Unternehmens zu gefährden.

Die Gesetzesbegründung verweist in diesem Zusammenhang auf die Business Judgement Rule. Es führt dazu aus: “Hinsichtlich der Auswahl der zu treffenden Gegenmaßnahmen und deren Durchführung steht den Geschäftsleiter der Beurteilungsspielraum zu, der ihnen nach Maßgabe der spezialgesetzlichen Regelungen für Maßnahmen der Geschäftsführung zuzubilligen ist.“

Die unternehmerische Entscheidung ist nach der Business Judgement Rule „auf der Grundlage angemessener Information“ (§ 93 Abs. 1 S. 2 AktG) abzustellen.

Dies bedeutet, dass das Krisenfrüherkennungssystem angemessene Informationen für die Maßnahmen des Krisenmanagements liefern müssen. Das Risikomanagementsystem ist, soweit es der Krisenfrüherkennung dient, so zu installieren, dass es diese angemessenen Informationen sicherstellt und bereithält. Von der Angemessenheit einer Information darf dann ausgegangen werden, wenn der Einschätzung eines vernünftig urteilenden Geschäftsleiters zur Folge die Verbesserung der Informationsqualität den dafür erforderlichen Aufwand an Zeit bzw. Geld nicht mehr rechtfertigt.[61]

Ein RMS i.S. des IDW PS 981 weist die folgenden miteinander in Wechselwirkung stehenden Grundelemente auf, die in laufenden Geschäftsabläufen eingebunden werden. Bei der Konzeption des RMS sind die Wechselwirkungen zwischen den Grundelementen zu berücksichtigen. Die Ausgestaltung des RMS hängt insb. von den festgelegten Zielen des RMS sowie von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens ab[62]:

Folgende Elemente sind dabei zu beachten:

1. Risikokultur
2. Ziele des RMS
3. Organisation des RMS
4. Risikoidentifikation
5. Risikobewertung
6. Risikosteuerung
7. Risikokommunikation
8. Überwachung und Verbesserung des RMS.

[61] Matthias Graumann: „Angemessene Informationsgrundlage von Prognosen bei unternehmerischen Entscheidungen“, 15. Januar 2021, ZIP 2021, S. 69.
[62] IDW PS 980, 4 Rdn. 31

Die Elemente des RMS sind sehr ähnlich zu den Elementen des CMS bzw. gleichen sich. Beide Systeme greifen, wie bereits dargestellt, auch ineinander. Da man beim Aufbau und Betrieb eines Risikomanagementsystems die Größe, Branche und Komplexität des Unternehmens berücksichtigen muss, stellt sich auch oft die Frage, welcher Aufwand an Zeit und Geld einzusetzen ist. Der zusätzliche Aufwand, den man für ein „Mehr“ an Informationsqualität investiert, sollte in einem vernünftigen Verhältnis durch ein entsprechendes „Mehr“ an Entscheidungsqualität gedeckt sein. Die durch die verbesserten Informationen gewonnen Erkenntnisse sollen nach Grenzaufwand und Grenznutzen zueinander im Verhältnis stehen.
Das Risikomanagementsystem sollte nicht in auffälliger Weise der Einschätzung eines vernünftig urteilenden Geschäftsleiters zuwiderlaufen. Nach der Business Judgement Rule, lässt sich das Risiko als Geschäftsleiter so weitgehend reduzieren.

2.2.1 Risikokultur

Die Risikokultur fördert wie beim CMS die grundsätzliche Einstellung der im Unternehmen tätigen Mitarbeiter. Es zeigt, wie der Umgang mit Risikosituationen erfolgen soll, ob Risiken bewusst eingegangen werden oder erst gar nicht gesehen werden. Sind sich die Mitarbeiter nicht bewusst, welches Risiko sie durch ihr Verhalten dem Unternehmen aussetzen und damit möglicherweise den Verlust ihres Arbeitsplatzes riskieren, so kann daraus kein Risikomanagementsystem entstehen. So muss dem Mitarbeiter klar sein, dass er durch ggf. zu hohen Beleihungen das Unternehmen gefährdet, da es auf Dauer Verluste erwirtschaftet und er damit aktiv dazu beigeträgt. Es muss ein Bewusstsein geschaffen werden, welche Risiken in einem Unternehmen zu erkennen sind. Zunächst sind die einzelnen Risiken auf der kleinsten Ebene zu bewerten. Als erstes sollte zu jedem einzelnen Risiko das mögliche Schadensausmaß vgl. bei CMS Abb. 1 in Geld abgeschätzt werden. Dies ist erforderlich, damit man die Auswirkungen auf den Gewinn oder die Liquidität bei Schadenseintritt und damit das Schadenspotenzial (=S) beziffern kann.
Danach sollte die Eintrittswahrscheinlichkeit (E) bestimmt werden und mit dem Schadenspotenzial (S) multipliziert werden, um das Produkt zum Risiko-Wert (R) zu erhalten. Damit ergibt sich folgende Formel:

(R = S x E).

Daraus kann man nun das Gesamtrisiko (S R) aggregieren und somit bestimmen, welchem Gesamtrisiko (S R) das Unternehmen ausgesetzt ist. Zunächst sollte jedoch eine Gegenüberstellung der Risikoexposition (S R) mit der

Risikotragfähigkeit erfolgen, wie sie sich aus der integrierten Finanzplanung ergeben könnte. Daraus kann dann der Grad der Existenzgefährdung abgelesen werden und zeigt damit den erforderlichen Handlungsbedarf.
Das Unternehmen muss konkret betrachtet werden. Sollte ein Gesamtrisiko von 300.000€ bestehen, das Unternehmen hält allerdings ausreichend Liquiditätsreserven vor und erzeugt zudem einen jährlichen positiven Cashflow, sind keine weiteren Maßnahmen erforderlich. Sind die Liquiditätsreserven jedoch gar nicht vorhanden oder sehr knapp und die Cashflows eher ausgeglichen oder negativ, so liegt wohl eine existenzgefährdende Risikoexposition vor. Damit sind entsprechende Maßnahmen der Risikosteuerung dringend notwendig.
Bei unserem Pfandhaus könnte ein Risiko, die Nichterfassung von Verkäufern von Gold sein. Nach dem Geldwäschegesetz sind zwar die Daten eines Goldverkäufers bis zu 10.000 Euro nicht zu erfassen, jedoch sind nach § 143 AO sämtliche Adressdaten eines Einlieferers zu erfassen. Hat nun der Mitarbeiter diese Daten nicht erfasst und macht das Finanzamt im Rahmen einer Betriebsprüfung gem. § 160 AO von ihrem Auskunftsverlangen Gebrauch, so besteht die Gefahr, dass der Ankauf des Goldes als Betriebsausgabe aufgrund formaler Mängel nicht als Betriebsausgabe anerkannt wird. Hat nun das Unternehmen für 1 Mio. Gold angekauft und kann dafür die Einlieferer nicht benennen, so entsteht bei einem Steuersatz von 30% (15% KSt und 15% GewSt) ein Schaden von 300.000 Euro. Da bereits jedoch die 1 Mio. als Ausgabe tatsächlich abgeflossen ist, kann dieser Betrag einen existenzbedrohenden Eingriff darstellen.

2.2.2 Ziele des RMS

Damit die Ziele des RMS formuliert werden können, ist zunächst die Unternehmensstrategie festzulegen. Anhand der Unternehmensstrategie ist die Risikostrategie festzulegen. Unternehmenspolitische Zielsetzungen bilden die Ausgangsbasis, die jedoch insbesondere die Tragfähigkeit bestimmter Risiken (Risikotragfähigkeit) des Unternehmens berücksichtigen muss. Ebenso hat der Unternehmensleiter mit seinen unternehmerischen Vorgaben zu bestimmen, wie mit einzelnen Risiken umzugehen ist. Damit steuert er den „Risikoappetit“. Aus Risikostrategie, Risikotragfähigkeit und Risikoappetit wird die Risikopolitik festgelegt.
Die Ziele des RMS sind darauf ausgerichtet sicherzustellen, dass die Unternehmensziele entsprechend der Risikostrategie erreicht werden.[63]

[63] Vgl. IDW PS 981

2.2.3 Organisation des RMS

Für den Aufbau eines RMS ist es erforderlich, die Organisation transparent darzustellen. Eine klare Definition zu Ablauf und Verantwortlichkeiten, die die Rollen regelt, abgegrenzt, kommuniziert und dokumentiert ist erforderlich. Nach dem IDW PS 981 ist Risikomanagement im Unternehmen zu institutionalisieren. Es ist zu empfehlen, einen Verantwortungsbereich "Risikomanagement" zu schaffen. Bei den meisten mittelständischen Unternehmen wird dies der Unternehmer selbst oder eine nahestehenden Person sein, die das "Risikomanagement" übernimmt. In größeren Einheiten spricht man von Corporate-Risk-Management. Es kommt häufig vor, dass der „Risikocontroller“ als Controller wahrgenommen wird, der jedoch nichts mit der Erreichung betriebswirtschaftlicher Ziele zu tun hat. Das Unternehmen muss die verantwortlichen Mitarbeiter persönlich und fachlich ausbilden und ihnen ausreichende Ressourcen für Risikomanagementmaßnahmen zur Verfügung stellen (insb. Personen, Technologien, Hilfsmittel).[64] Die wesentlichen Regelungen zur Aufbau- und Ablauforganisation sind nach dem IDW PS 981 zu dokumentieren und durch die Verantwortlichen verbindlich vorzugeben.

Merkmale der Organisation des RMS sind nach dem Anwendungshinweis des IDW PS 981 u.a.

1. die klare Festlegung von Rollen und Verantwortlichkeiten im RMS. Hierzu gehören die Festlegung der Verantwortlichkeit für die Koordination und Steuerung des RMS sowie die Festlegung der Aufgaben und der hierarchischen Stellung bzw. der organisatorischen Einordnung und der Berichtslinien. Diese Aufgabe kann durch eine Stelle/Abteilung oder durch ein Gremium (z.B. Risikokomitee) ausgeführt werden. Die Festlegung der Rollen und Verantwortlichkeiten wird in der Praxis zum Teil anhand des "Three-lines-of-Defense Modells" vorgenommen.[65]
2. die Festlegung der Ablauforganisation, insb. für die Risikoerkennung, Risikosteuerung, Kommunikation und Überwachung. Hierzu gehört auch die Festlegung von Rahmenvorgaben zu Methoden des Risikomanagements sowie der Verzahnung mit weiteren Corporate Governance Systemen und Steuerungsinstrumenten. Die Ablauforganisation wird in Form von Handbüchern oder Regelwerken dokumentiert und kommuniziert. Es können unterschiedliche Stellen oder Abteilungen mit Risikomanagementaufgaben befasst sein, unabhängig davon, ob diese als "Risikomanagement" bezeichnet werden (z.B. Risikomanagementaktivitäten im Controlling, in der

[64] Vgl. IDW PS 981, Tz A24
[65] Vgl. IDW PS 981, Tz. 45

Treasury, im Qualitätsmanagement oder in der strategischen Planung). In kleineren Unternehmen werden Aufgaben des Risikomanagements zum Teil zentral von der Geschäftsführung selbst wahrgenommen.

3. Einsatz technischer Hilfsmittel und erforderlichenfalls einer angemessenen IT-Unterstützung in den einzelnen RMS-Grundelementen (z.B. web-basierte Abfragesysteme und Controlling Systeme).

Risikomanagement im Mittelstand ist nicht Aufgabe einer wie auch immer bezeichneten und wo auch immer organisatorisch angesiedelten Abteilung, sondern Risikomanagement geht jeden Mitarbeiter im Unternehmen an und ist primär Aufgabe jedes Mitarbeiters.

Die tatsächliche Umsetzung des RMS muss in der Praxis von den Mitarbeitern in ihren Aufgaben- und Verantwortungsbereichen umgesetzt werden. Teamleiter und/oder Prozessverantwortliche sind in ihren Zuständigkeiten verantwortlich für die Umsetzung. Das ist schon allein deshalb sinnvoll, da die Risiken vor Ort entstehen (z. B. in der Beleihung) und der vor Ort Zuständige und Verantwortliche (z. B. Gutachter für Edelsteine) das Risikopotenzial am besten erkennen, bewerten und diesem entsprechend gegensteuern kann. Von ihm geht auch die Risikokommunikation aus.

2.2.4 Risikoidentifikation

Da ein Unternehmen ein dynamischer Organismus ist, ist die Analyse der Ereignisse und Entwicklungen permanent im Hinblick zu den Risiken zu betrachten. Stark veränderte Risiken, wie bspw. die Rohstoffpreisentwicklung, Verknappung von Gütern, etc…, werden ständig bzw. in kürzeren Abständen beobachtet. Risiken, die sich nicht so schnell verändern, wie z.B. Betriebsunterbrechungen, können mit größeren Abständen analysiert werden und im Ein- oder Mehrjahresrhythmus angesehen werden. Dies ist jedoch nur dann der Fall, wenn die Veränderung der Organisation, Prozesse oder Geschäftsmodell weniger Eingriffe bedarf. Eine systematische Risikoidentifikation sollte unter Einbezug der verschiedenen Ebenen und Funktionen des Unternehmens, nach dem IDW PS 981, einbezogen werden. Diese umfassen u.a. die folgenden Merkmale:

1. eine (vollständige) Betrachtung der Ursachen und Faktoren wesentlicher Risiken sowohl innerhalb des Unternehmens als auch im Umfeld, bspw. unterstützt durch themen- bzw. branchenspezifische Risikokataloge
2. eine systematische Analyse von Frühwarnindikatoren und Kennzahlen, aus deren Beobachtung frühzeitig mögliche kritische Entwicklungen erkannt werden können. Diese können sowohl aus vorausschauenden Indikatoren

und Prognosewerten bestehen (Früherkennung) als auch der Aufdeckung von Schadensfällen und der Analyse von Trends dienen.

