Scherer (Autor)

GMRC
INTERNATIONAL INSTITUTE FOR
GOVERNANCE.MANAGEMENT.RISK & COMPLIANCE

Wie viel Standard braucht der Mensch?

Zum Anwendungsbereich eines Standards: Welche Standards (ISO, IDW, COSO, DIIR, etc.) sind für Ihr Unternehmen / Ihre Organisation relevant und wie sind sie angemessen anzuwenden?

Scherer:
Wie viel Standard braucht der Mensch?

Zum Anwendungsbereich eines Standards: Welche Standards (ISO, IDW, COSO, DIIR, etc.) sind für Ihr Unternehmen / Ihre Organisation relevant und wie sind sie *angemessen* anzuwenden?

Rn. 1 Summary

Summary

1. Für ein (Compliance-) Risiko-Managementsystem und viele weitere Systeme (QM, IKS, Revision, Nachhaltigkeit (Corporate social responsibility), Informationssicherheit, etc. etc.) gibt es eine Vielzahl von Standards, die u.a. für die Ausgestaltung des Managementsystems und für Audit-Zertifizierung als Referenzgröße dienen können.

2. Die Beantwortung der Frage, welcher Standard für welches Unternehmen / welche Organisation der passende ist, sollte nicht dem Bauchgefühl überlassen werden, sondern stellt eine unternehmerische Entscheidung (Business Judgment Rule) (§ 93 Abs. 1 AktG) im Zusammenhang mit der Einrichtung, Ausgestaltung und Bewertung des jeweiligen Systems dar.

3. Es ist u. a. zu klären, ob der auszuwählende Standard überhaupt auf die Art, Branche, Größe, Komplexität der jeweiligen Organisation anwendbar ist.

4. Darüber hinaus ist zu entscheiden, ob der Standard zertifizierbar sein soll, internationale Anerkennung und Anerkennung bei den relevanten interested parties (z. B. Kunden) findet.

5. Wichtig ist u. a. auch, ob der zu verwendende Standard eher „generisch wissenschaftlich“ oder pragmatisch und verständlich ausgestaltet sein soll.

6. Standards sind keine Rechtsnormen. Sie können aber u. U. „strafbarkeitskonstituierende“ Wirkung haben. Der auszuwählende Standard sollte sich daher primär an aktueller Gesetzgebung, Rechtsprechung und dem **„Anerkannten Stand von Wissenschaft und Praxis“** oder gar dem höheren „Stand der Technik“ orientieren. Keinesfalls ist ein Standard anzuwenden, sofern er diesen Anforderungen widerspricht.

7. Die Auswertung von Unternehmens-, Umfeld-, interested parties- und (Compliance-) Risiko-Analyse gibt gute Hinweise für die Wahl des angemessenen Standards.

8. Nicht nur die Auswahl, sondern auch die Entscheidung, welche Anforderungen / Vorgaben des Standards erfüllt werden müssen / sollen (Umfang der Anwendung der Standards), richtet sich nach dem Ergebnis entsprechender Analysen.

9. Der ausgewählte Standard sollte fordern bzw. zumindest ermöglichen, dass im Zuge der „digitalen Transformation“ die Maßnahmen zur Erfüllung seiner Anforderungen in die Ablauforganisation (zu digitalisierende Prozesse) integriert werden: „Prozessorientierter Ansatz“.

Für ein (Compliance-) Risiko-Managementsystem und viele weitere Systeme (QM, IKS, Revision, Nachhaltigkeit (Corporate social responsibility), Informationssicherheit, etc. etc.) gibt es eine Vielzahl von Standards, die u.a. für die Ausgestaltung des Managementsystems und für Audit-Zertifizierung als Referenzgröße dienen können.

Rn. 2 Text der ISO 31000 und der ISO 19600 1 Anwendungsbereich

1 Text der ISO 31000 und der ISO 19600

1.1 Text der ISO 31000:2018

„1 Anwendungsbereich
Dieses Dokument legt Leitlinien für das Umgehen mit Risiken fest, denen Organisationen ausgesetzt sind. Die Anwendung dieser Leitlinien kann an jede Organisation und deren Kontext angepasst werden.

Dieses Dokument bietet einen allgemeinen Ansatz für das Umgehen mit jeglicher Art von Risiko und ist nicht industrie- oder sektorspezifisch.

Dieses Dokument kann während der gesamten Lebensdauer der Organisation genutzt und auf alle Aktivitäten einschließlich der Entscheidungsfindung auf allen Ebenen angewendet werden.“

1.2 Text der ISO 19600:2016

*„**1 Anwendungsbereich***
Diese Internationale Norm gibt Empfehlungen für den Aufbau, die Entwicklung, die Umsetzung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines adäquaten und wirksamen Compliance-Managementsystems innerhalb einer Organisation.

Diese Leitlinien für Compliance-Managementsysteme gelten für alle Formen von Organisationen. Der Umfang der Anwendung dieser Leitlinien hängt von der Größe, Struktur, Art und Komplexität der Organisation ab. Diese Internationale Norm basiert auf den Grundsätzen der Good Governance, der Verhältnismäßigkeit, der Transparenz und der Nachhaltigkeit.“

Rn. 3 Erläuterung (Kommentierung) des „Anwendungsbereiches eines Standards“

2 Erläuterung (Kommentierung im engeren Sinne)

2.1 Definition des „Anwendungsbereichs eines Standards“ in allgemein zugänglichen Informationsquellen

Anwendungsbereich: „Bereich, in dem etwas Anwendung findet.“[1]

„Anwendungsbereich“ am Beispiel *der hier dargestellten Standards* „ISO 31000“ für ein Risiko-Managementsystem und „ISO 19600“ für ein Compliance-Managementsystem:

Rn. 4 Abgrenzung zwischen Anwendungsbereich des *Standards* und Anwendungsbereich des *Managementsystems*

Abgrenzung: Es geht an dieser Stelle *nicht* um den Anwendungsbereich des (Compliance-) Risiko-*Managementsystems*, (vgl. dazu z.B. ISO High Level Structure, Punkt 4.3) sondern um den Anwendungsbereich des *Standards.*

Die Beantwortung der Frage, welcher Standard für welches Unternehmen / welche Organisation der passende ist, sollte nicht dem Bauchgefühl überlassen werden, sondern stellt eine unternehmerische Entscheidung (Business Judgment Rule) (§ 93 Abs. 1 AktG) im Zusammenhang mit der Einrichtung, Ausgestaltung und Bewertung des jeweiligen Systems dar.

[1] http://www.duden.de/rechtschreibung/Anwendungsbereich

Es ist u. a. zu klären, ob der auszuwählende Standard überhaupt auf die Art, Branche, Größe, Komplexität der jeweiligen Organisation anwendbar ist.

Unternehmen stehen vor einer großen Auswahl möglicher Standards mit Bezug zu Risiko-Managementsystemen:
ISO 31000:2018, COSO II:2017, IDW PS 981:2017, DIIR Nr. 2, Ma Risk, ÖNORM 4900 ff., etc. etc.
Ebenso groß ist die Auswahl an Standards für Compliance-, IKS- und sonstigen Managementsystemen.

Gleich an dieser Stelle sei der wichtige Hinweis erlaubt, dass Compliance-Risiken ebenso wie jegliche andere Art von Risiken (Finanz-, Strategie-, Reputations-Risiken) von einem Risiko-Managementsystem mit umfasst werden müssen: Vgl. den Text der ISO 31000: „**jegliche** Art von Risiko".
Sofern ein Compliance-Managementsystem sich in Unternehmen/Organisation um Compliance-Risiken (Welcher Standard passt zu uns?) kümmert, ist eine enge Verbindung sicherzustellen, um eine angemessene Gesamt-Risiko-Bewertung und -Aggregation zu gewährleisten.
Die Frage „Welcher Standard passt zu uns?" stellt sich damit auch in Bezug auf das Compliance-Managementsystem und sollte intern harmonisiert werden:

Das passende Risiko-Managementsystem ist somit auch für ein angemessenes Compliance-Managementsystem wichtig.

Wenn Sie sich an einem bestimmen Standard orientieren wollen, sollte diese Entscheidung also nicht auf „Bauchgefühl" beruhen, sondern wohl überlegt sein:

Rn. 5 Angesprochene Unternehmen und Organisationen - Welcher Standard ist für das jeweilige Unternehmen/Organisation geeignet?

Entscheidende Frage ist somit auch, ob der angestrebte *Standard* überhaupt für das jeweilige Unternehmen / die jeweilige Organisation anwendbar und geeignet ist.

So ist z. B. die *MA Risk* branchenbezogen vor allem auf Kreditinstitute anwendbar.
IDW PS 981:2017 beispielsweise regelt nur, *wie* Wirtschaftsprüfer in Deutschland ein Risiko-Managementsystem zu prüfen haben. Er sieht außerdem vor, dass das zu prüfende Unternehmen einen anderen Standard als Referenzgröße heranzieht.
Außerdem ist der deutsche IDW PS 981 u. U. im Ausland nicht anerkannt, was international agierende Unternehmen eher auf die international in etwa zu jeweils 50% verbreiteten Standards ISO 31000 oder COSO II verweist.
Ähnliches gilt für DIIR Nr. 2: Er regelt, wie und was die *Revision* in Bezug auf das Risiko-Managementsystem zu prüfen hat.

Die Vorgaben / Anforderungen dieser Standards ISO 31000 oder ISO 19600 dagegen beziehen sich auf die *Ausgestaltung* des Managementsystems und sind auf alle Arten von Unternehmen oder Organisationen (öffentlich-rechtlich, privatrechtlich, profit- / non-profit-Organisationen) unabhängig von der Größe, Struktur, Natur und Komplexität anwendbar.

Der vom Unternehmen / der Organisation zu wählende *Standard sollte* sich an Anforderungen von Gesetzgebung und Rechtsprechung an (Risiko-) Managementsysteme mit seinen Komponenten und an (international) anerkannten und angewendeten Standards und damit i.d.R. an dem *„Anerkannten Stand von Wissenschaft und Praxis"* orientieren.
Der „*Universal-Standard Risiko-Managementsystem (2019)*"[2] des Internationalen Institutes für Governance, Management, Risk & Compliance der Technischen Hochschule Deggendorf stellt in diesem Zusammenhang keinen weiteren zusätzlichen Standard dar, sondern versucht, durch

[2] Zum kostenlosen Download auf www.scherer-grc.net/publikationen.

synoptische Darstellung der diversen „markt-gängigen“ Standards einen einheitlichen Aufbau darzustellen und zugleich Gesetzgebung, Rechtsprechung und den Anerkannten Stand von Wissenschaft und Praxis zu berücksichtigen.
Diese „Referenzgrößen“ dienen als sozusagen „höherrangige“ Basis zur Differenzierung zwischen „Muss- und Soll-Anforderungen“ eines Standards, unabhängig davon, was das Normungsgremium „in den Standard geschrieben“ hat.

Rn. 6 Ist der Standard eine mögliche Grundlage für die Zertifizierung eines (Risiko-) Managementsystems?

Darüber hinaus ist zu entscheiden, ob der Standard zertifizierbar sein soll, internationale Anerkennung und Anerkennung bei den relevanten interested parties (z. B. Kunden) findet.

Die ISO 31000 spricht unter Punkt „1 Anwendungsbereich" in **Satz 1** von Leitlinien und in **Satz 3** von einem allgemeinen Ansatz.

Da sie nur als „Leitlinie“ ausgestaltet wurde und also keine Muss-Vorgaben enthält, ist diese Norm auch nicht zertifizierbar.
Anders der „*Universal-Standard Risiko-Managementsystem (2019)*“ und voraussichtlich 2020 auch die ÖNORM 4900 ff: Diese sind zertifizierbar ausgestaltet.
Der IDW PS 981 dient als Grundlage für ein Wirtschaftsprüfer-*Testat*.

Interessant erscheint die neue Entwicklung im Bereich der *Digitalisierung*, die durch *Human Workflows* versucht, sicherzustellen, dass sich Mitarbeiter an zuvor auch im Hinblick auf Compliance optimierte Prozesse halten, indem sie durch diese ohne legale Möglichkeit, abzuweichen, geführt werden.

Rn. 7 Anforderungen des „Anwendungsbereichs der Standards ISO 31000 und ISO 19600 im Lichte von Gesetzgebung und Rechtsprechung

2.2 Anforderung an den „Anwendungsbereich eines Standards“ im Lichte von Gesetzgebung und Rechtsprechung

Standards sind keine Rechtsnormen. Sie können aber u. U. „strafbarkeitskonstituierende“ Wirkung haben. Der auszuwählende Standard sollte sich daher primär an aktueller Gesetzgebung, Rechtsprechung und dem „Anerkannten Stand von Wissenschaft und Praxis“ oder gar dem höheren „Stand der Technik“ orientieren. Keinesfalls ist ein Standard anzuwenden, sofern er diesen Anforderungen widerspricht.

Rn. 8 Rechtsnatur eines Standards

Zur Rechtsnatur eines Standards:

Ein Standard stellt in der Regel keine verbindliche (Rechts-)Norm dar (Ausnahme, falls ein Gesetz / Rechtsverordnung die Anwendung eines Standards für verbindlich erklärt[3]), sondern kann unter Umständen wie ein „antizipiertes Sachverständigengutachten“ wirken und die Vermutung auslösen, einen derzeitigen Entwicklungsstand („Stand von Wissenschaft und Praxis“, „Allgemein anerkannte Regeln der Technik“), widerzuspiegeln.[4]

[3] Vgl. z. B. § 315a HGB und die „IAS-Verordnung der EU“.
[4] Vgl. hierzu ausführlich: *Scherer/Fruth*, Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis“ auf Organhaftung und Corporate Governance - am Beispiel der ISO 19600 (2014) Compliance-Managementsystem, in Corporate Compliance Zeitschrift (CCZ), 2015, S. 9 - 17 mit Kommentierung von *Withus*, Die Angemessenheit eines CMS - eine rein juristische Bewertung oder anerkannter Stand von betriebswirtschaftlichen Grundsätzen?, in Corporate Compliance Zeitschrift (CCZ) 2015, S. 139 ff.

Sofern Gesetze oder Rechtsprechung einen bestimmten Entwicklungsstand fordern *und* der betreffende Standard diesen tatsächlich widerspiegelt, kann der Standard mittelbar als verpflichtend bezeichnet werden.
Bzgl. Compliance-Managementsystem-Standards hat der Vorsitzende Richter des ersten Strafsenats des *BGH*, *Raum*, von einer u. U. „*strafbarkeitskonstituierenden Wirkung*“ gesprochen.

Auch vertraglich lässt sich die Einhaltung von zu bezeichnenden Standards verbindlich vereinbaren.

Ein (Compliance-) Risiko-Managementsystem muss in erster Linie den Vorgaben von Gesetz und Rechtsprechung sowie dem „Anerkannten Stand von Wissenschaft und Praxis“ entsprechen.