3. Analyse sowohl aus Sicht der Unternehmensleitung (Top Down) als auch aus Sicht der operativ mit der Erkennung und Steuerung von Risiken befassten Bereiche (Bottom Up)
4. Erfassung und Kommunikation von als kritisch erkannten Entwicklungen an die für die nachfolgende Risikobewertung und -steuerung zuständigen Bereiche
5. eine vollständige und nachvollziehbare Dokumentation der Risikoidentifikation.

Grundsätzlich sind sich die folgenden Fragen zu stellen:

a) Welche Risiken haben das Potenzial, den Fortbestand des Unternehmens zu gefährden? (Identifikation von Risiken)
b) Wie hoch wird das Schadenspotenzial der einzelnen identifizierten Risiken geschätzt? (Bewertung von Risiken)
c) Wie geht das Unternehmen mit den Risiken um? (Steuerung von Risiken durch konkrete Maßnahmen wie z. B. Vermeiden/Vermindern/Transferieren/Akzeptieren)
d) Wie wird die Wirksamkeit der Maßnahme gemessen? / Wann und wie oft werden diese bewertet? (Regelmäßige Überwachung von Risiken)
e) Wie stellt sich die Risikosituation übersichtlich dar und zeigt die Wirksamkeit der Maßnahmen? (Bericht der Risiken)

2.2.5 Risikobewertung

Damit ein hoher Wirkungsgrad der Risikosteuerung erzielt werden kann, ist die Bewertung der Risiken transparent, nachvollziehbar und nach einer konsistent angewandten Systematik vorzunehmen. Durch Bildung von. „best case“ und „worst case“-Szenarien können gemessen an der Zielabweichung die Auswirkungen bestimmt werden. Wichtig dabei ist, dass auch die Zeitabläufe identisch sind. Abhängig von der Branche können diese Zeithorizonte zu unterschiedlichen Zeiten durchgeführt werden.

Die Eintrittswahrscheinlichkeit kann qualitativ (z.B. hoch, mittel oder niedrig), quantitativ (z.B. durch Angabe von Prozentwerten oder Bandbreiten) sowie durch Angabe einer Häufigkeit bezogen auf einen Zeitraum bestimmt werden.[66]

Dauerhafte strategische Risiken werden ebenfalls quantitativ bewertet. Sofern operative oder strategische Risiken nicht objektiv nachvollziehbar bewertet werden können (wie bspw. das Risiko eines Imageverlustes), erfolgt eine

[66] IDW PS 981, Tz A25

qualitative Bewertung. Hierbei sollte aber auch eine Abschätzung der Risikotragweite nach festgelegten Kriterien (bspw. über eine Bandbreitenzuordnung oder der Klassifizierung bspw. als "high priority risk") erfolgen. Die Bewertungsergebnisse sind Grundlage für die weitere Verwendung zu Steuerungs-/Überwachungszwecken im RMS. Es ist erforderlich, die Bewertungsmethoden festzulegen; qualitativ Risiken zu bewerten und in zuvor definierte Wertklassen einzuordnen. Auf dieser Basis kann auf übergeordneter Ebene in regelmäßigen Abständen eine Aggregation der ermittelten Einzelrisiken für einzelne Risikofelder erfolgen. Hierbei werden Korrelationen berücksichtigt. Zur qualitativen Unterstützung der Risikobewertung kann es u.U. sachgerecht sein, Verfahren der Risikosimulation einzusetzen.
Der Prozess der Risikobewertung sollte nachvollziehbar dokumentiert werden, z.B. als Prozessbeschreibung in einer Risikorichtlinie, einem RM-Handbuch oder einer bereichs- oder funktionsbezogenen Verfahrensanweisung.
Das Unternehmen sollte quantitative und qualitative Faktoren festlegen.

Beispiele für quantitative Faktoren sind:

1. Anteil am Gesamtumsatz
2. Verhältnis der Ergebnisbeiträge
3. Netto-Investitionssumme
4. Angestrebte/geplante Rendite.

Beispiele für qualitative Faktoren sind:

1. Dezentraler Autonomiegrad des Managements
2. Komplexität des Geschäftsmodells
3. Grad der Regulierung/Anfälligkeit für Regelverstöße
4. Standardisierungsgrad von Prozessen
5. Zentralisierung von Prozessen und Funktionen
6. Standardisierung wesentlicher Entscheidungen
7. Marktstrukturen und Veränderungsdynamik des Marktes.

2.2.6 Risikosteuerung

Wie die Risikosteuerung umgesetzt wird, obliegt der Entscheidung des Unternehmensleiter. Diese sollte durch die Beurteilung der Einzelrisiken und einer nachvollziehbaren Erläuterung gegenüber den Mitarbeitern erfolgen. Zur besseren Nachvollziehbarkeit sollte dies schriftlich dokumentiert werden. Grundsätzlich sollten ggf. regulatorische Anforderungen bei der Ausgestaltung der Risikosteuerung berücksichtigt werden. In der Dokumentation sollten vertragliche Verpflichtungen (bspw. bei Versicherungsverträgen), Vorgaben zum

Risikoappetit oder Wirtschaftlichkeitsüberlegungen sowie explizite Maßnahmen zur Risikosteuerung enthalten sein.

Die Geschäftsleitung hat die Risikosteuerungsmaßnahmen zu überwachen. Die Überwachung der Risikosteuerungsmaßnahmen beschränkt sich hierbei auf die grundsätzliche Umsetzung und die Wirksamkeit eingeleiteter Risikosteuerungsmaßnahmen.

Durch die Bestimmung von Maßnahmen bei bestimmten Kriterien kann eine systematische Risikosteuerung erfolgen. Die Maßnahmen sind hinsichtlich ihres Umsetzungsstandes ("in Planung" vs. "initiiert" vs. "bereits effektiv umgesetzt") zu beurteilen.

Die in das RMS involvierten Personen werden im Hinblick auf die Ziele des RMS, den RM-Prozess und die eingesetzten Verfahren und Tools angemessen geschult. Das RMS, möchte man es iSd § 1 I StaRUG einrichten, kommt ohne eine integrierte Finanzplanung nicht aus. Dies zeigt einmal mehr, dass auch ein RMS ohne die entsprechenden Verzahnungen zu anderen Bereichen nicht eigenständig betrieben werden kann. Letztendlich dient alles zum Schutz des Unternehmens und sollte so auch verstanden werden. Die vorgeschriebenen Überwachungen von (Fehl-)Entwicklungen (=Risiken), die den „Fortbestand der juristischen Person gefährden“ sollen in erster Linie dem Unternehmen helfen und nicht die Verantwortlichen belasten. Bestandsgefährdungen können nur durch eine Gegenüberstellung, von Risikoexposition und Risikotragfähigkeit erkannt werden, wie sie sich aus einer integrierten Finanzplanung ergeben. Aus diesem Grund ist von einer Verpflichtung aller KMUs haftungsbeschränkter Gesellschaftsformen auszugehen,[67] ab sofort integrierte Finanzplanungen zu erstellen, die als geschlossenes und schlüssiges Zahlenwerkt ein Risikomanagement ermöglichen, das den Anforderungen des § 1 I StaRUG genügt.

2.2.7 Risikokommunikation

Die Risikokommunikation umfasst u.a. die folgenden Elemente:

1. Kommunikation der Regelungen des RMS und von relevanten Risikobereichen an die betroffenen Personen
2. Festlegung der Berichtspflichten (Anlässe und Zeitpunkte) und der Berichtswege für die Kommunikation von Risiken an die zuständigen Stellen im Unternehmen einschließlich Unternehmensleitung und Aufsichtsgremien
3. Sicherstellung aktueller, zutreffender entscheidungsrelevanter Informationen.

[67] Matthias Kühne und Frank Lienhard, „Ausgestaltung eines Risikofrüherkennungssystems gemäß § 1 StaRUG und die Haftungsfolgen für die Geschäftsleitung“, SanB 2020, S. 144.

Der Prozess der Risikokommunikation ist nachvollziehbar festzulegen und zu dokumentieren z.B. Terminvorgaben, Berichtsformate und Kommunikationswege. Die Kommunikation der Regeln des RMS kann z.B. in Form von Mitarbeiterbriefen, RMS-Handbüchern oder Schulungsveranstaltungen erfolgen.
Das Format und die Struktur der Berichterstattung sind adressatengerecht und aussagefähig auszugestalten. Die übersichtliche Darstellung der Risikosituation erfolgt bspw. in einem regelmäßigen Risikobericht in standardisierter Form. Hierin kann eine Clusterung der Risiken nach ihrer Wesentlichkeit erfolgen, sodass eine Priorisierung der Risiken für Steuerungs-/Überwachungszwecke möglich ist. Die hierzu festzulegenden Grenzbereiche werden maßgeblich durch die jeweils gewählte Risikostrategie bestimmt. Eskalationsstufen können auf der Basis angemessener Schwellenwerte eingerichtet werden.
Für eilbedürftige Risikomeldungen ist ein Verfahren zur ad hoc-Risikoberichterstattung etabliert. Die Risikomeldung erfolgt hierbei initial durch die jeweils betroffene Berichtseinheit.
Voraussetzung für eine angemessene Risikokommunikation ist, dass entscheidungsrelevante Informationen so aus internen und externen Quellen gesammelt, aufbereitet, geprüft und aktualisiert werden, wie sie nach wirtschaftlichem Ermessen für die Risikoidentifikation und Risikobewertung von den hierfür Verantwortlichen benötigt werden.

2.2.8 Überwachung und Verbesserung des RMS

Das Unternehmen hat schriftliche Vorgaben für die prozessintegrierte Überwachung des RMS als Prozessbeschreibung (bspw. in einer Risikorichtlinie bzw. einem RM-Handbuch oder einer Verfahrensanweisung der jeweiligen Organisationseinheit) jedem Mitarbeiter auszuhändigen. Eine systematische prozessintegrierte Überwachung sollte implementiert sein. Eine regelmäßige Prüfung der Aktualität und Angemessenheit des Risikomanagements muss in regelmäßigen Abständen vorgenommen werden.
Eine wichtige Funktion im Bereich der prozessintegrierten Überwachung des RMS bilden die speziell für dessen Ablaufprozesse etablierten Kontrollen, z.B. Überwachung der Risikoidentifikation und -bewertung durch einen Risikobeauftragten. Diese werden auf Ebene sämtlicher in das RMS einbezogenen Organisationseinheiten (bspw. Zentralbereiche wie Treasury, Einkauf etc., operative Einheiten) implementiert und in Abhängigkeit von Komplexität und Bedeutung der jeweiligen RMS-Prozesse ausgestaltet. Sie dienen der Vermeidung bzw. Begrenzung ablauforganisatorischer Risiken innerhalb des RMS.

Die Überwachung beinhaltet auch regelmäßige Beurteilungen des RMS, die sowohl auf die Angemessenheit als auch auf dessen Wirksamkeit gerichtet sind.
Gegenstand einer prozessunabhängigen Überwachung können u.a. folgende Aspekte sein:

1. Vollständige Erfassung aller Risikofelder des Unternehmens
2. Angemessenheit der eingerichteten Regelungen zur Risikoerfassung und Risikokommunikation
3. Angemessenheit und kontinuierliche Anwendung der Risikosteuerungsmaßnahmen vor dem Hintergrund der gewählten Risikostrategie und der Ziele des RMS
4. mögliche beabsichtigte Umgehungen eingerichteter Prozesse und Kontrollen.

Die Ergebnisse von Überwachungsmaßnahmen werden zwecks Ursachenanalyse und Entwicklung von Maßnahmen zur Verbesserung des RMS im Unternehmen kommuniziert.
Ergeben sich im Rahmen der Überwachung oder bei sonstigen Maßnahmen des RMS Hinweise auf Mängel des RMS, werden als Bestandteil der Durchsetzung des RMS Maßnahmen zur Verbesserung des RMS (z.B. Schulungen, Änderung von Berichtslinien und -frequenzen sowie -inhalten, Sanktionen etc.) getroffen. Stand und Verbesserungspotenzial des RMS werden z.B. anhand von Best Practices, Benchmarking oder Reifegradmodellen beurteilt.