Es gilt stets folgende **Prüfungsreihenfolge** bzgl. der Frage, wonach sich ein (Compliance-) Risiko-Managementsystem als Soll-(Referenz-) Größe zu orientieren hat:

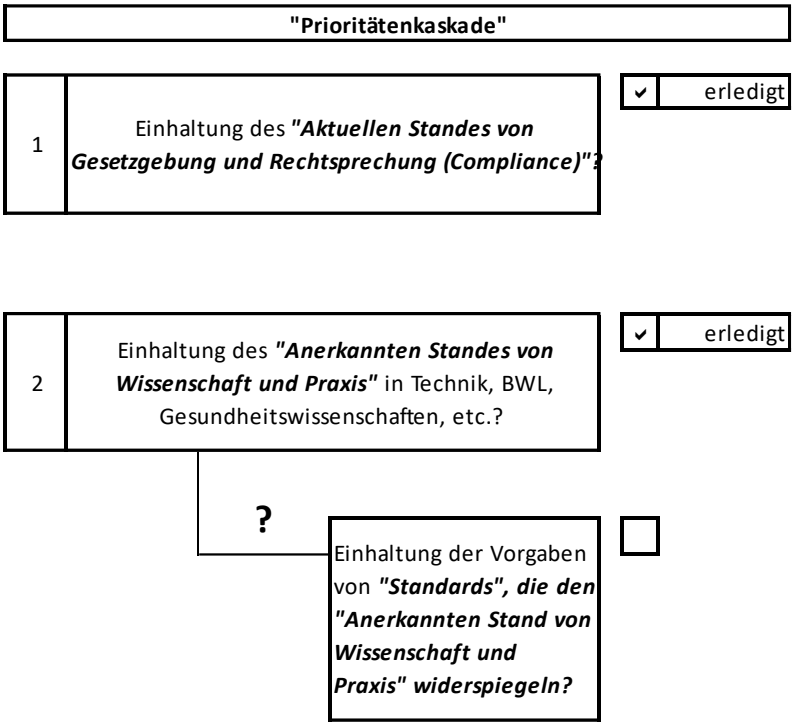

Abbildung 1: Prioritätenkaskade[5]

Ob „Leitlinien“ bzw. Standards – hier: die ISO 31000 und die ISO 19600 ff.– diese Anforderungen erfüllen, ist zu klären.

„***Legal and Regulatory Factors***
Governance may be impacted by complex legal, jurisdictional and liability issues. Standards that do not recognize these factors run the possibility of creating new risks to individuals and organizations.
In addition, government and regulatory policy for governance may be mature in some countries and less so in others. ISO/TC309 has an opportunity to (further) develop standards (e.g. in areas of compliance, whistleblowing, anti-bribery, governance, and prevention of corruption and fraud) that both complement existing, and inform the development of, new policy and regulatory frameworks.
ISO/TC309 deliverables will not replace, undermine or negate existing national policy, regulation or legislation but will support such instruments. The growth in volume and range of international guidance

[5] Vgl. *Scherer/Fruth* (Hrsg.), Governance-Management, Band 1, 2014, S. 115.

suggests that government and regulators globally are showing an increasing interest in governance and management systems that support governance."[6]

Wichtiger Hinweis:
Bei Widerspruch zwischen Vorgaben des Standards zu relevanten Gesetzen, Rechtsprechung oder dem Anerkannten Stand von Wissenschaft und Praxis sind die jeweiligen Vorgaben eines Standards nicht (!) zu befolgen!

Dies erwähnt explizit als einer der wenigen Standards nur *ISO 37001:2016 Antikorruptions-System* unter Punkt 1 *Anwendungsbereich*:

„Wenn eine Anforderung dieser Internationalen Norm vollständig oder teilweise mit dem geltenden Recht im Widerspruch steht oder verboten ist, dann ist die Organisation nicht zur vollständigen oder teilweisen Erfüllung dieser zutreffenden Anforderung verpflichtet."

Hinweis: Gleichwohl ist diese Klarstellung irreführend bzw. gefährlich: Falls die Erfüllung einer Anforderung der ISO 37001 verboten wäre, besteht nicht nur eine „Befreiung" von der Pflicht zur Erfüllung der ISO-Norm-Anforderung, sondern die Erfüllung der Anforderung würde einen (u.U.) haftungsbegründenden Pflicht-(Compliance-)Verstoß darstellen!
Ebenso verhält es sich natürlich mit Anforderungen aus der ISO 31000 oder der ISO 19600.

Rn. 9 Umfang der Anwendung des Standards

In welchem Umfang ist der passende Standard in Ihrem Unternehmen / in Ihrer Organisation anzuwenden?

Idealerweise sollte sich die Anwendung des Standards, respektive dessen Anforderungen auf alle (Prozess-) Themenbereiche der Organisation (Finanzen, Personal, Einkauf, Vertrieb, IT, …) erstrecken. Viele Organisationen beginnen jedoch zumeist mit ausgewählten Bereichen oder Fachthemen (z.B. operative Risiken, Einkauf, Produktion, Vertrieb, etc.). Es ist aber zu reflektieren und zu kommunizieren, dass sich Risk, Compliance, etc. auf *alle* Bereiche beziehen.

Die **ISO 19600** spricht in **Satz 3 von Punkt „1 Anwendungsbereich"** zu Recht davon, dass der „*Umfang der Anwendung dieser Leitlinien von Größe, Struktur, Art und Komplexität der Organisation*" abhänge.

Dies entspricht auch der Rechtsprechung des *LG München* („Neubürger"), die bzgl. der Ausgestaltung eines CMS „*Angemessenheit*" („Geeignetheit zur Erreichung der Ziele") fordert.

Vgl. *LG München* v. 10.12.2013:
***„Entscheidend für den Umfang im Einzelnen** sind dabei Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz, wie auch die Verdachtsfälle aus der Vergangenheit […]".*

Ebenso hat sich nunmehr der Vorsitzende Richter des 1. Strafsenats des BGH *Raum* zu den „inhaltlichen Maßgaben" für ein angemessenes **Compliance**-Managementsystem mit u.U. strafbarkeitsvermindernder Wirkung (!) geäußert:

***„Inhaltliche Maßgaben"* für Angemessenheit / Ordnungsmäßigkeit eines CMS:**[7]
1. *„Permanent zu aktualisierende Risikoanalyse"*

[6] ISO Strategic Business Plan ISO/TC309 vom 26.01.2018 (final for ballot).
[7] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 40, Rn. 27 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

2. Fortbildung der Mitarbeiter
„Vermittlung der für die Mitarbeiter in ihrem Tätigkeitsfeld maßgeblichen Normen" […]

3. Anonymitätswahrendes Hinweisgebersystem:
„Wichtig ist die Vertraulichkeit, […]"
4. Konsequente Ahndung von Verstößen
(Compliance-Verstoß-Erkennungs- und Reaktionsprozess: Casemanagement-Prozess)

Vgl. hierzu auch den *BGH* bzw. *Raum*:

*„Die **permanent zu aktualisierende Risikoanalyse**[8] **setzt voraus, dass Vorkehrungen getroffen sind**, die es erlauben, den Markt ständig im Blick auf mögliche Gefahrensituationen zu beobachten." […]*
*„Für die **Bemessung der Geldbuße** ist zudem **von Bedeutung, inwieweit** die Nebenbeteiligte ihrer **Pflicht, Rechtsverletzungen aus der Sphäre** des Unternehmens **zu unterbinden**, **genügt und ein** effizientes („effektives")[9] **Compliance-Management installiert** hat, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss.*[10]

*Dabei kann auch eine Rolle spielen, ob die Nebenbeteiligte **in der Folge dieses Verfahrens entsprechende Regelungen optimiert** und **ihre betriebsinternen Abläufe so gestaltet hat**,*[11] *dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden."*[12]

„Ein Compliance-System wird vom Organ des Unternehmens installiert, […].
*Das Organ erfüllt durch die Etablierung eines solchen Systems, […], **seine ihm kraft Gesetzes obliegende Verantwortung**.*
*Das **Organ ist verpflichtet, Rechtsverletzungen**, die aus der Sphäre des unter seiner Herrschaft betriebenen Unternehmens begangen werden, **zu unterbinden bzw. gar nicht erst entstehen zu lassen**.*
*Wie der **Bundesgerichtshof in ständiger Rechtsprechung** entscheidet, gehört zu den Pflichten der Organe von Kapitalgesellschaften, den Vorteil der Gesellschaft zu wahren und Schaden von ihr abzuwenden. **Dies schließt die Sorge um das rechtmäßige Verhalten der Gesellschaft nach außen mit ein."***[13]

Interessant ist der Aufsatz von *Raum*[14] auch insofern, als *Raum* auch von einer u.U. ***„strafbarkeitskonstituierenden" Wirkung von Standards*** (!) spricht.
Die dargestellten Grundsätze der Rechtsprechung lassen sich direkt auf ein (Compliance-) Risiko-Managementsystem anwenden.

Rn. 10 Prozessabläufe

[8] Anmerkung: Hervorhebung durch Verfasser
[9] Anmerkung des Verfassers: Effektiv (Ziel wird erreicht) und effizient (ressourcenschonend) wird häufig verwechselt. Gemeint war sicher „effektiv"
[10] *Raum* in Hastenrath, Compliance – Kommunikation, 2. Aufl., S. 31 f.
[11] Anmerkung: Fettdruck durch Verfasser
[12] *BGH*, Urteil vom 09.05.2017 Az. 1 StR 265/16, Rn. 118 (Beck RS 2017, 114548).
[13] *Raum* im Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 31, Rn. 2, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.
[14] *Raum* im Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 31, Rn. 2, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

2.3 Prozessbeschreibung

Der ausgewählte Standard sollte fordern bzw. zumindest ermöglichen, dass im Zuge der „digitalen Transformation“ die Maßnahmen zur Erfüllung seiner Anforderungen in die Ablauforganisation (zu digitalisierende Prozesse) integriert werden: „Prozessorientierter Ansatz“.

Bzgl. der Prozesse zur Prüfung des *„Umfangs der Anwendung dieser Leitlinien“* nach der ISO 31000 und ISO 19600 wird auf die Prozesse „Unternehmens-, Umfeld- und interested parties-Analyse“ sowie den Prozess für die Risikoanalyse verwiesen.

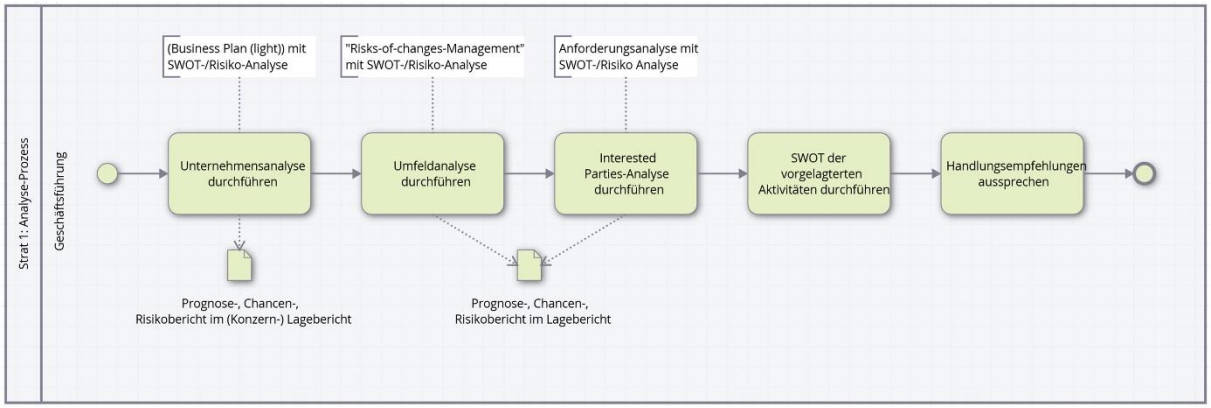

Abbildung 2: Prozesse im Bereich Unternehmens-, Umfeld- und Interested parties-Analyse.

Die Bewertung der Analysen ergibt Hinweise, *wie* ein (Compliance-) Risiko-Managementsystem auszugestalten ist und in welchem Umfang der gewählte Standard zur Anwendung kommen muss.

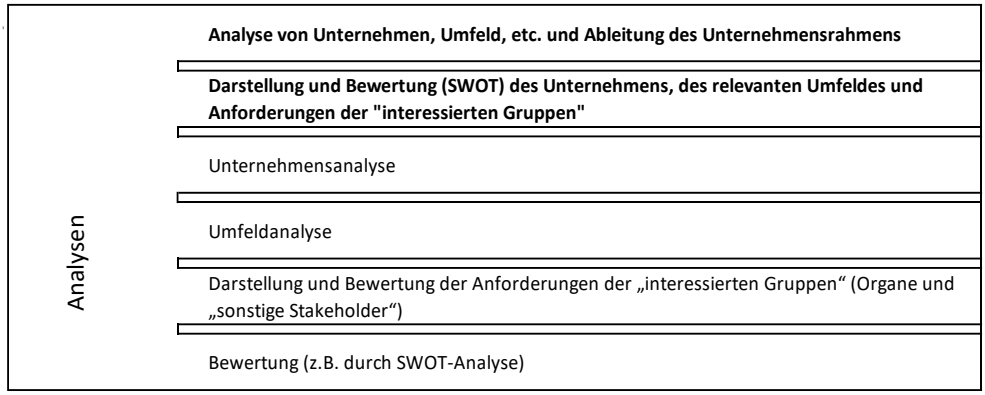

Abbildung 3: Unternehmens-, Umfeld-, Interested Parties-Analyse-Prozess.