2.3 Internes Kontrollsystem (IKS) IDW PS 982

Wie auch schon bei der Einführung von CMS und RMS liegt die Verantwortung bei der Installation, der Durchführung und der Überwachung eines funktionierenden und auf das Unternehmen abgestimmten IKS bei der Geschäftsführung. Die Geschäftsführung muss festlegen, an wen, was und wann berichtet werden muss. Zudem ist ein wesentlicher Bestandteil des IKS das VIER-AUGEN-PRINZIP sowie die Funktionstrennung. Die Personalabteilung ist von der Buchhaltung zu trennen. Wer für die Bestellung von Ware verantwortlich ist, hat nicht auch die Zahlungen freizugeben. Es sollte eine klare Aufgabenverteilung vorhanden sein. Diese Aufgabenverteilung ist zu beschreiben und nachprüfbar zu hinterlegen. Wird das Unternehmen nach § 316 HGB prüfungspflichtig, so ist auch festzulegen, wie die rechnungslegungsrelevanten Informationen in das Berichtswesen einfließen.[68]
Kontrolle bzw. Überwachung ist ein „mehrstufiger Informations- und Entscheidungsprozess, der alle Maßnahmen umfasst, durch die festgestellt

[68] Vgl. IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) (Stand: 24.09.2002), Tz. 14, 19 ff.

werden soll, ob Zustände oder Vorgänge einer Norm entsprechen bzw. normgerecht durchgeführt werden“.[69] Das interne Kontrollsystem (IKS) stellt die Gesamtheit aller Regelungen (Grundsätze, Verfahren und Maßnahmen) eines Unternehmens dar, die

1. die Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (inklusive Schutz des Vermögens, Verhinderung und Aufdeckung von Vermögensschädigungen).
2. die Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
3. die Einhaltung der relevanten rechtlichen Vorschriften

zum Ziel haben.[70]

Ein internes Kontrollsystem iSd des IDW-Prüfungsstandards 982 weist die folgenden miteinander in Wechselwirkung stehenden Grundelemente auf, die in die Geschäftsabläufe eingebunden sind.

1. Kontrollumfeld
2. IKS-Ziele
3. Risikobeurteilung
4. Kontrollaktivitäten
5. Information und Kommunikation
6. Überwachung des internen Kontrollsystems

Bei der Konzeption des internen Kontrollsystems sind die Wechselwirkungen zwischen den Grundelementen zu berücksichtigen. Wie auch schon bei den anderen Systemen ist die Ausgestaltung an das Unternehmen von Komplexität und Branche abhängig.

Anders als beim CMS oder RMS stellt das IKS keine eigene Abteilung dar. IKS ist das gelebte VIER-AUGEN-PRINZIP, in dem niedergeschrieben wird, wer welche Aufgabe wahrnimmt und wer diese überwacht. Die Lohnabrechnungsstelle erstellt die Lohnabrechnungen, erstellt die Meldungen zur Lohnsteuer, Sozialversicherung und Unfallversicherung, die Buchhaltungsabteilung überwacht den Mittelabfluss und die Geschäftsleitung gibt die Zahlungen frei. In der Literatur werden sowohl die Begriffe „internes Kontrollsystem (IKS)“ als auch „internes Überwachungssystem (IÜS)“ verwendet[71], was zuweilen Verwirrung stiftet. Nach dem Institut der

[69] Lück in DB 1998, S. 9
[70] Vgl. IDW PS 261 n. F., Tz 19
[71] Lück, DB 1998 S. 9 f.

Wirtschaftsprüfer stellt das IKS den Oberbegriff dar.[72] Es besteht aus dem IÜS und dem internen Steuerungssystem.

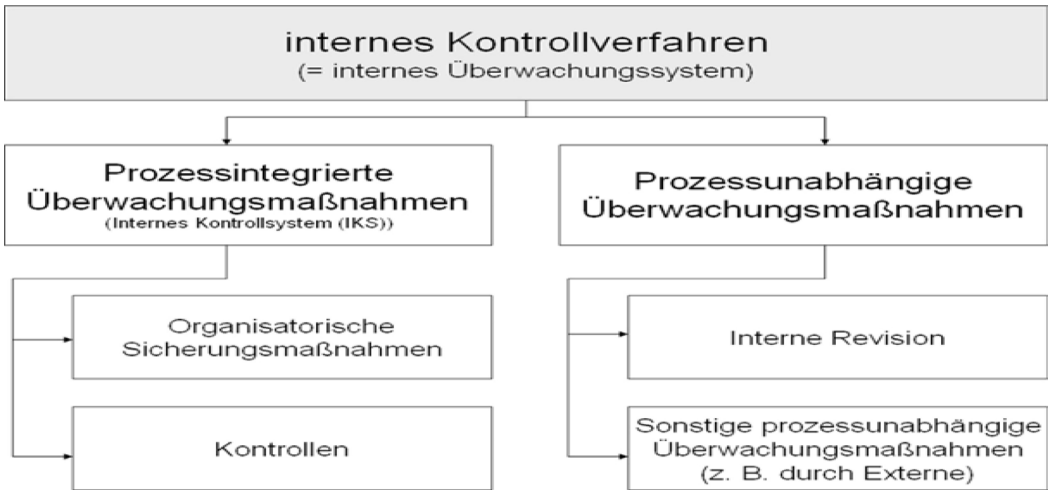

Abb. 3: Regelungsbereiche der internen Kontrollverfahren[73]

Das interne Kontrollsystem steht dem sog. Compliance-Management-System (CMS) inhaltlich sehr nahe.[74] Während das interne Kontrollsystem alle Bereiche eines Unternehmens umfasst, wird in der Abschlussprüfung lediglich die jahresabschlussbezogenen IKS geprüft. Gerade im IKS wird das VIER-AUGEN-Prinzip für alle Geschäftsbereiche manifestiert, wohingegen das CMS sich meist mit Regelverstößen bzw. der Verhinderung von Regelverstößen beschäftigt. Wie bereits dargestellt, bildet der Dreiklang zwischen CMS, RMS und IKS die Grundlage von einer guten Unternehmensführung der sog. Corporate Governance.

2.3.1 Wer ist verpflichtet, ein internes Kontrollsystem einzurichten?

Spätestens mit der Entscheidung des OLG Nürnberg [75] wird klar, dass jedes Unternehmen und sei es noch so klein, ein funktionierendes IKS einrichten muss. Unterlässt das Unternehmen die Einrichtung und kommt deshalb jemand zu Schaden, so begeht der Geschäftsführer eine Ordnungswidrigkeit nach § 130 OWIG, was zumindest nach dem OLG Nürnberg eine Haftung nach § 823 II BGB begründet. Aktiengesellschaften sind nach § 107 III 2 AktG verpflichtet, dieses einzuführen. Daneben gibt es branchenabhängige Unternehmen, die verpflichtet sind, dieses einzurichten, dazu zählen Kreditinstitute und Versicherungsgesellschaften. Das Überwachungsorgan der AG, also der Aufsichtsrat, hat folgendes zu überwachen:

[72] IDW PS 261 n. F., Tz 20
[73] Welsch/Foshag in: Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, 2. Aufl. 2019, I.5 Internes Kontrollsystem Compliance – Gestaltungsmöglichkeiten zur Überwachung von Compliance-Grundsätzen, -Mitteln und -Verfahren
[74] Graumann, wirtschaftliches Prüfungswesen, S. 235
[75] Fn. 15

1. den Rechnungslegungsprozesses,
2. die Wirksamkeit des internen Kontrollsystems,
3. das Risikomanagementsystems und
4. ggf. das internen Revisionssystems.

Letztendlich hat er damit die folgenden Systeme zu überwachen:

1. internes Kontrollsystem (IKS),
2. Risikomanagementsystem (RMS),
3. internes Revisionssystem (IRS) und
4. Compliance Management System (CMS)

Diese Regelung gibt es nur im Aktienrecht und AGs haben diese Verpflichtung einzuhalten. In mittelständischen Unternehmen existiert meist kein Aufsichtsrat, auch wenn er fakultativ bei der GmbH implementiert werden kann. Dennoch hat der Geschäftsführer, wenn auch sicherlich in „abgespeckter" Version, diese Systeme zu implementieren, auch wenn er nicht überwacht wird, da er meist auch selbst der Gesellschafter ist. Nach § 46 GmbHG haben jedoch die Gesellschafter die Geschäftsführung zu überwachen. Wie bereits zu den RMS und CMS beschrieben, ist weder durch den Gesetzgeber noch in der Literatur eindeutig definiert, wie ein solches System auszusehen hat. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme verweise ich auf die bereits dargestellten Ausführungen. Unterlässt allerdings der Geschäftsführer eines Unternehmens organisatorische Maßnahmen, wie die Wahrung des Vier-Augen-Prinzips und entsteht dadurch anderen ein Schaden, so kann er hierfür haften.[76]

2.3.2 Wie ist das interne Kontrollsystem aufzubauen

Das interne Kontrollsystem ist so aufzubauen, dass durch eine vernünftige Funktionstrennung und einem einzuführenden Freigabesystem eine Kontrolle möglich wird. Nehmen wir unser Pfandleihhaus. Der Mitarbeiter, der vom Kunden ein Pfandgut entgegennimmt, hat dieses zu bewerten. Damit hier bereits eine Kontrolle möglich wird, übergibt er es einem fachkundigen Kollegen, der das Gut bewertet. Während der eine Mitarbeiter das Pfandgut bewertet, überprüft, der andere Mitarbeiter, ob Mitteilungen zu Diebstählen von der örtlichen Polizei vorliegen. In der Regel arbeiten Pfandleiher und die Polizei so eng miteinander, dass diese per Fax, sobald Diebesgut im Umlauf ist, von der Polizei informiert werden. Hat der Bewerter nun den Beleihungswert festgelegt, so kann der annehmende Mitarbeiter Verplausibilisieren, ob er auf einen ähnlichen Betrag

[76] OLG Nürnberg, Urt. v. 30. 3. 2022 - 12 U 1520/19 ECLI:DE: OLGNUER:2022:0330.12U1520.19.00

kommt. Letztlich soll das Pfandgut ja die Kosten, Zinsen und ggf. die Versteigerungsgebühren bei einer Versteigerung erzielen. Ist der Beleihungswert ermittelt, bekommt der Kunde den Betrag mitgeteilt. Ist der Kunde einverstanden, so hat der Mitarbeiter, der den Kunden bedient, nun das Pfandgut zu katalogisieren und der Kasse, die durch einen weiteren Mitarbeiter bedient wird, die Mitteilung zu geben, welches Pfandgut (mit Pfandschein) mit welchem Betrag beliehen werden kann. Damit ist sowohl bei der Bewertung als auch bei der Auszahlung eine weitere Kontrollinstanz eingebunden. Es ist dabei auch wichtig, dass bestimmte Wertgrenzen definiert werden, ab welchem Betrag die vorgesetzte Stelle bzw. die Geschäftsführung einzubinden ist.

2.3.2.1 Das Kontrollumfeld

Damit ein echtes Kontrollbewusstsein entstehen kann, ist zunächst ein günstiges Kontrollumfeld zu schaffen. Den Mitarbeitern muss die Notwendigkeit der einzelnen Schritte klar sein. Es darf auch nicht so sein, dass der Mitarbeiter fahrlässig wird, denn er wird ja nochmal kontrolliert. Es muss in das Bewusstsein der Mitarbeiter, dass es zum Schutz des Unternehmens und letztendlich zum Schutz ihres Arbeitsplatzes eingeführt wurde. Je glaubwürdiger der Vorgesetzte es lebt, umso bestrebter sind die Mitarbeiter diese Struktur einzuhalten.
Das Kontrollumfeld nach dem IDW PS 982 kann insb. durch die folgenden Merkmale beeinflusst werden:

1. Das Unternehmen verpflichtet sich zur Wahrung der Integrität und zur Einhaltung ethischer Werte.
2. Die Unternehmensleitung gibt Verhaltensgrundsätze vor und richtet die persönlichen Verhaltensweisen konsequent an den vorgegebenen Prinzipien aus.
3. Das Aufsichtsorgan ist unabhängig von den gesetzlichen Vertretern und übt seine Überwachungstätigkeit in Bezug auf die Entwicklung und Funktionsfähigkeit des internen Kontrollsystems angemessen aus.
4. Das Unternehmen führt Maßnahmen, Berichtsstrukturen sowie angemessene Berechtigungen und Verantwortlichkeiten zur Erfüllung der Ziele des internen Kontrollsystems ein.
5. Das Unternehmen verpflichtet sich, in Übereinstimmung mit den Zielen des internen Kontrollsystems Mitarbeiter mit der notwendigen Kompetenz anzuwerben, weiterzuentwickeln und zu binden.
6. Das Unternehmen schafft klare Verantwortlichkeiten für seine Mitarbeiter im Zusammenhang mit deren Rolle im internen Kontrollsystem, um die Zielerreichung zu unterstützen.

7. Die Unternehmensorganisation beachtet die Grundsätze der Funktionstrennung und ist den Mitarbeitern bekannt gemacht.

2.3.2.2 IKS-Ziele

Das Ziel des IKS soll nicht nur einen Schaden des Unternehmens, sondern auch von den Kunden verhindern. Es muss ein Berichtswesen für die Geschäftsführung etabliert werden, welches es möglich macht, dass die Geschäftsführung jeden einzelnen Vorgang nachvollziehen kann. Daher ist es erforderlich, dass die Geschäftsführung jedem Mitarbeiter die Ziele, die durch das IKS verfolgt werden, nahebringt. Einer besonderen Bedeutung kommt das IKS für Rechnungslegungszwecke zu. Diese sind besonders zu dokumentieren und ggf. in Anhang und Lagebericht je nach Größe des Unternehmens mit aufzunehmen. Handelt es sich um ein prüfungspflichtiges Unternehmen, so wird dies von Wirtschaftsprüfern geprüft.