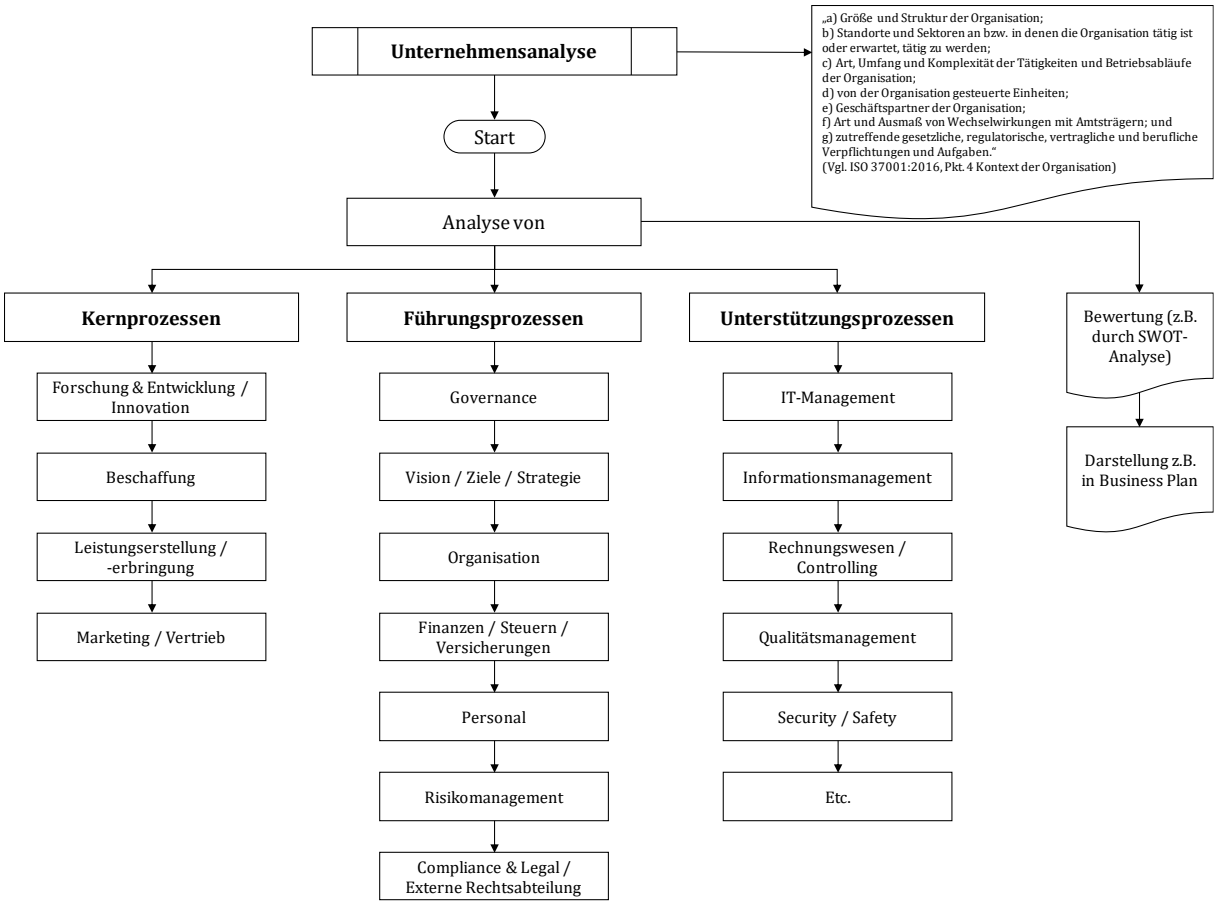

Abbildung 4: Unternehmensanalyse.

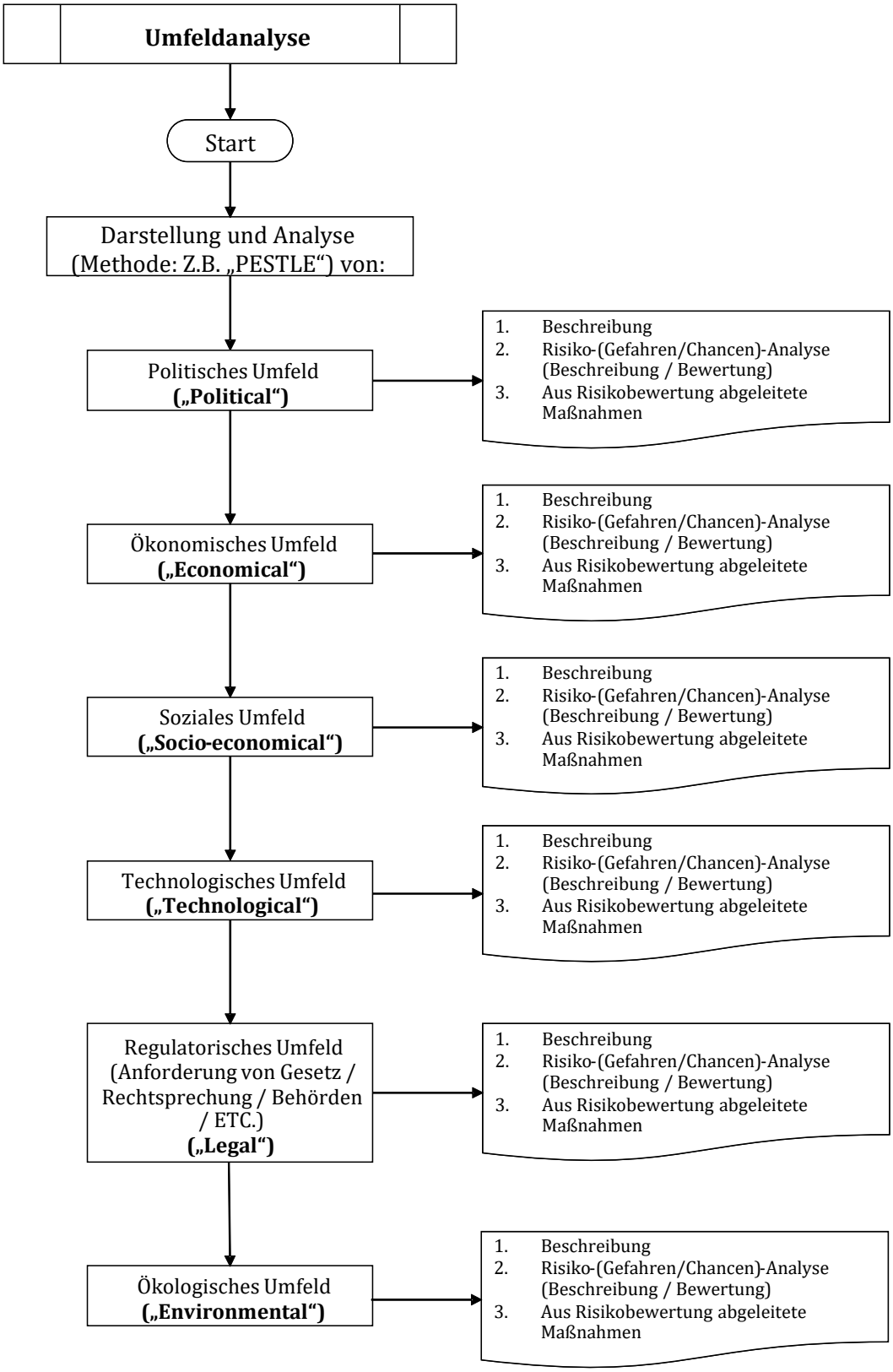

Abbildung 5: Umfeldanalyse.