2.3.2.3 Risikobeurteilung

Die Geschäftsführung hat die Risiken zu beurteilen. Damit die Beurteilung nicht von Tagesform der Geschäftsführung abhängt, sollte systematisch vorgegangen werden und wie auch beim CMS und RMS die Risiken bewertet werden. Es wird genauso mit Eintrittswahrscheinlichkeit und Schadenshöhe gearbeitet.
Damit die Risikobeurteilungen systematisch beurteilt werden kann, hat der IDW PS 982 folgende Grundsätze entwickelt:

1. Das Unternehmen spezifiziert seine IKS-Ziele für das Berichtswesen mit hinreichender Klarheit, sodass die damit zusammenhängenden Risiken identifiziert und analysiert werden können.
2. Das Unternehmen identifiziert die zur Erreichung seiner IKS-Ziele für das Berichtswesen relevanten Risiken ganzheitlich und analysiert und bewertet diese Risiken.
3. Das Unternehmen berücksichtigt die Möglichkeit von Verstößen bei der Beurteilung von Risiken für die Erreichung der IKS-Ziele.
4. Das Unternehmen identifiziert und beurteilt Veränderungen, die einen wesentlichen Einfluss auf das interne Kontrollsystem nehmen könnten.

2.3.2.4 Kontrollaktivitäten

Die Kontrollaktivitäten sind in Steuerungs- und Kontrollmaßnahmen mit fehlervermeidender und fehleraufdeckender Wirkung zu unterscheiden.
Durch die tägliche Praxis entstehen Erfahrungswerte, aus denen sich häufige Fehler ableiten lassen. Die Kontrollaktivität soll diese Fehler vermeiden. Dies ist von fehleraufdeckenden Maßnahmen zu unterscheiden. Fehler, die begangen

worden sind, werden durch eine nachgelagerte Überprüfung festgestellt und werden im Idealfalle behoben oder zumindest so dokumentiert und erkannt, dass sie zukünftig nicht mehr vorkommen können. Durch das Bewusstsein der Mitarbeiter, dass die Vorgänge auch im Nachhinein nochmal überprüft werden, entsteht ein positiver Effekt, da der Mitarbeiter bemüht ist, alles gleich richtig zu machen und so Fehler schneller vermieden werden.

Nach dem IDW PS 982 können Steuerungs- und Kontrollmaßnahmen durch folgende Grundsätze beeinflusst werden:

1. Das Unternehmen führt Steuerungs- und Kontrollmaßnahmen aus, welche die Risiken im Hinblick auf die IKS-Ziele für das Berichtswesen auf ein akzeptables Niveau reduzieren.
2. Das Unternehmen führt Steuerungs- und Kontrollmaßnahmen im Zusammenhang mit den für Zwecke des Berichtswesens eingesetzten IT-Systemen aus, um eine effektive Zielerreichung zu unterstützen.
3. Das Unternehmen führt Steuerungs- und Kontrollmaßnahmen aus, indem es Verfahrensanweisungen und Maßnahmen zu deren Umsetzung implementiert.
4. Kontrollaktivitäten können in manuelle und IT-Kontrollen unterschieden werden. Mögliche überwiegend manuelle Kontrollaktivitäten betreffen bspw.:
   - 4.1 Funktionstrennungen
   - 4.2 Genehmigungsverfahren und Unterschriftsregelungen
   - 4.3 Unabhängige Gegenkontrollen (4-Augen-Prinzip)
   - 4.4 Kennzahlenanalysen
   - 4.5 Physische Inaugenscheinnahme.
   - 4.6 Mögliche Maßnahmen und Verfahren, die sich im Wesentlichen auf die IT-Infrastruktur beziehen, können sein:
   - 4.7 Physische IT-Sicherungsmaßnahmen
   - 4.8 Logische IT-Zugriffskontrollen
   - 4.9 Datensicherungs- und Auslagerungsverfahren
   - 4.10 Maßnahmen für den geordneten IT-Regelbetrieb sowie für den Notbetrieb
   - 4.11 Maßnahmen zur Sicherung der IT-Betriebsbereitschaft.
5. Mögliche IT-Kontrollen, die sich im Wesentlichen auf die Geschäftsprozesse der Unternehmensberichterstattung beziehen, können sein:
   - 5.1 In den IT-Anwendungen enthaltene Eingabe-, Verarbeitungs- und Ausgabekontrollen

5.2 Alle im IT-System vorgesehenen prozessinternen Kontrollen und organisatorischen Sicherungsmaßnahmen, z.B. Berechtigungskonzepte oder Netzwerkkontrollen

5.3 Maßnahmen, die sich unabhängig von einer einzelnen IT-Anwendung auf das gesamte IT-System auswirken (z.B. Kontrollen zur Entwicklung, Einführung und Änderung von IT-Anwendungen).

2.3.2.5 Information und Kommunikation

Wie auch schon beim CMS und dem RMS ist die Informationspolitik und die unternehmensweite Kommunikation das A und O. Die Mitarbeiter müssen in ihrer täglichen Arbeit wissen, bei welchen Entscheidungen sie andere Mitarbeiter einzubinden haben und welche Kompetenz diese Kollegen haben. Es sind Regeln aufzustellen aus denen erkannt werden kann, bis zu welchen Größenordnungen welcher Mitarbeiter die Entscheidungsgewalt hat. Die Informationswege sind am besten grafisch darzustellen, so dass schnell erkannt wird, wer bei welchen Prozessen einzubeziehen ist.

Information und Kommunikation können gem. IDW PS 982 durch die folgenden Maßnahmen positiv beeinflusst werden:

1. Das Unternehmen erhält oder generiert und nutzt relevante sowie qualitative Informationen zur Unterstützung der Funktionsfähigkeit des internen Kontrollsystems.
2. Das Unternehmen kommuniziert intern die notwendigen Informationen zur Unterstützung der Funktionsfähigkeit des internen Kontrollsystems (einschließlich der Ziele der Steuerungs- und Kontrollmaßnahmen und der Verantwortlichkeiten für die Steuerungs- und Kontrollmaßnahmen).
3. Das Unternehmen kommuniziert mit Externen, bspw. Lieferanten, in Bezug auf Sachverhalte, die einen Einfluss auf die Funktionsfähigkeit des internen Kontrollsystems haben.
4. Das Unternehmen sorgt durch entsprechende Schulungs- und Informationsmaßnahmen dafür, dass die Mitarbeiter ihre Rolle und Bedeutung im jeweiligen Prozess und deren Abhängigkeiten von vor- und nachgelagerten Prozessschritten bzw. internen Kontrollen kennen.

2.3.2.6 Überwachung des internen Kontrollsystems

Die Verantwortlichen sollten Überwachungsmaßnahmen so anlegen, dass eine Überprüfung unvorhergesehen stattfinden können. Es ist auch nicht erforderlich, dass alle Vorgänge überprüft werden. Den Maßstab der Überwachungsmaßnahmen sollte nur den für die Überwachung verantwortlichen bekannt sein. Die Überwachung kann durch Prozessbeschreibungen sowie nach

Sichtung der dokumentieren Vorgänge erfolgen. Es ist dabei ein Soll-/Ist-Vergleich vorzunehmen.
Je nach Größe des Unternehmens wird hierfür auch die interne Revision genutzt. Bei kleinen und mittelständischen Unternehmen erfolgt meist die Überwachung durch die Geschäftsführung selbst oder durch besonders qualifiziertes Vertrauenswürdige Mitarbeiter.
Die Überwachung und Verbesserung des internen Kontrollsystems sind im IDW PS 982 wie folgt beschrieben:

1. Das Unternehmen nimmt kontinuierliche und/oder separate objektive Beurteilungen vor, um das Vorhandensein und die Funktion der sechs Grundelemente des internen Kontrollsystems festzustellen.
2. Das Unternehmen beurteilt und kommuniziert Mängel im internen Kontrollsystem zeitnah an die für deren Behebung Verantwortlichen sowie an die gesetzlichen Vertreter und ggf. das Aufsichtsorgan.
3. Das Unternehmen verbessert durch die tatsächliche (zeitnahe) Behebung von Mängeln sowie die Implementierung notwendiger (Interim-) Steuerungs- und Kontrollmaßnahmen das interne Kontrollsystem.

2.3.2.7 IKS-Beschreibung

Die Beschreibung des IKS ist so zu gestalten, dass ein objektiver Dritter oder auch neue Mitarbeiter schnell erkennen können, wie die Aufgaben und Zuständigkeitsverteilung im Unternehmen sind. Je größer das Unternehmen, desto umfangreicher ist die Beschreibung vorzunehmen. Bei kleineren Unternehmen reicht es meist ein Organigramm zu erstellen und wie bereits beschreiben ein Informationsdiagramm zu erstellen. Diese Grafiken können ausgehängt werden, so dass eine Übersicht schnell vorhanden ist.
Etwas umfangreicher wird es, wenn das Unternehmen größer ist, dann empfiehlt es sich, dass die IKS-Beschreibung Angaben zu den der Unternehmensberichterstattung zugrundeliegenden Rechnungslegungs-vorschriften (bspw. HGB, IFRS, US-GAAP) enthält, da dieser Einfluss auf die Ausgestaltung der Regelungen haben können.
Da dies bei KMUs eher untergeordnete Bedeutung hat, wird auf die weiteren Ausführungen dazu verzichtet.

2.3.3 Rechtsgrundlagen und Rechtsfolgen

Da zunächst davon ausgegangen wurde das IKS nur etwas für größere Unternehmen, insbesondere für AG ist wurde auch aus der

Gesetzesbegründung[77] zum BilMoG ausgeführt, dass die in § 107 Abs. 3 Satz 2 AktG - das zunächst lediglich die innere Ordnung des Aufsichtsrats betrifft - genannten Bereiche als eine Konkretisierung der allgemeinen Überwachungsaufgabe des Aufsichtsrats aus § 111 Abs. 1 AktG anzusehen sind. Die Vorschriften des § 111 AktG finden jedoch nicht nur auf die Aktiengesellschaft und die Kommanditgesellschaft auf Aktien (KGaA) (§ 278 Abs. 3 AktG), sondern nach § 25 Abs. 1 Satz 1 Nr. 2 MitbestG, § 3 Abs. 2 MontanMitbestG, § 3 Abs. 1 MitbestErgG, § 1 Abs. 1 Nr. 3 DrittelbG, § 24 Abs. 2 Satz 2 MgVG auch auf die mitbestimmte GmbH Anwendung. Auf die mitbestimmungsfreie GmbH findet § 111 AktG nach § 52 Abs. 1 GmbHG nur insoweit Anwendung, als im Gesellschaftsvertrag nicht etwas anderes bestimmt ist.

Daher ist schon lange klar, dass die entsprechenden Systeme bei den obigen Gesellschaftsformen vorhanden sein müssen und die Einrichtung, Ausgestaltung und Überwachung der Systeme eine im Organisationsermessen des Vorstands stehende unternehmerische Entscheidung darstellt. Die konkrete Ausgestaltung ist hierbei insb. von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens abhängig. Der Sorgfaltsmaßstab wird durch § 93 Abs. 1 Satz 2 AktG konkretisiert, wonach eine Pflichtverletzung nicht vorliegt, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln. Aufgrund der Gesetzesbegründung zu § 93 I AktG wird diskutiert, ob die Grundsätze zum IKS auf die GmbH nach § 43 I GmbHG ebenfalls anzuwenden sind. Diese Diskussion muss m. E. erneut geführt werden, jedoch unter der im Urteil des OLG Nürnberg[78] aufgestellten Rechtsanwendung.

Die Rechtsentwicklung neuer Verabschiedeter Gesetze sowie die Entwicklung in der Rechtsprechung zeigt, dass faktisch alle kleinen und mittelständischen Unternehmen ein ihrer Komplexität und Gefahrenlage entsprechendes IKS einzuführen haben. Das Gericht spricht hier vom VIER-AUGEN-PRINZIP. Mit Blick auf die Sicherung der Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung ist das interne Kontrollsystem insbesondere auf die Erfassung von Geschäftsvorfälle die in Übereinstimmung mit den gesetzlichen Vorschriften vollständig und zeitnah, mit dem richtigen Wert, in der richtigen Buchungsperiode und auf den richtigen Konten erfasst werden sollen. Die Erfassung, Verarbeitung und Dokumentation der Geschäftsvorfälle muss in Übereinstimmung mit der Satzung bzw. dem Gesellschaftsvertrag sowie den generellen und ggf.

[77] Sammlung des Bundesrechts, Bundesgesetzblatt III 4121-1
[78] Fn. 15

besonderen Regelungen der Unternehmensleitung erfolgen. Die Unterlagen der Buchführung müssen richtig und vollständig sein. Die Inventur muss ordnungsgemäß durchgeführt werden, bei festgestellten Inventurdifferenzen sind geeignete Maßnahmen einzuleiten. Ein zutreffender Ansatz und Ausweis sowie eine sachgerechte Bewertung der Vermögensgegenstände und Schulden im Abschluss müssen gegeben sein. Verlässliche und relevante Informationen sind zeitnah und vollständig bereitzustellen. Schlüsselsatz: Aufgrund der notwendigen unternehmensindividuellen Ausgestaltung des internen Kontrollsystems gibt es nicht das eine Muster, welches für alle Fälle gleichermaßen angewendet und „kopiert" werden kann. Jedoch wird sich auch der kleine und mittelständische Unternehmer den Haftungsgefahren nicht nur gegenüber dem Finanzamt aussetzen sondern auch gegen Gläubiger im Insolvenzfalle, so dass nur eine entsprechende gelegte und dokumentiertes IKS den Geschäftsführer entlastet.

2.4 Tax Compliance-Management-System (TCMS)

Das Steuerrecht stellt für Unternehmen immer ein besonders hohes Haftungsrisiko dar. Aufgrund der Änderung des AEAO durch das BMF-Schreiben vom 23.5.2016[79] haben sich aber nunmehr Möglichkeiten aufgetan, um die Haftung zu reduzieren: Die Einrichtung eines innerbetrieblichen Kontrollsystems kann den Vorsatz- bzw. Leichtfertigkeitsvorwurf entkräften. Das Institut der Wirtschaftsprüfer hat hierzu den Praxishinweis IDW 1/2016 veröffentlicht und damit auf privater Basis eine Lücke geschlossen, da der Gesetzgeber bislang keine konkreten Vorgaben entwickelt hat.

Dieser Praxishinweis beschreibe konkret, welche Elemente ein Tax Compliance Management System enthalten muss. Ebenso wie im allgemeinen CMS sind sieben Elemente, wie z. B. die Vorgabe einer Compliance-Kultur und die Ausgestaltung von Compliance-Zielen, etc. einzuhalten. Tax Compliance und Tax-Risk Management sind zunächst inhaltlich voneinander abzugrenzen. Während das Tax-Risk Management Steuerrisiken evaluieren, aufdecken und vermeiden soll,[80] hat Tax Compliance u. a. die Befolgung der für das Unternehmen relevanten Rechtsnormen zum Inhalt. Tax-Risk Management beinhaltet nicht eine Entscheidung für gesetzestreues Handeln. Da Tax Compliance jedoch auch eine präventive Haftungsvermeidung inhärent ist, wird Tax-Risk Management in einem Tax Compliance-System eingebettet, zu einem

[79] Az: IV A 3 - S 0324/15/10001

[80] Vgl. Loose, T.: Tax Management der kapitalmarktorientierten internationalen Unternehmung 2009, S. 205 ff.; Risse, R.: Steuercontrolling- und Reporting 2009, S. 93 ff.

zentralen Bestandteil. Tax Compliance im hier dargestellten Sinn beinhaltet mithin ein funktionsfähiges Tax-Risk Management.[81]

2.4.1 Warum ein TCMS?

Gesetzlich sind Unternehmen nicht zur Einrichtung eines bestimmten innerbetrieblichen Kontrollsystems zur Erfüllung ihrer Steuerpflichten verpflichtet. Die Einrichtung solcher Systeme hat allerdings nicht nur im Besteuerungsverfahren, sondern auch für ein mögliches Steuerstrafverfahren Relevanz. Verwaltungsseitig hat das BMF aktuell im AEAO zu § 253 AO den Grundstein für die Einführung von TCMS gelegt. Bei Fehleranzeige nach § 253 AO kann ein solches System zumindest Indiz gegen bedingten Vorsatz – und damit gegen eine vermeintliche Selbstanzeige sein. Eine veränderte Rechtsprechung des Bundesfinanzhofs[82] führt dazu, dass ein neues Problem auftritt, weißt man nicht die Gewissenhaftigkeit nach, kann es im Rahmen einer Betriebsprüfung zu einem bösen Erwachen kommen.

Durch die Digitalisierung sowie dem zunehmenden Einsatz von Programmen, Tools und generell IT stehen Unternehmen ständig vor neuen Herausforderungen. Zu den Anforderungen, die sich aus der Abgabenordnung und den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form (GoBD) ergeben, kommen künftig auch noch die Verfahrensdokumentation und die Tax Compliance hinzu, was die Unternehmen im Mittelstand in der Regel absolut überfordert.

2.4.2 Verfahrensdokumentation als Teil des TCMS

Die Verfahrensdokumentation ist ein Teil bzw. kann als Grundlage zur Einrichtung nicht nur eines TCMS genutzt werden. Die wesentlichen Bestandteile einer Verfahrensdokumentation werden für ein übergeordnetes CMS, wie auch für ein RMS als auch für ein IKS benötigt. Auch wenn davon abzuraten ist, eine Musterverfahrensdokumentation einfach zu übernehmen, stellt dies ein gutes Gerüst dar, mit der Dokumentation zu beginnen. Möchte das Unternehmen die Buchhaltung digitalisieren und die Bücher und die sonst erforderlichen Aufzeichnungen elektronisch führen, so sind auch auf die damit in Zusammenhang stehenden Verfahren und Bereiche des DV-Systems zu erfassen. Das Unternehmen kommt nicht darum herum, die Organisationsstruktur und letztlich den Weg des Originalbelegs zu beschreiben und muss für jedes DV-

[81] Vgl. Besch, Ch. / Starck, A.: Tax Compliance, in: Hauschka, C. E. (Hrsg.): Corporate Compliance, 2. Aufl. 2010, § 34, Tz. 9.
[82] BFH vom 04.12.2012 - VIII R 50/10

System eine übersichtlich gegliederte Verfahrensdokumentation vorhalten. Sie umfasst den Inhalt, Aufbau, Ablauf und die Ergebnisse des DV-Verfahrens vollständig und schlüssig. Auch hier bestimmt die Komplexität und Größe den Umfang der im Einzelfall erforderlichen Dokumentation. Ohne Verständnis für das DV-Verfahren, die Bücher und Aufzeichnungen sowie die aufzubewahrenden Unterlagen, kann die Verfahrensdokumentation nicht betrieben werden. Die Verfahrensdokumentation muss verständlich und damit für einen sachverständigen Dritten in angemessener Zeit nachprüfbar sein.

Auch bei der Verfahrensdokumentation sind die organisatorisch und technisch gewollten Prozesse zu beschreiben. Der Weg des Belegs ist z. B. bei elektronischen Dokumenten von der Entstehung der Informationen über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion zu beschreiben.

Bei einer Verfahrensdokumentation ist folgendes zu beachten:

1. allgemeine Beschreibung einer Anwenderdokumentation,
2. eine technische Systemdokumentation und eine Betriebsdokumentation.
3. für den Zeitraum der Aufbewahrungsfrist muss gewährleistet und nachgewiesen sein, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten Verfahren voll entspricht. Dies gilt insbesondere für die eingesetzten Versionen der Programme (Programmidentität).
4. bei Änderungen der Programme oder wesentlichen Updates ist eine neue Verfahrensdokumentation zu erstellen und die alte Verfahrensdokumentation ist weiterhin zu archivieren. Es ist eine nachvollziehbare Änderungshistorie vorzuhalten.
5. eine Beschreibung, wie die Ordnungsvorschriften (z. B. §§ 145 ff. AO, §§ 238 ff. HGB) eingehalten werden und damit die in dem BMF-Schreiben[83] enthaltenen Anforderungen beachtet werden.
6. Die Aufbewahrungsfrist für die Verfahrensdokumentation läuft nicht ab, soweit und solange die Aufbewahrungsfrist für die Unterlagen noch nicht abgelaufen ist, zu deren Verständnis sie erforderlich ist.

Eine fehlende oder ungenügende Verfahrensdokumentation hat keine negativen Folgen, wie bspw. die Verwerfung der Buchhaltung soweit Nachvollziehbarkeit und Nachprüfbarkeit nicht beeinträchtigt werden. Ein Vorteil bietet die

[83] IV A 4-S 0316/13/10003, 2014/0353090

Verfahrensdokumentation jedoch, da Papierbelege vernichtet werden können, wenn sie entsprechend vorhanden ist.

2.4.3 Rechtsgrundlagen und Rechtsfolgen

Eine Verpflichtung zur Erstellung einer Verfahrensdokumentation ist seit 2015 verpflichtend, wenn elektronische Bücher geführt werden und die Belege elektronisch verarbeitet werden. Ein Vorteil bietet sie gerade für kleine und mittelständische Unternehmen, da sie leicht mit Elementen aus CMS und RMS ergänzt werden kann und damit die durch die Rechtsprechung geforderte Dokumentation der Überwachungssysteme nachgewiesen werden können. Die Errichtung der Verfahrensdokumentation zusammen mit einem TCMS kann der Einstieg in eine doch für die meisten Mittelständler ungewohnte Dokumentation der Prozesse sein. Die Einführung solcher Systeme im Steuerrecht bedeutet auch nicht, dass das Unternehmen sich als verlängerter Arm der Finanzverwaltung sehen sollte. „Compliant“ sein sollte so verstanden werden, dass Geschäftsvorfälle und Sachverhalte auf die steueroptimale Lösung untersucht werden ohne Gesetzesverstöße zu begehen. Tax Compliance hat das legitime Ziel, die Steuerbelastung zu reduzieren und dabei die gesetzlichen Anforderungen zu berücksichtigen und pflichtwidriges Verhalten zu vermeiden - insbesondere als Abgrenzung zu missbräuchlichen Gestaltungen iSd. § 42 AO[84]. Die Finanzverwaltung äußert regelmäßig in Erlassen ihre Rechtsauffassung, es ist legitim, eine andere Auffassung zu vertreten, sofern dies offengelegt wird[85].
Tax Compliance gewinnt zunehmend an Bedeutung, da mit dem BMF-Schreiben vom 23.5.2016 der AEAO zu § 153 AO dahin gehend geändert wurde, dass ein implementiertes und gelebtes steuerliches internes Kontrollsystem ein Indiz sein kann, dass im Zusammenhang mit einer Pflichtverletzung weder vorsätzlich noch fahrlässig gehandelt wurde.[86] Anderseits kann ein gelebtes TCMS auch im Rahmen der Aufsichtspflichten des OWiG eine Belegfunktion für eine Exkulpation der Leitungsorgane darstellen.

3. Praktisches Beispiel GWG

Durch das Maßnahmepaket der EU-Kommission zur Bekämpfung der Geldwäsche vom Juli 2019.[87] wurde das Geldwäschegesetzes (GwG) zum

[84] Vgl. Geuenich/Kiesel, BB 2012, 155 ff.
[85] Vgl. Beyer, NWB 2016, 3854 ff.
[86] BMF v. 23.05.2016 - IV A 3 - S 0324/15/10001
[87] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52019DC0360&from=EN.

01.01.2020 und der Verschärfung der strafrechtlichen Bekämpfung der Geldwäsche, welche am 18.03.2021 in Kraft getreten ist.[88], geändert.
Mit dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) sollen Geldwäsche und Terrorismusfinanzierung verhindert werden. Hierzu werden für bestimmte Verpflichtete zu beachtende Sicherungsmaßnahmen und Sorgfaltspflichten vorgeschrieben.

3.1 Besondere Sorgfaltspflichten für ein Pfandleihhaus?

Da ein Pfandleihhaus aufgrund der Eigenart des Geschäfts mit hohen Bargeldzahlungen und Vermögenswerten zu tun hat, ist dieses ein Verpflichteter i. S. d. § 2 GWG. Doch muss es nicht nur die Aufzeichnungspflichten nach § 3 PfandIV und die Schwellenwerten nach § 4 GWG beachten, sondern auch die Auszeichnungspflichten nach § 239 HGB und die nach §§ 143 ff. AO. Die Überwachungspflichten nach dem GWG wurden herabgesetzt und dabei auf die Schwelle für anonyme Bargeldzahlungen, z.B. beim Kauf von Goldmünzen und Goldbarren, Kunstwerken und Antiquitäten auf 10.000 Euro (früher 15.000 Euro) reduziert. Diese Grenze kennt das Steuerrecht in der Ausgestaltung des § 143 AO nicht. Das Steuerrecht erlaubt lediglich für Bargeschäfte bis zu 250 Euro mit vielen verschiedenen Kunden, dass die Verpflichtung, jeder einzelnen Transaktion unter Angabe von Namen und Anschrift des Kunden aufzuzeichnen, unterbleiben kann. Daher braucht diese Verpflichtung bei Massentransaktionen nicht erfüllt werden, wenn sie nachweislich Waren von geringem Wert an eine unbestimmte Vielzahl nicht bekannter und auch nicht feststellbarer Personen verkaufen. Dies ist jedoch in der Regel bei Pfandleihhäusern nicht der Fall. In der Regel kaufen und verkaufen Pfandleihhäuser Goldmünzen, Silbermünzen, Schmuck und Antiquitäten oder beleihen diese bis zur Verwertung. Würde also nur auf die Einhaltung des GWGs geachtet werden, so würden andere geltende Rechtsvorschriften verletzt werden. Wird die vom Steuergesetzgeber nach § 143 AO erforderliche Aufzeichnungspflicht nicht erfüllt, kann dies schwerwiegende Konsequenzen nach sich ziehen, denn in § 160 AO ist geregelt, dass die Finanzverwaltung Betriebsausgaben nicht anerkennen braucht, wenn der Empfänger der Gegenleistung nicht benannt wird.

3.2 Auswirkungen auf ein Compliance-Management-System

Anhand des Beispielfalles eine Pfandleihhauses soll dargestellt werden, wie ein Compliance-Management-System aufgebaut werden sollte.

[88] BGBl. I 2021, S. 327.