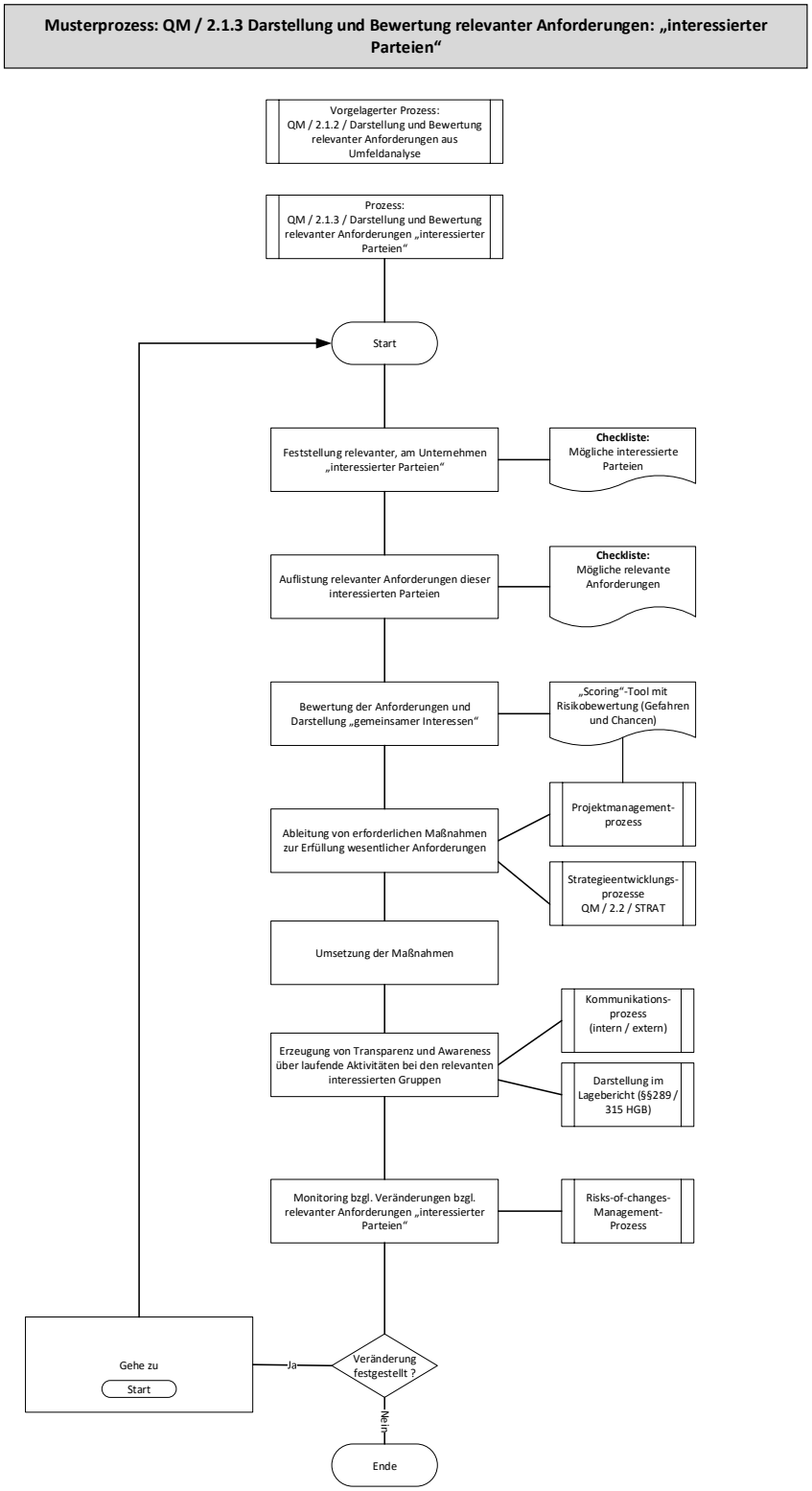

Abbildung 6: Bestimmung der Anforderungen der interessierten Parteien.

Rn. 11 Beispiele aus Unternehmen

2.4 Beispiele aus der Praxis

BMW-Group

Unternehmen, wie beispielsweise die *BMW Group*, **dokumentieren die Umsetzung und Anwendung der Compliance-Anforderungen auch in den Lage- bzw. Geschäftsberichten**.

„Das BMW Group Compliance Committee […] steuert und überwacht die erforderlichen Aktivitäten zur Vermeidung von Rechtsverstößen. Hierzu gehören Trainings-, Informations- und Kommunikationsmaßnahmen sowie Compliance-Kontrollen und die Verfolgung von Rechtsverstößen. […]
Die Entscheidungen des BMW Group Compliance Committee werden im BMW Group Compliance Committee Office konzeptionell vorbereitet und operativ umgesetzt. […]
Basis des Compliance-Management-Systems ist der BMW Group Verhaltenskodex, in dem sich der Vorstand der BMW AG zu Compliance als gemeinsamer Aufgabe bekennt („Tone from the Top").“[15]

Flughafen München

Beim Flughafen München werden die Compliance-Risiken durch eine eigene Konzerneinheit überwacht, erkannt und minimiert:

„Der Flughafen München hat dazu ein konzernweites Compliance-Management-System eingerichtet […]. […] Eine Kernaufgabe der Konzerneinheit Compliance ist die Schulung und Beratung der Beschäftigten und der Führungskräfte in Compliance-Fragen, um so Compliance-Verstöße bereits präventiv zu verhindern. […]
Über ein elektronisches Hinweisgebersystem […] können Mitarbeiter des Flughafens München, Geschäftspartner und auch Kunden Hinweise auf unternehmensschädigendes Verhalten geben.“[16]

RWE AG

Die Rheinisch-Westfälische Elektrizitätswerk AG verfügt über einen Bereich Interne Revision & Compliance, welcher über die Einhaltung des *RWE*-Verhaltenskodex inkl. der Vermeidung von Korruptionsrisiken wacht. Der Prüfungsausschuss richtete sein besonderes Augenmerk auf das Risikomanagementsystem des Konzerns und *„[…] befasste […] sich mit Compliance-Fragen sowie mit der Planung und den Ergebnissen der internen Revision“*[17].
Zudem wurde 2015 ein IKS-Komitee eingerichtet:

„[…] Es soll darauf hinwirken, dass das IKS im gesamten Konzern mit hohen Ansprüchen an Korrektheit und Transparenz und nach einheitlichen Grundsätzen „gelebt“ wird. Die Mitglieder des Komitees sind Vertreter der Bereiche Rechnungswesen, Controlling & Compliance sowie Verantwortliche aus den Funktionen Finanzen, Personal, Einkauf, Handel und IT, die eine wichtige Rolle für die Rechnungslegung spielen.“[18]

[15] BMW Group, Geschäftsbericht (2015), S. 184 ff.
[16] Flughafen München, Integrierter Bericht (2016), S. 100 ff.
[17] RWE AG, Geschäftsbericht (2016), S. 11 und S. 77 ff.
[18] RWE AG, Geschäftsbericht (2016), S. 85 ff.

Technische Hochschule Deggendorf

An der THD sorgt ein Compliance-Komitee für ein einheitliches Complianceverständnis und Compliancebewusstsein. Dabei initiiert und begleitet es die Entwicklung eines Compliance-Managementsystems: *„[…] Für die Umsetzung und Einhaltung der jeweiligen Compliance-Maßnahmen ist jeder Mitarbeiter innerhalb seines Zuständigkeitsbereiches persönlich verantwortlich.*
Die Implementierung eines Compliance-Managementsystems hat nach dem P / D / C / A-Regelkreis zu erfolgen.“[19]

Rn. 12 Tools / Toolbox

2.5 Betriebswirtschaftliche Instrumente (Tools und Methoden)

Zu den Tools zur Überprüfung, welcher Standard für das jeweilige Unternehmen/Organisation der passende und welcher Umfang der Anwendung des Standards (beispielsweise ISO 31000 und ÖNORM 4900 ff.) angemessen ist, zählen die Auswertung von Unternehmens-, Umfeld-, Interested Parties-Analyse und einer (Compliance-) Risiko-Analyse (vgl. oben)!

Nicht nur die Auswahl, sondern auch die Entscheidung, welche Anforderungen / Vorgaben des Standards erfüllt werden müssen / sollen (Umfang der Anwendung der Standards), richtet sich nach dem Ergebnis entsprechender Analysen.

Außerdem sollte der Beschluss der Geschäftsleitung, der verbindlich festlegt, an welchen Standard(s) sich die Organisation orientiert sowie etwaige Einschränkungen der Anwendung (vgl. Punkt 2.2) dokumentiert sein.

Rn. 13 Synopsen (analoge Regelungen) in anderen Standards

3 Synopsen: Aussagen zum „Anwendungsbereich *des Standards*“ in anderen Managementsystem-Standards

Rn. 14 Text des Universal-Standards: „Standardorientierung – Anwendungsbereich des Standards“

3.1 Text des Universal-Standards (Compliance-) Risiko-Managementsystem des International Institute for Governance, Management, Risk & Compliance: Stand 01/2019 (www.gmrc.de)

„1.1.3 Standardorientierung – Anwendungsbereich des Standards

Anwendungsbereich dieses hier dargestellten Universal-Standards für ein (Compliance-) Risiko-Managementsystem:

Die Vorgaben / Anforderungen dieses Standards sind auf alle Arten von Unternehmen oder Organisationen (öffentlich-rechtlich, privatrechtlich, profit- / non-profit-Organisationen) unabhängig der Größe, Struktur, Natur und Komplexität anwendbar.

[19] FAQs zum Compliance-Komitee, TH Deggendorf (2017), S. 3 ff.

Dieser Standard orientiert sich an Anforderungen von Gesetzgebung und Rechtsprechung an Risiko-Managementsysteme und an (international) anerkannten und angewendeten Standards und damit i.d.R. an dem „Anerkannten Stand von Wissenschaft und Praxis“.[20]

Rn. 15 Weitere Synopsen

3.2 Text des IDW PS 981:2017: Prüfung eines Risiko-Managementsystems

„1. Vorbemerkungen

1 ***Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) verdeutlicht in diesem IDW Prüfungsstandard den Inhalt freiwilliger Prüfungen von Risikomanagementsystemen*** *und legt die Berufsauffassung dar (…).*

2 *§ 107 Abs. 3 Satz 2 AktG sieht vor, dass der Aufsichtsrat aus seiner Mitte einen Prüfungsausschuss bestellen kann, der sich neben der Überwachung der Abschlussprüfung befasst mit*
- der Überwachung des Rechnungslegungsprozesses,
- der Wirksamkeit
- des internen Kontrollsystems,
- des Risikomanagementsystems und
- des internen Revisionssystems.