3.2.1 Grundelemente des CMS am Beispiel

Zunächst müssen die Grundelemente eines CMS definiert werden. Bei dem Prozess für die Einrichtung des CMS speziell für steuerrechtliche Anforderungen und den Anforderungen des Geldwäschegesetzes ist der Referenzrahmen das Gesetz, also die Abgabenordnung und das GWG. Natürlich soll hier nicht das Gesetz abgeschrieben werden, jedoch muss bei der Formulierung der CMS-Grundsätze konkrete inhaltliche Anforderungen an das System definiert und bei der Einrichtung des Systems zugrunde gelegt werden. Der Mitarbeiter muss wissen, was von ihm verlangt wird. Aus der praktischen Erfahrung fällt es Mitarbeitern leichter, sich an Anforderungen zu halten, wenn sie wissen, warum eine bestimmte Vorgehensweise von ihnen verlangt wird.

Zu den Pflichten eines gewerblichen Unternehmers gehören Aufzeichnungen nach § 3 PfandIV, § 143 AO und ggf. nach § 17 I GWG.

Diese Aufzeichnungspflichten weichen jedoch stark und in wesentlichen Punkten voneinander ab. Während das Steuerrecht als Ziel hat, die Besteuerung sicherzustellen und durch geeignete Kontrollen alle Steuerpflichtigen gleichermaßen der Besteuerung zu unterwerfen, haben die Schwellenwerte im GWG das Ziel, bestimmte Verpflichtete dazu zu veranlassen, dass zur Verhinderung von Geldwäsche und von Terrorismusfinanzierung ein wirksames Risikomanagement eingerichtet wird.

3.2.2 Risikomanagement als Teil des CMS

Das Risikomanagement muss, im Hinblick auf Art und Umfang der Geschäftstätigkeit angemessen sein. Dieses Risikomanagement umfasst gemäß § 4 Abs. 2 GwG eine Risikoanalyse (§ 5 GwG) sowie interne Sicherungsmaßnahmen (§ 6 GwG).

Die nach § 5 Abs. 1 GwG durchzuführende Risikoanalyse verlangt von den verpflichteten Unternehmen insb. eine Ermittlung und Bewertung derjenigen Risiken der Geldwäsche und der Terrorismusfinanzierung, die für die von ihnen betriebenen Geschäfte bestehen.

Das Beispiel zeigt auf, dass die Aufzeichnungspflichten in unterschiedlicher Tiefe und Ausführlichkeit geführt werden müssen. Dabei macht es Sinn, im CMS alle notwendigen Aufzeichnungspflichten aufzunehmen, damit alle Regelungen eingehalten werden.

Bei der Ausgestaltung des CMS entscheiden die gesetzlichen Vertreter, also der Unternehmensleiter, welche CMS-Grundsätze angewendet werden sollen. Für nach dem GwG Verpflichtete ist die Beachtung des GwG vorgeschrieben. Er muss jedoch das „Rad“ nicht neu erfinden, er kann auch allgemein anerkannte

Rahmenkonzepte, andere geeignete Rahmenkonzepte oder individuell entwickelte geeignete Geldwäsche-CMS-Grundsätze auf sein Unternehmen übertragen und entsprechend anpassen. Bei der individuellen Entwicklung von Geldwäsche-CMS-Grundsätzen können die gesetzlichen Vertreter auch entscheiden, sich an verfügbaren Informationen über die Praxis anderer Unternehmen zu orientieren. Sofern das angewandte Rahmenkonzept nicht alle CMS-Grundelemente abdeckt, bietet sich eine Ergänzung durch andere Grundsätze an, die individuell entwickelt, im Rahmen von Vergleichen mit der Praxis anderer Unternehmen festgestellt oder einem anderen Rahmenkonzept entnommen werden können. Bei der Entwicklung von individuellen Geldwäsche-CMS-Grundsätzen kann sich das Unternehmen zudem an den nachfolgend beschriebenen Grundelementen eines Geldwäsche-CMS orientieren.

3.3 Analyse der wirksamen Maßnahmen

Die Unternehmensleitung muss analysieren, welche wirksamen Maßnahmen ergriffen werden müssen, damit sie der individuellen Risikoexposition des Unternehmens gerecht wird. Oft wird in der Praxis ohne Sinn und Verstand ein Muster abgetippt und in die Schublade gelegt. Es wird versäumt, sich mit den Eigenarten des Geschäfts und mit dem für das Unternehmen vorhandene Risiko auseinanderzusetzen. § 4 Abs. 1 GWG verlangt ein wirksames Risikomanagement, welches auf Art und Umfang der Geschäftstätigkeit angemessen sein muss. Es ist Sache des Unternehmens jedoch nicht nur die Risiken, die aufgrund des GWG entstehen, zu analysieren und zu regeln, die Unternehmensleitung kann auch ihre eigenen wirtschaftlichen Risiken definieren und damit minimieren.

Nach § 6 Abs. 1 GwG sind angemessene geschäfts- und kundenbezogene interne Sicherungsmaßnahmen einzurichten, um die Risiken von Geldwäsche und von Terrorismusfinanzierung in Form von Grundsätzen, Verfahren und Kontrollen zu steuern und zu mindern.

Hierzu gehören insb.:

1. Grundsätze, Verfahren und Kontrollen in Bezug auf
2. den Umgang mit den im Rahmen der Risikoanalyse identifizierten Risiken (§ 6 Abs. 2 Nr. 1 a) GwG),
3. die Kundensorgfaltspflichten nach den §§ 10 bis 17 GwG, (§ 6 Abs. 2 Nr. 1 b) GwG),
4. die Erfüllung der Meldepflicht nach § 43 Abs. 1 GwG, (§ 6 Abs. 2 Nr. 1 c) GwG),
5. die Aufzeichnung von Informationen und die Aufbewahrung von Dokumenten nach § 8 GwG (§ 6 Abs. 2 Nr. 1 d) GwG),

6. die Einhaltung der sonstigen geldwäscherechtlichen Vorschriften (§ 6 Abs. 2 Nr. 1 e) GwG),
7. die Verhinderung des Missbrauchs von neuen Produkten und Technologien zur Geldwäsche oder zur Begünstigung der Anonymität von Geschäftsbeziehungen (§ 6 Abs. 2 Nr. 4 GwG)
8. die Einrichtung geeigneter Maßnahmen zur Prüfung der Zuverlässigkeit der Beschäftigten (§ 6 Abs. 2 Nr. 5 GwG)
9. die Implementierung von Verfahren und Informationen zur Unterrichtung der Beschäftigten über Typologien und aktuelle Methoden der Geldwäsche sowie die bestehende Pflichtenlage (§ 6 Abs. 2 Nr. 6 GwG)
10. die Einrichtung eines Hinweisgebersystems für Mitarbeiter und ähnliche Personen unter Wahrung der Vertraulichkeit ihrer Identität zur Meldung von geldwäscherechtlichen Verstößen (§ 6 Abs. 5 GwG)
11. ggf. die Bestellung eines Geldwäschebeauftragten und seines Stellvertreters (§ 6 Abs. 2 Nr. 2, § 7 GwG).

3.4 Compliance-Kultur

Die Geldwäsche-Compliance-Kultur ist ein Teil der allgemeinen Compliance-Kultur eines Unternehmens. Das Aufsetzen und Vorleben einer angemessenen Compliance-Kultur unterstützt die Unternehmensleiter, das Vertrauen in die eigene Organisation nachhaltig zu stärken. Sie bildet die Grundlage für ein angemessenes und wirksames CMS und wird insb. geprägt durch die Grundeinstellungen und Verhaltensweisen der Mitarbeiter und die Rolle der für die Überwachung Verantwortlichen sowie die Art und Weise, wie die Geschäftsleitung die zentralen Unternehmenswerte und die weiteren Grundelemente in der Organisation verankern. Ausprägungen der Compliance-Kultur eines Unternehmens lassen sich z.B. an der Art und Weise der Hervorhebung der Bedeutung der Geldwäsche-Prävention im Unternehmen sowie der regelmäßigen Kommunikation von Geldwäsche-Themen auf Ebene der Unternehmensleitung (tone at the top) und durch die Unternehmensleitung in das Unternehmen hinein (tone from the top) erkennen.

Ohne eine fest verankerte Compliance Kultur greifen viele Sicherungsmaßnahmen z.B. zur Geldwäschebekämpfung oder zur präventiven Aufzeichnung für eine Betriebsprüfung der Finanzverwaltung ins Leere. Das Vorbild der Unternehmensleitung und der Führungskräfte trägt dazu bei, dass die Mitarbeiter des Unternehmens der Beachtung von Regeln zur Verhinderung von Geldwäsche und Terrorismusfinanzierung die notwendige Bedeutung beimessen und zu deren Bereitschaft zu regelkonformem Verhalten. In einer günstigen Compliance-Kultur bringt die Unternehmensleitung schlüssig und glaubhaft

gegenüber den handelnden Personen innerhalb und außerhalb des Unternehmens zum Ausdruck, dass die Verhinderung von Geldwäsche und Terrorismusfinanzierung eine hohe Bedeutung hat und aufgedeckte Regelverstöße ohne Ansehen der Person und von Hierarchien angemessene Sanktionen nach sich ziehen.
Die Grundeinstellungen und erwarteten Verhaltensweisen können z.B. im Rahmen eines Leitbilds oder eines Verhaltenskodexes kommuniziert und dokumentiert werden.

3.5 Praktische Probleme des GWG

Weiterhin muss ggf. ein Geldwäschebeauftragter bestellt werden. Dies ist der Fall, wenn über 50% des Gesamtumsatzes im vorherigen Wirtschaftsjahr, insgesamt mit mindestens zehn Mitarbeiterinnen oder Mitarbeiter in den Bereichen Akquise, Kasse, Kundenbuchhaltung, Verkauf und Vertrieb einschließlich Leitungspersonal (insbesondere Geschäftsführung) beschäftigt waren und nach § 4 Absatz 4 GwG die Verpflichtung besteht, über ein wirksames Risikomanagement zu verfügen, dies ist z.B. bereits bei Bargeldannahme von 10.000 € und mehr der Fall.
Dem mittelständischen Unternehmer ist oft nicht bewusst, welche Aufzeichnungs- und Dokumentationspflichten er einhalten muss. Er kennt seine Kunden schon seit Jahrzehnten. Der Kunde zahlt immer bar, mal unter 10.000 Euro mal über 10.000 Euro. Er kommt gar nicht auf die Idee, dass er auf einmal eine erhöhte Dokumentationspflicht hat und sich auch von langjährigen Kunden den Personalausweis zeigen lassen muss. Meist reduziert sich die Dokumentation auf das Ausfüllen des Formulars[89] und der Anlage zu Dokumentationsbogen zur Durchführung verstärkter Sorgfaltspflichten nach § 15 GWG für Verpflichtete aus dem Nichtfinanzsektor. In Ausnahmefällen kann sogar die Bestellung des Geldwäschebeauftragten für einen der o.g. Güterhändler oder wie hier für das Pfandleihhaus auch entfallen, wenn der Behörde nachgewiesen werden kann, dass kein Geldwäscherisiko besteht. Dennoch sind geeignete Maßnahmen zunächst zu treffen, um das Risiko zu identifizieren, und im Nachgang die Bewertung des Risikos vornehmen zu können.

3.6 Formulierungen von CMS-Zielen

Die Einhaltung der geldwäscherechtlichen Vorschriften stellt eine gesetzliche Anforderung dar, die bei der Erreichung der Unternehmensziele zu beachten ist.

[89]https://rp.baden-wuerttemberg.de/fileadmin/RP-Internet/Themenportal/Sicherheit/_DocumentLibraries/Documents/Geldwaesche/Allgemeingueltige_Informationen_und_Formulare/Geldwaesche_Checkliste_verst_SP.pdf

Für die Festlegung der Geldwäsche-Compliance-Ziele bietet es sich an, eine erste Risikoanalyse auf Gesamtunternehmensebene durchzuführen, um ggf. Bereiche zu identifizieren, für die aufgrund von Risikoabwägungen die Einrichtung besonderer Geldwäsche-Regelungen erforderlich erscheint, z.B. wenn aufgrund des Vorliegens besonderer Risikofaktoren die verstärkten Sorgfaltspflichten nach § 15 GwG zu erfüllen sind.

Faktoren, die bei der Festlegung der Compliance-Ziele eine Rolle spielen können, sind z.B.

1. besondere Risiken, basierend auf den aus der Geschäftsstrategie des Unternehmens folgenden Produkten bzw. Dienstleistungen, Kunden, Prozessen, Transaktionen und Regionen,
2. Erkenntnisse über Geldwäscheverstöße aus der Vergangenheit,
3. die Abwägung, ob ein Verstoß gegen geldwäscherechtliche Vorschriften zu einer operativen Beeinträchtigung der Geschäftstätigkeit führen kann (z.B. hinsichtlich zu erwartender Kontrollen durch Behörden oder zu erwartenden Sanktionen),
4. das Risiko von Reputationsschäden durch das öffentliche Bekanntwerden von Verstößen gegen geldwäscherechtliche Vorschriften,
5. das gewünschte bzw. geforderte Sicherungsniveau im Unternehmen (Erfüllung der gesetzlichen Vorgaben oder Best-in-Class, allgemeine, verstärkte oder vereinfachte Sorgfaltspflichten nach dem GwG) oder
6. finanzielle Schäden (insb. Geldstrafen) durch Regelverstöße.