In der Gesetzesbegründung zum BilMoG wird ausgeführt, dass die in § 107 Abs. 3 Satz 2 AktG – der 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 (vgl. Tz. A1). Zudem wird in der Gesetzesbegründung klargestellt, dass der Aufsichtsrat die genannten Aufgaben selbst wahrzunehmen hat, wenn er keinen Prüfungsausschuss einrichtet.[21]

3 ***Die Überwachungsaufgaben des Aufsichtsrats umfassen auch die Maßnahmen des Vorstands, die sich auf die Begrenzung der Risiken aus möglichen Verstößen gegen gesetzliche Vorschriften und interne Richtlinien (Compliance) beziehen.*** *Dem trägt Ziffer 5.3.2 des Deutschen Corporate Governance Kodex (DCGK) Rechnung, der zu den Aufgaben des Prüfungsausschusses ausführt, dass sich der Prüfungsausschuss – falls kein anderer Ausschuss damit betraut ist – auch mit der Compliance des Unternehmens befasst.*

4 *Während die Befassung durch den Aufsichtsrat und den Prüfungsausschuss voraussetzt, dass die entsprechenden Systeme vorhanden sind****, ist – ungeachtet der Pflichten nach § 91 Abs. 2 AktG – die Einrichtung, Ausgestaltung und Überwachung der Systeme eine im Organisationsermessen des Vorstands stehende unternehmerische Entscheidung, durch die der Vorstand vor dem Hintergrund der unternehmensindividuellen Gegebenheiten seinen allgemeinen Organisations- und Sorgfaltspflichten nachkommt (vgl. Tz. A2).***

5 ***Die*** *durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden* ***Corporate Governance Systeme***

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

[20] *„Da sich der hier vorgestellte Standard überwiegend an zwingenden Vorgaben (Gesetze und Rechtsprechung) und bzgl. der sonstigen Anforderungen an gängige ISO- / COSO- / IDW- / etc.-Standards anlehnt, ist bzgl. der Vorgaben an das ordnungsgemäße Entstehen eines Standards auf die jeweiligen Verfahrensweisen der dort standardsetzenden Organisation zu verweisen.“*

[21] *Vgl. BT-Drucks. 16/10067, S. 102.*

sind weder im Gesetz noch in der Literatur eindeutig definiert. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme lehnt sich dieser IDW Prüfungsstandard an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement[22] an.

6 *(…) Die Prüfung der Wirksamkeit dieser Systeme durch einen unabhängigen Wirtschaftsprüfer kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten des Vorstands und des Aufsichtsrats dienen.*

7 ***Dieser IDW Prüfungsstandard behandelt die Prüfung des Teils des unternehmensweiten Risikomanagements, der sich mit den strategischen Risiken und den operativen Risiken aus der Geschäftstätigkeit*** *(Risiken aus den Leistungserstellungsprozessen)* ***befasst****.* ***Die Prüfung umfasst stets sämtliche Grundelemente des Risikomanagementsystems*** *(vgl. Tz. 30).* ***Eine isolierte Prüfung einzelner Grundelemente liegt nicht im Anwendungsbereich dieses IDW Prüfungsstandards*** *(vgl. Tz. A4).*

8 *Die Zielsetzung einer nach diesem IDW Prüfungsstandard durchgeführten* ***Systemprüfung*** *liegt in der Beurteilung****, inwieweit das Unternehmen durch Einrichtung eines RMS Vorsorge getroffen hat, wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen.*** *Ziel ist es dagegen nicht, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete oder durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet oder wirtschaftlich sinnvoll sind. Die Prüfung ist auch nicht darauf ausgerichtet, ein Prüfungsurteil über den Fortbestand des geprüften Unternehmens zu erteilen.*

9 ***Die Prüfung des RMS kann auf das Management der strategischen Risiken begrenzt werden.*** *(…) Im Falle der Prüfung des strategischen RMS erfolgt daher i.d.R. keine Eingrenzung auf einzelne Unternehmensprozesse oder Bestandteile der Unternehmensorganisation (vgl. Tz. A6).*

10 *Operative (betriebliche) Risiken betreffen (…).* ***Für Zwecke der Prüfung des operativen Risikomanagementsystems sieht dieser IDW Prüfungsstandard eine Abgrenzung zu prüfender Teilbereiche durch die gesetzlichen Vertreter vor.***

11 *Die* ***Abgrenzung*** *eines zu prüfenden Teilbereichs i.S. dieses IDW Prüfungsstandards* ***bestimmt sich nach einzelnen operativen Risikoarten und/oder Unternehmensprozessen bzw. Organisationseinheiten*** *(z.B. Geschäftsbereichen, Funktionsbereichen, Geschäftsprozessen, Niederlassungen und/oder Regionen) (vgl. Tz. A3).*

12 ***Für die Prüfung des Compliance Management Systems, des internen Kontrollsystems der Unternehmensberichterstattung sowie des internen Revisionssystems hat das IDW gesonderte IDW Prüfungsstandards veröffentlicht.[23] Die Abgrenzung*** *der Prüfungsgegenstände* ***ist dabei nicht notwendigerweise überschneidungsfrei.***

---

[22] *Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk (COSO ERM): http://www.coso.org/ERM.htm.*

[23] *Vgl. IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980) (Stand: 11.03.2011). Zurzeit in Bearbeitung: Entwurf eines IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems der Unternehmensberichterstattung (IDW EPS 982) und*

13 ***Die Prüfung des RMS ist von der Prüfung des gemäß § 91 Abs. 2 AktG einzurichtenden Überwachungssystems zur frühzeitigen Erkennung von den Fortbestand der Gesellschaft gefährdenden Entwicklungen (sog. „Risikofrüherkennungssystem“) nach § 317 Abs. 4 HGB zu unterscheiden. Die Prüfung des Risikofrüherkennungssystems umfasst*** *zwar die Grundelemente Risikoidentifikation, Risikobeurteilung, Risikokommunikation und Überwachung,* ***nicht*** *aber* ***die Risikosteuerung****. Die Reaktionen des Vorstands auf erfasste und kommunizierte Risiken selbst sind somit nicht Gegenstand der Maßnahmen i.S.d. § 91 Abs. 2 AktG und damit auch nicht Gegenstand der Prüfung nach § 317 Abs. 4 HGB.[24] Ferner ist anders als der Prüfungsgegenstand i.S. dieses IDW Prüfungsstandards die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB nur auf bestandsgefährdende Risiken ausgerichtet. Bei der Prüfung nach § 317 Abs. 4 HGB werden jedoch alle Zielkategorien des unternehmensweiten Risikomanagements betrachtet und nicht nur strategische und operative Risiken.*

14 *(…)*

15 ***Dieser IDW Prüfungsstandard*** *behandelt Prüfungsaufträge zur Erlangung hinreichender Sicherheit. Er* ***steht im Einklang mit dem International Standard on Assurance Engagements (ISAE) 3000 (Revised)*** *„Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ (Stand Dezember 2013).[25]*

16 *Dieser IDW Prüfungsstandard ist erstmals anzuwenden bei freiwilligen Prüfungen von RMS (vgl. Tz. A7), die nach dem 31.12.2016 beauftragt werden.[26]“*

3.3 Synopse zu IDW PS 980:2011: Prüfungsstandard für Compliance-Managementsysteme

„1 Vorbemerkung

Der IDW Prüfungsstandard ist nicht anzuwenden auf Prüfungen von Systemen, für die spezielle IDW Prüfungsstandards bestehen, z.B. auf die Prüfung von Risikofrüherkennungssystemen i.S.d. IDW PS 340[27] oder die Prüfung von Risikomanagementsystemen i.S.d. IDW EPS 525[28].