Bei der Festlegung der Geldwäsche-Compliance-Ziele sind ferner die folgenden Aspekte von Bedeutung:

1. Konsistenz der unterschiedlichen Ziele
2. Verständlichkeit und Praktikabilität der Ziele
3. Messbarkeit des Grades der Zielerreichung
4. Abstimmung mit den verfügbaren Ressourcen.

Die festgelegten Geldwäsche-Compliance-Ziele sind die Grundlage für die weitergehende systematische Aufnahme und Beurteilung der Risiken für Regelverstöße. Aus dieser regelmäßigen Befassung mit den Compliance-Risiken können sich im Zeitablauf auch Rückwirkungen auf die Festlegung der Geldwäsche-Compliance-Ziele ergeben.

Die Geldwäsche-Compliance-Ziele bilden den Rahmen und die Aufgaben für die Steuerungsfunktion des Geldwäschebeauftragten.

Geldwäsche-Compliance-Ziele können z.B. in einer Richtlinie, in einem Verhaltenskodex oder in ähnlicher Form dokumentiert werden.

Unter Berücksichtigung der Geldwäsche-Compliance-Ziele werden Geldwäsche-Compliance-Risiken, d.h. Risiken für Verstöße gegen einzuhaltende Regeln zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, identifiziert. Das Ziel der nach dem GwG durchzuführenden Risikoanalyse ist es, die spezifischen Risiken in Bezug auf Geldwäsche und Terrorismusfinanzierung im Geschäftsbetrieb des Verpflichteten umfassend und vollständig zu erfassen.[90] Hierzu wird entsprechend eine der Unternehmensorganisation angemessene systematische Risikoidentifikation und -bewertung durchgeführt. Es bietet sich an, eine Risiko-Kontroll-Matrix zu erstellen, mittels derer den Risiken entsprechende Maßnahmen des Compliance-Programms gegenübergestellt werden.

Die Risikomatrix nach Nohl

Eintritts-wahrscheinlichkeit	Schadensausmaß			
	ohne Arbeitsausfall (keine Rechtsfolgen)	leicht, Erste Hilfe (Rechtsfolgen möglich)	schwer, reversibel (Rechtsfolgen wahrscheinlich)	sehr schwer, Tod (dramatische Rechtsfolge)
sehr wahrscheinlich, oft	4	5	6	7
wahrscheinlich, gelegentlich	3	4	5	6
möglich, selten	2	3	4	5
praktisch unmöglich	1	2	3	4

Abb. 4 [91]

§ 5 GwG sieht vor, dass die Verpflichteten diejenigen Geldwäsche-Risiken zu ermitteln und zu bewerten haben, die für Geschäfte bestehen, die von ihnen betrieben werden. Hierbei haben sie insb. die in den Anlagen 1 und 2 des GwG genannten Risikofaktoren sowie die Informationen zu berücksichtigen, die auf Grundlage der nationalen Risikoanalyse[92] zur Verfügung gestellt werden. Darüber hinaus können auch weitere Informationsquellen relevant sein, etwa (Jahres-)Berichte, Typologiepapiere oder sonstige Veröffentlichungen der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) des Bundeskriminalamts bzw. der Landeskriminalämter sowie der Financial Action Task Force (FATF) (und ggf. weiterer internationaler Organisationen). Die Verpflichteten sollten darüber hinaus risikobasiert entscheiden, inwieweit die Informationen aus der supranationalen Risikoanalyse der EU-Kommission relevant sind.[93]

---

[90] BT-Drs. 18/11555, S. 110.
[91] https://www.domeba.de/wp-content/uploads/2021/06/schaubild_risikomatrix.png
[92] Vgl. § 5 Abs. 1 Satz 2 GwG. Die erste nationale Risikoanalyse wurde im Oktober 2019 veröffentlicht und steht auf der Internetseite des BMF als Download zur Verfügung (Service>Publikationen>Broschüren/Bestellservice).
[93] Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der mit grenzüberschreitenden Tätigkeiten im Zusammenhang stehenden
Risiken der Geldwäsche und der Terrorismusfinanzierung für den Binnenmarkt

Der Umfang der vom Verpflichteten zu erstellenden Risikoanalyse richtet sich nach der Art und dem Umfang der Geschäftstätigkeit des Unternehmens (§ 5 Abs. 1 Satz 3 GwG). Anhaltspunkte für eine Risikoeinstufung können u.a. sein:

1. Art und Dauer der Dienstleistung oder Geschäftsbeziehung
2. Bestehen von ersten Verdachtsmomenten hinsichtlich Geldwäsche
3. Risikofaktoren gemäß Anlagen 1 und 2 zum GwG: Kundenrisiko; Produkt-Dienstleistungs-, Transaktions- oder Vertriebskanalrisiko; geografisches Risiko
4. Informationen, die auf Grundlage der nationalen Risikoanalyse zur Verfügung gestellt werden
5. Politisch exponierte Personen (PeP) als Vertragspartner oder wirtschaftlich Berechtigte
6. Informationen, die von der FIU im Rahmen ihrer Zuständigkeit nach § 28 Abs. 1 Satz 2 Nr. 8 GwG (Durchführung von strategischen Analysen) bereitgestellt werden.

Im Rahmen der Analyse des Risikos der Geschäftsfelder und Prozesse wird insb. analysiert, wie hoch das jeweilige Risiko der jeweiligen Tätigkeit ist, z.B. stellt die Annahme, Weiterleitung oder Verwaltung von Barmitteln und gleichgestellten Zahlungsmitteln grundsätzlich ein höheres Risiko dar.

Auf Grundlage der durchgeführten Analyse des Geschäftsrisikos können die identifizierten Risiken bewertet und kategorisiert werden. Anhand der bewerteten Einzelfälle kann eine Gesamtschau für das Unternehmen erstellt werden. Dabei können folgende drei Risikokategorien angenommen werden:

1. Geringeres Risiko: Dem Risiko der Geldwäsche kann bereits durch vereinfachte Sorgfaltspflichten begegnet werden (§ 14 GwG).
2. Mittleres Risiko: Dem Risiko der Geldwäsche kann noch durch allgemeine Sorgfaltspflichten begegnet werden (§ 10 GwG).
3. Höheres Risiko: Dem Risiko der Geldwäsche kann nur durch Einhaltung der verstärkten Sorgfaltspflichten begegnet werden (§ 15 GwG).

Gemäß § 9 Abs. 1 Satz 1 GwG haben Verpflichtete, die Mutterunternehmen einer Gruppe sind, eine Risikoanalyse für alle Zweigstellen, Zweigniederlassungen und gruppenangehörigen Unternehmen im In- oder Ausland durchzuführen, die dem Mutterunternehmen nachgeordnet sind und die an ihren Standorten ebenfalls geldwäscherechtlichen Vorschriften unterliegen.

Die Risikoanalyse ist zu dokumentieren und regelmäßig (mindestens einmal im Jahr) zu überprüfen und soweit erforderlich zu aktualisieren (§ 5 Abs. 2 Nr. 1 und

---

(nachfolgend auch bezeichnet als “Supranationale Risikoanalyse”), https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2017:340:FIN.

2 GwG). Sie ist der jeweils zuständigen Aufsichtsbehörde auf Verlangen zur Verfügung zu stellen (§ 5 Abs. 2 Nr. 3 GwG).

4. Übertragbarkeit auf den Mittelstand

Es wird häufig die Auffassung vertreten, dass der Mittelstand mit der Flut von immerwährenden Gesetzesänderungen überfordert sei. Es ist zwar richtig, dass durch die Internationalisierung der Richtlinien und Verordnungen in der EU zusätzlich zu den nationalen Gesetzen ein Urwald von Vorschriften entsteht, die kaum noch zu überblicken sind. Dennoch ist dem entgegenzuhalten, dass gerade dieses Problem durch eine Systematisierung entgegengetreten wird. Es ist gerade sinnvoll, in den Bereichen, in dem die Unternehmen aus verschiedenen Branchen und Industrien bestehen, in ihrer Arbeit die ständigen Veränderungen berücksichtigen. Dafür ist gerade ein funktionierendes CMS da. Die Schock-Starre muss gar nicht sein. Es ist wie bei einem Kind, es lernt von Tag zu Tag. Befasse ich mich jedoch nur mit dem Zielbild, weiß man nicht, wo man bei der Einführung von CMS ansetzen muss.

Die Erwartungshaltung ist bei einigen Geschäftsführern und dessen Beratern von KMUs, dass der Gesetzgeber konkrete Handlungsempfehlungen unterlassen hat und dass sie daher die Anforderungen verdrängen.

Zudem ist im Mittelstand qualifiziertes Personal schwierig zu finden. Mängel, die zwar erkannt werden, können jedoch meist durch fehlendes bezahlbares qualifiziertes Personal nicht abgestellt werden. Kommt dann noch der Umstand hinzu, dass eine etwaige Haftung nur in der Krise entstehen kann und durch Nichtumsetzung des bspw. § 1 StaRUG weder eine Straftat noch eine Ordnungswidrigkeit begründet wird, ist der mittelständische Unternehmensleiter resigniert: Die Reaktion auf mögliche Anforderungen und Risiken ist meist: „Das ist nicht so einfach, das ist nicht so eindeutig, das machen wir dann mal, wenn wir Zeit dazu haben und bis dahin machen wir erst mal nichts."

Doch davor sei ausdrücklich gewarnt, denn diese Sorgfaltspflichtverletzung könnte den Geschäftsleiter im Krisen- bzw. Insolvenzfall sehr teuer zu stehen kommen! Eine Verletzung bspw. des § 1 Abs. 1 StaRUG könnte nach § 43 Abs. 2 GmbHG zu einer Innenhaftung für daraus entstandene Schäden führen.

4.1 CMS Pflicht oder Kür?

Verfolgt man Presseberichten der letzten zwei Jahren, so sind Firmen wie Wirecard, Grenke, Adler Immobilen ins Fadenkreuz der Untersuchungen gekommen. Verfolgt man den Fall Grenke, so fällt auf, dass im Jahr 2021 der verantwortliche Vorstand für Compliance zurücktreten musste. „Die Kritikpunkte im Bereich Compliance bezogen sich auf prozessuale Schwächen bei der

Dokumentation von Related Parties, mangelnde Nachvollziehbarkeit von Aktualisierungen des Compliance-Handbuchs, Infragestellung der Messgrößen für die Bewertung der Compliance-Risiken, unzureichende Dokumentation der schriftlichen Jahresberichte der Compliance-Funktion sowie auch hier eine nicht angemessene personelle Ausstattung der Compliance-Funktion."

Wie soll also das kleine oder mittelständische Unternehmen diese Anforderungen erfüllen, wenn es noch nicht einmal große börsennotierte Unternehmen mit den erforderlichen Ressourcen hinbekommen?

Es mag schnell der Eindruck entstehen, dass man resigniert, da es ja noch nicht mal die „Großen" richtig umsetzen können.

Auf ein Compliance Management System in einem Unternehmen und ist es noch so klein, zu verzichten, sollte schon aus zwei Gründen abgeraten werden:

1. Haftungsrisiken
2. Wettbewerbsnachteile

Die Anzeichen durch Gesetzgebung und verschärfender Rechtsprechung zeigt, dass sich kein Unternehmen mehr vor der Einrichtung funktionierender CMS, RMS und IKS versperren sollte. Zwar besteht keine explizite gesetzliche Pflicht für diese Systeme, doch wird von Unternehmen, und insbesondere von Geschäftsführern, erwartet, dass sie sämtliche für sie geltenden Vorschriften beachten und befolgen bzw. darauf achten, dass diese befolgt werden.

Geschäftsführer haben geeignete Überwachungsmaßnahmen zu ergreifen und können, bei fahrlässiger Aufsichtspflichtverletzung persönlich haftbar gemacht werden. Im Rahmen der allgemeinen Sorgfaltspflicht eines Geschäftsführers sollten Unternehmen ernsthaft abwägen, die strafrechtliche Verantwortung zu verringern, indem Maßnahmen zur Risikoprävention eingeführt werden.

Daher ergibt sich eine praktische Notwendigkeit für die Einführung eines strukturierten Systems, welches sowohl Compliance, allgemeine Risiken, bestandsgefährdende Risiken sowie die internen Kontrollen im Mittelstand dokumentiert. Ein am Markt etabliertes Unternehmen würde gar nicht funktionieren, wenn es diese Systeme in der täglichen Praxis nicht umsetzen würde. Dennoch fehlt es meist am Bewusstsein und der Dokumentation. Die Schadenshöhe für regelwidriges Verhalten ist gerade für mittelständische Unternehmen von nicht zu unterschätzender Höhe. Etwaige Strafen ergeben sich in erster Linie aus rechtlichen Folgen wirtschaftskriminellen Verhaltens und umfassen neben Freiheitsstrafen auch Ersatzansprüche und Auftragssperren.

Insbesondere bei international agierenden Unternehmen können resultierende Geldbußen von existenzbedrohender Höhe sein. Schließlich gibt es bei der erfolgreichen Durchführung einer Exportkontrolle oder einer KYC-Prüfung einige

Faktoren zu beachten, die gerade für kleinere Unternehmen nicht unmittelbar ersichtlich sein können.

Ein funktionierendes Compliance Management System und die Zertifizierung dieser sind mitunter ein wesentlicher Beweggrund für Auftraggeber, Großkunden und der öffentlichen Hand, um Aufträge zu erteilen oder verwehrt zu bekommen. Konzerne, sind durch die Änderung des § 289c HGB daran interessiert, bei ihren Geschäftsbeziehungen mit Mittelständlern darauf vermehrt zu achten, dass diese sich durchgehend gesetzeskonform verhalten und im Einklang mit den eigenen Compliance Vorgaben stehen. Vorstandsmitglieder und Geschäftsführer haften bei strafrechtlichen Verstößen und sind in der Pflicht, die Einhaltung von Compliance nachzuweisen.

Nicht zuletzt haben Compliance Verstöße gegen Kartellgesetze, Datenschutzrichtlinien und den richtigen Umgang mit Einladungen und Geschenken erhebliche Auswirkungen auf die Reputation von Unternehmen.

Meist tun sich Mittelständler auch heute noch schwer, Compliance Maßnahmen für Teilbereiche ihrer Firma einzuführen. Gerade bei der Überwachung von Ruhezeiten und Überstunden sind die Mittelständler froh, dass die Arbeit erledigt wird. Ständige Personalknappheit und krankheitsbedingte Ausfälle verleiten dazu, diese Arbeitnehmerschutzrechte nicht zu beachten. Wird dies jedoch, meist durch den Zoll festgestellt, drohen empfindliche Strafen. Die Kosten gemessen an den drohenden Strafen sind überschaubar. Eigentlich sollte jeder Mitarbeiter auch bereit sein, seinen Teil dazu beizutragen, so dass relativ schnell ein brauchbares Grundkonzept vorliegt. Die zunehmende Digitalisierung kann auch als Anlass genommen werden, auf der Grundlage der Verfahrensdokumentation zu beginnen die Ziele der CMS, RMS und IKS zu definieren und dort zu ergänzen.

Zunächst gilt es für das Unternehmen zu prüfen, welche Maßnahmen womöglich schon längst Bestandteil der Unternehmensprozesse sind und eigentlich nur dokumentiert werden müssen.

Auf der Grundlage eines modularen Vorgehens können Unternehmen gezielt einzelne Bereiche der Organisation durch Compliance Maßnahmen stärken. Bei dieser Strategie können Unternehmen je nach Risikograd ein Compliance Programm für bestimmte Abteilungen oder Bereiche erstellen, bei denen die Gefährdung am größten ist. Je nach Branche und dem Gefährdungspotenzial des Unternehmens bietet sich ein risikobasierter Ansatz an. Dort wo die Haftungsgefahr am größten ist, wird begonnen.

Die erfolgreiche Einführung eines Compliance Programms in mittelständischen Unternehmen wurde in einer Studie “Compliance im Mittelstand” von Deloitte verbildlicht.

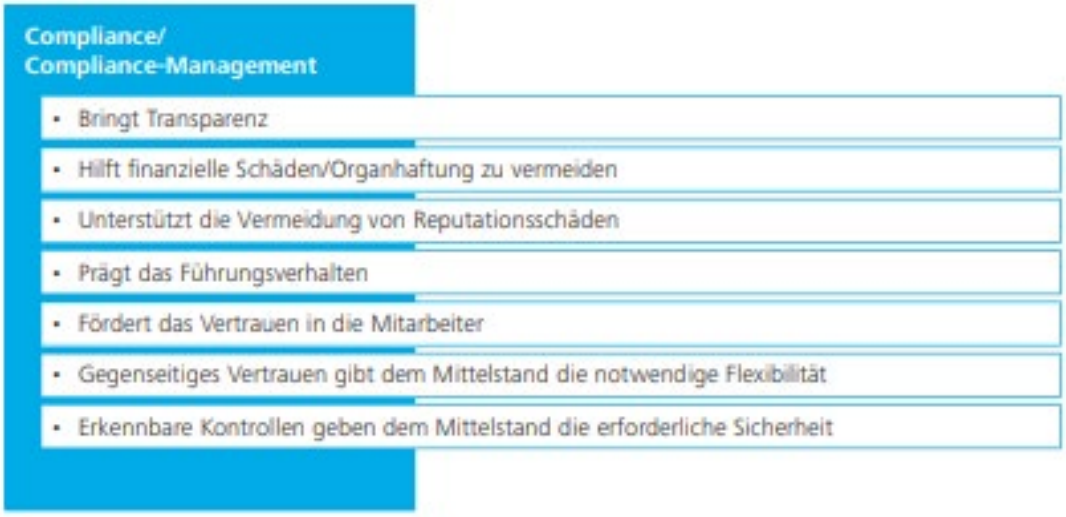

Abb.5 „Studie „Compliance im Mittelstand“[94]

5. Ausblick und Fazit

Prinzipiell ist es für mittelständische Unternehmen zu empfehlen ein CMS, RMS und IKS zu etablieren. Meist sind die Strukturen bereits vorhanden und müssen nur dokumentiert werden und ins Bewusstsein treten. Regelungen, die der Gesetzgeber getroffen hat, die den Unternehmer zwingen, geeignete Maßnahmen, wie eine integrierte Finanzplanung sowie ein Frühwarnsystem einzurichten sind notwendige und wichtige Instrumente eines erfolgreichen Unternehmens. Leider wird die Notwendigkeit meist mit dem Argument, man können doch sowieso nicht in die Zukunft sehen, begegnet. Es wird leider bei KMUs oft verkannt, dass die Regeleinheit, Befolgung von Gesetzen, der richtige Umgang mit Risiken und die internen Kontrollen weniger ein Papiertiger sein sollen als wirklich gelebte wichtige Instrumente. Es zeigt, dass die Einsicht leider erst kommt, wenn die Unternehmen bzw. die dafür Verantwortlichen mit empfindlichen Strafen belegt werden. Das OLG Nürnberg hat mit der Bezugnahme auf den § 130 OWIG als Schutznorm den Weg eröffnet, auf zivilrechtlichem Wege Haftungsansprüche nach § 823 II BGB geltend zu machen. Es darf gespannt sein, ob der BGH an seiner im Jahr 1994 vertretenen Auffassung, dass § 130 OWIG eben keine Schutznorm iSd § 823 II BGB darstellt, festhalten wird. Aufgrund der wirtschaftlichen angespannten Lage werden sicherlich in den nächsten Jahren zahlreiche Haftungsprozesse gegen

[94] Aus der Studienserie „Erfolgsfaktoren im Mittelstand” von Deloitte Compliance im Mittelstand,

Geschäftsführer geführt werden und der ein oder andere Gläubiger wird versuchen, sein Geld vielleicht über diesen Weg zu bekommen. Es ist auf jeden Fall zu empfehlen, dass sich der Mittelstand entsprechend beraten lässt und seine Haftungsrisiken durch die Einführung von CMS, RMS und IKS reduziert. Gerade durch die Verabschiedung von neueren Gesetzen ist zu erkennen, dass der Gesetzgeber Unternehmen zur Einhaltung von Regeln und dessen Überwachung stärker fordert. Immer öfter werden Formulierungen, wie ein angemessenes Risikosystem, Frühwarnsysteme, etc. in Gesetzen oder Gesetzesbegründungen aufgenommen Die Rechtsprechung des OLG Nürnberg im März dieses Jahres wird einigen Unternehmen negative Überraschungen bringen. Es ist zu erwarten, dass zunehmend ein Boom auf D&O Versicherungen entsteht, die das Risiko von Geschäftsführern reduzieren sollen. Dieser Trend wird jedoch auch bei der Rechtsprechung festzustellen sein und es wird mehr Urteile geben, die sich mit der Frage beschäftigen, ob durch die pflichtwidrige unterlassene Einrichtung von CMS, RMS und IKS die Geschäftsführer in die persönliche Haftung genommen werden. Es ist zu erwarten, dass in den kommenden Jahren diese Haftungsprozesse zunehmen werden. Allerdings auch die erneute Aussetzung der Bußgelder wegen verspäteter Offenlegung wird in den nächsten Jahren bei Insolvenzverfahren die Gerichte beschäftigen. Es ist an der Zeit auch bei kleinen und mittelständischen Unternehmen für entsprechende Dokumentation und Einführung von Überwachungsmaßnahmen zu sorgen.

Literaturverzeichnis

Acker, Wendelin	Vorstand/Geschäftsführer muss für funktionierendes Compliance-System sorgen! IBR 2014 Heft 5, 309
Beyer, Dirk	Die Grenze zur Steuerhinterziehung bei fehlerhafter Steuererklärung, NWB 2016, S. 3854 ff.
Dachner, Anja	Die Haftung eines GmbH-Geschäftsführers für „Non-Compliance“ Zugleich Besprechung von OLG Nürnberg, Endurteil vom 30.3.2022 - 12 U 1520/19, in ZWH 2022, 161-163
Dohrn, Daniel	Entscheidungsbesprechung LG München I zu den Compliance Pflichten eines Vorstands in Newsdienst Compliance 2014, 22101, beck-online
Fissenewert, Peter	Compliance in mittelständischen Unternehmen, 2. aktualisierte Auflage, E-Book, Reguvis Fachmedien GmbH Compliance für den Mittelstand, 2. Auflage 2018, C.H.Beck Verlag München
Fleicher, Holger	Aktienrechtliche Compliance Pflichten im Praxistest: Das Siemens/Neubürger Urteil des LG München I, NZG Heft 9, 2014
Flick, Martin	Jedes Vorstandsmitglied ist für die Einrichtung und Überwachung eines Compliance-Systems verantwortlich in GWR 2014, 151
Flöther, Lucas/ Goetker, Uwe	Kommentar: StaRUG - Unternehmensstabilisierungs- und restrukturierungsgesetz, 1. Auflage 2021, C.H. Beck Verlag
Geuenich, Marcus/ Kiesel, Hanno	Tax Compliance bei Unternehmen – einschlägige Risiken und Folgerungen für die Praxis, in BB 2012, 155
Graumann, Mathias	Wirtschaftliches Prüfungswesen, 5. Auflage 2017, NWB Verlag GmbH & Co. KG Angemessene Informationsgrundlage von Prognosen bei unternehmerischen Entscheidungen in ZIP 2021, 50-51
Goette, Constantin/ Barring, Philipp	Compliance-Management-Systeme und Compliance Due Diligence in DStR 2021, 1238
Hauschka, Christoph/ Moosmayer, Klaus/ Lösler, Thomas	Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Auflage 2016, C. H. Beck Verlag
Kremer, Thomas/ Bachmann, Gregor/ Lutter, Marcus/ von Werder, Axel	Kommentar zu Deutscher Corporate Governance Kodex, 8. Auflage. 2021, C. H. Beck Verlag
Kühne, Mathias/ Lienhard, Frank	Ausgestaltung eines Risikofrüherkennungssystems gemäß § 1 StaRUG und die Haftungsfolgen für die Geschäftsleitung“, SanB 2020, S. 144
Loose, Thomas	Tax Management der Kapitalmarktorientierten internationalen Unternehmung, 1. Auflage 2009, Josef Eul Verlag
Lück, Wolfgang	Der Umgang mit unternehmerischen Risiken durch ein Risikomanagementsystem und durch ein Überwachungssystem:

	Anforderungen durch das KonTraG und Umsetzung in der betrieblichen Praxis in DB 1998, 9 ff.
Nestler, Diana/ Modi, Julian	Leitfaden IT-Compliance, 1. Auflage 2019, IDW Verlag GmbH
Noack, Ulrich	Noack/Servatius/Haas, Kommentar zu GmbHG, 23. Auflage 2022, C. H. Beck Verlag
Reker, Jürgen	Compliance im Mittelstand, eine Studie von Deloitte aus dem Jahr 2011 abrufbar unter https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Mittelstand/Studie-Compliance-im-Mittelstand.pdf
Risse, Robert	Konzernsteuerquote und deren Bedeutung für das Steuermanagement, 1. Auflage 2010, GWV Fachverlag GmbH
Schieffer, Anita	in Minkoff/Sahan/Wittig, Konzernstrafrecht, 1. Auflage 2020, C. H. Beck Verlag München
Schwab, Sarah	Dissertation, Einführung und Ausgestaltung eines Compliance-Management-Systems für einen SE-Konzern mit Sitz in Deutschland, 2018
Welsch, Jens/ Foshag, Ute	Renz/Hense/Marbeiter, Wertpapier-Compliance in der Praxis, 2. Auflage 2019, Erich Schmidt Verlag
Zeitschriften	
BB	Betriebs-Berater
DB	Der Betrieb
DStR	Deutsches Steuerrecht
GWR	Gesellschafts- und Wirtschaftsrecht
IBR	Immobilien und Baurecht
NWB	NWB- Steuer und Wirtschaftsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
SanB	Sanierungsberater
ZIP	Zeitschrift für Wirtschaftsrecht
ZWH	Wirtschaftsstrafrecht und Haftung im Unternehmen
Sonstige Quellen	
Internetquellen	letzter Zugriff 04.12.2022
IDW	Institut der Wirtschaftsprüfer PS (Prüfungsstandards)
BMF-Schreiben	Schreiben des Bundesministeriums der Finanzen

Compliance-Management-Systeme; Pflicht oder Kür für den Mittelstand? – Ein Überblick aus Handels-, Steuer- und Insolvenzrecht
Erklärung über selbständige Bearbeitung

Hiermit versichere ich, Lars-Holger Tilgner, dass ich die Masterarbeit selbstständig verfasst und weder diese Arbeit noch Teile davon an anderer Stelle zu Prüfungszwecken eingereicht habe, sowie keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Mannheim, 06.12.2022, Lars Tilgner