Dieser IDW Prüfungsstandard ist erstmals anzuwenden bei CMS-Prüfungen, die nach dem [30.06.2011] durchgeführt werden.

Entwurf eines IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW EPS 983).

[24] *Vgl. IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340) (Stand: 11.09.2000), Tz. 4–6.*

[25] *https://www.ifac.org/ISAE3000.*

[26] *Eine freiwillige frühere Anwendung dieses IDW Prüfungsstandards ist zulässig.*

[27] „IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340) (Stand: 11.09.2000).“

[28] „Entwurf IDW Prüfungsstandard: Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung (IDW EPS 525) (Stand: 06.03.2009)“

Dieser IDW Prüfungsstandard steht im Einklang mit dem International Framework for Assurance Engagements und dem International Standard on Assurance Engagements (ISAE) 3000 „Assurance Engagements other than Audits or Reviews of Historical Financial Information".[29]"

„6. Anwendungshinweise und Erläuterungen
Vorbemerkungen [Tz. 1 ff.]"

Dieser IDW Prüfungsstandard ist nicht anzuwenden bei Aufträgen zur Durchführung vereinbarter Untersuchungshandlungen (sog. agreed upon procedures). Unter Aufträgen zur Durchführung vereinbarter Untersuchungshandlungen sind solche Aufträge zu verstehen, bei der ein Wirtschaftsprüfer Untersuchungshandlungen einschließlich einer Berichterstattung hierüber nach zuvor mit dem Auftraggeber vereinbarten Anforderungen durchführt (z.B. ob bei der Erfassung der Reisekosten für eine oder mehrere Personen Belege vorliegen). Dabei wird weder ein zusammengefasstes Gesamturteil über den Untersuchungsgegenstand abgegeben, noch enthält die Berichterstattung einzelne Urteile in Bezug auf die jeweiligen Untersuchungshandlungen.
Der Wirtschaftsprüfer berichtet lediglich über seine tatsächlichen Feststellungen (factual findings) zu den jeweils untersuchten Sachverhalten. Die Schlussfolgerungen sind durch den Berichtsempfänger aus den Feststellungen des Wirtschaftsprüfers zu ziehen.[30]

3.4 Synopse zu COSO I:2013: Internal Control[31]

Das COSO-Modell beschreibt ein Rahmensystem interner Kontrollen, das die Beherrschung von Risiken sowie die Governance innerhalb einer Organisation unterstützt. Das interne Kontrollsystem soll hinreichende Gewissheit bringen, dass die operativen, Berichtslegungs- und Complianceziele der Organisation erreicht werden.
Auch COSO I dürfte auf alle Arten von Organisationen anwendbar sein.
COSO wird häufig als Grundlage für Testierungen durch Wirtschaftsprüfer herangezogen.

3.5 Synopse zu ISO 37001:2016: Antikorruption[32]

Die ISO-Norm 37001:2016: Antikorruption zielt auf die Konzeptionierung, Implementierung, Überwachung und kontinuierliche Verbesserung eines Managementsystems, das der Verhinderung von Korruption und der Compliance insbesondere mit Antikorruptionsgesetzen dient. Korruption wird dabei in einem weiten Sinne als jegliche unmittelbare oder mittelbare Vorteilsgewährung oder Vorteilsnahme, Bestechung oder Bestechlichkeit verstanden, die widerrechtlich ein Tun oder Unterlassen bewirken soll; andere (Straf-) Tatbestände sind dagegen nicht explizit umfasst.
Das Managementsystem kann als Insel-System ausgestaltet oder Teil eines integrierten Systems sein und (angepasst an die konkreten Bedingungen) *in jeder Art von Organisation* zum Einsatz kommen.

[29] "Vgl. IFAC, Handbook of International Standards on Auditing, Assurance, and Ethics Pronouncements, New York 2008, Part I, S. 188 ff. und 922 ff."
[30] Vgl. International Standard on Related Services (ISRS) 4400 „Engagements to perform Agreed-upon Procedures regarding Financial Information", IFAC, Handbook of International Standards on Auditing, Assurance, and Ethics Pronouncements, New York 2008, Part I, S. 952 ff.
[31] COSO I:2013 F. Summary of Changes to the COSO Internal Control – Integrated Framework (1992).
[32] ISO 37001:2016: „1 Anwendungsbereich"

3.6 Synopse zu ISO 9001:2015: Qualitäts-Managementsystem[33]

Basierend auf der Plan/Do/Check/Act-Methode definiert die ISO-Norm 9001:2015: Qualitäts-Managementsystem ein risikoorientiertes Qualitäts-Managementsystem, dessen (kontinuierliche Verbesserungs-) Prozesse gewährleisten, dass bei der Leistungserbringung systematisch vertragliche und sonstige (rechtliche) Verpflichtungen eingehalten werden, um dadurch die Zufriedenheit des Kunden mit dem Produkt oder der Dienstleistung zu steigern. Der ISO Standard 9001:2015 Qualitäts-Managementsystem eignet sich ebenfalls *für alle Arten von Organisationen und Branchen.*
Die ISO 9001:2015 ist zertifizierbar.

3.7 Synopse zu PAS 99:2012: Integrated Management System[34]

Die Spezifikation beinhaltet kein eigenes Managementsystem, sondern beschreibt die Grundstruktur für integrierte Systeme, indem die gemeinsamen Elemente (insbesondere von ISO-Normen) herausgestellt werden. Sie ist **für Organisationen aller Art geeignet, die zwei oder mehr Managementsysteme eingeführt haben oder einführen wollen**.

Rn. 16 Literatur zum Thema „Anwendungsbereich eines Standards“

4 Literatur

Scherer/Fruth (Hrsg.), Handbuch Integriertes Managementsystem (IMS) „on demand“ *mit Governance, Risk und Compliance (GRC)*, 2018, Punkt 1.1.3.: Standardorientierung – Anwendungsbereich des Standards

Scherer/Fruth (Hrsg.), Handbuch Integriertes Managementsystem (IMS) „on demand“ *mit Governance, Risk und Compliance (GRC)*, (eBook), 2019, Punkt 1 Anwendungsbereich

Rn. 17 Checkfragen zum Anwendungsbereich

5 Checkfragen

Checkfragen zum „*Anwendungsbereich des Standards*“

5.1. Wurden die *zwingenden* Anforderungen an ein (Compliance-) Risiko-Managementsystem aus der für die betroffene Organisation relevanten Gesetzgebung und Rechtsprechung eruiert, analysiert und erfüllt?

5.2. Wurde eine Unternehmens-, Umfeld-, Interested-Parties-Analyse sowie eine „(Compliance-) Risiko-Analyse“ durchgeführt und bewertet, um die Auswahl (ISO, COSO, IDW, DIIR, ÖNORM) und den Umfang der Anwendung der ausgewählten Standards zu bestimmen?

5.3. Gibt es eine verbindliche Aussage der Geschäftsleitung, welcher Standard bzw. welche (mehreren) Standards als Referenz-(Soll-) Größe für das (Compliance-) Risiko-Managementsystem / Integriertes Managementsystem (inklusive Risikomanagementsystem) im Unternehmen gelten soll?

[33] ISO 9001:2015: „1 Anwendungsbereich“
[34] PAS 99:2012: „1 Scope“

5.4. Wurde der konkrete Umfang der Anwendung des Standards auf „*Angemessenheit*“ (Geeignetheit, um die Ziele des (Compliance-) Risiko-Managementsystems zu erreichen) überprüft?