BCM | Berufsverband der Compliance Manager

COMPLIANCE 2015
PERSPEKTIVEN EINER ENTWICKLUNG

S. 83 - 107:

Buchbeitrag von Prof. Dr. Josef Scherer und RiAG Klaus Fruth,

Danke, ISO!
Über die neue ISO 9001: 2015 (Qualitätsmanagementsystem) zum integrierten, ganzheitlichen Managementsystem mit Governance, Risk und Compliance (GRC)

INHALT

05

Danke, ISO!
Über die neue ISO 9001: 2015 (Qualitätsmanagementsystem) zum integrierten, ganzheitlichen Managementsystem mit Governance, Risk und Compliance (GRC)

Prof. Dr. Josef Scherer
Klaus Fruth

Inhaltsverzeichnis

1. Einführung

Gemäß der ISO-Survey 2013 sollen Ende 2013 über 1,1 Millionen Unternehmen in über 180 Ländern ISO 9001 (Qualitätsmanagementsystem) zertifiziert gewesen sein, wobei der größte Verbreitungsgrad in China, Deutschland und Italien herrsche. Über 50.000 Unternehmen seien nach dem (Automotive) Standard ISO TS 16949 zertifiziert. Viele Unternehmen halten zudem ein entsprechendes Qualitätsmanagementsystem vor, ohne sich zertifizieren zu lassen, da sie in einer Zertifizierung keine angemessene Kosten/Nutzen – Relation (Wertbeitrag) sehen. Seit Mai 2014 existiert ein Draft (Entwurf) International Standard (DIS) mit einer deutschen Übersetzung, Stand August 2014 (E DIN EN 750 9001: 2014 – 08). Auf diese Version wird nachfolgend Bezug genommen.

Für das Jahr 2015 wird der „Final Draft International Standard (FDIS)" erwartet. Unternehmen, die sich neu zertifizieren lassen, müssen mit der neuen Norm bereits mit deren Verabschiedung konform gehen. Bei Rezertifizierungen gibt es eine dreijährige Übergangsphase.

Thesen:

1. Der neue ISO-Standard 9001:2015 (Qualitätsmanagementsystem) weist etliche für (zertifizierungswillige) Unternehmen zu beachtende Änderungen auf.
2. Dieser Standard ist Basis für weitere branchenspezifische Standards (z.B. Automotive (ISO TS 16949) / Luftfahrt (EN 9100 ff.) / Kliniken (EN 15224:2012 / etc.) und wird auf diese Standards ausstrahlen, ebenso auf andere Funktionsbereiche wie z. B. Umweltmanagement (ISO 14001), Arbeitssicherheit (OSHAS), etc.
3. Der Standard weist nach wie vor Schwächen auf. Einige (rudimentäre) Ansätze sind begrüßenswert.
4. Der „risikobasierte und gestärkte prozessorientierte Ansatz" bleibt unverständlich und praxisfern.
5. Die Anforderungen an ein (Qualitäts-)Managementsystem sind vielfältiger, als in diesem neuen Standard auf den ersten Blick dargestellt:

5.1 Zunächst müssen Prozesse, Systeme, Produkte, Dienstleistungen, etc., zwingenden Verpflichtungen (Gesetz/Rechtsprechung) entsprechen (Compliance-orientierter Ansatz und allgemeine Legalitätspflicht).

5.2 Bei freiwillig zu erfüllenden Anforderungen ist die Business Judgment Rule anzuwenden.[1]

1 Aus E DIN EN ISO 9001:2014-08:
(…)
„B.7 QMP 6 – Faktengestützte Entscheidungsfindung
a) **Aussage** – Entscheidungen auf Grundlage der Analyse und Auswertung von Daten und Informationen **werden wahrscheinlich eher zu den gewünschten Ergebnissen führen.**
b) **Begründung** – Entscheidungsfindung kann ein komplexer Prozess sein und weist immer eine gewisse Unsicherheit auf. Häufig umfasst sie sowohl verschiedene Arten und Quellen von Eingaben, als auch deren Interpretation, die subjektiv sein kann. Es ist wichtig, die Zusammenhänge von Ursache und Wirkung sowie die möglichen unbeabsichtigten Folgen zu verstehen. Tatsachen, Nachweise und Datenanalyse führen zu größerer Objektivität und Vertrauen in getroffene Entscheidungen." (…)
Anm. des Verfassers: Ein sicher hilfreicher, aber in dieser Form entbehrlicher Hinweis: Die sog. „Business Judgment Rule" ist bereits gesetzlich verankert, § 93 Abs. 1, S. 2 AktG. Hilfreich wäre der rein deklaratorische Hinweis, dass zunächst alle verpflichtenden (zwingenden) Anforderungen aufgrund des Legalitätsprinzips zu beachten sind. Auf den verbleibenden Spielraum ist sodann die Business Judgment Rule anzuwenden.

6. Der neue Standard für das Qualitätsmanagementsystem versucht, Anforderungen anderer Disziplinen miteinzubeziehen (z. B. Risikomanagement und Compliancemanagement), schafft jedoch wieder nur eine von vielen „Managementinseln" und stellt – trotz neuer Erwähnung der „interested parties" („Stakeholder, am Unternehmen/dessen Leistungen interessierte Gruppen/Organisationen/Personen) – primär und zu eng zumeist nur auf Kundenanforderungen ab.
7. Aktuelle Umfeldentwicklungen und zwingende, rechtliche Anforderungen verlangen einen integrierten Ansatz, der die Komplexität und Kostenbelastung für Unternehmen auflöst (Governance, Risk und Compliance (GRC) als die „gemeinsame Klammer" um die Managementinseln).
8. Die Umrüstung eines Qualitätsmanagement-Systems auf ein ganzheitliches, integriertes Governance (GRC-) System ist einfach und erzielt hohe Wertbeiträge.

Führt die neue ISO 9001 (2015) (Qualitätsmanagement) in Richtung „Integriertes Managementsystem" und „Industrie 4.0"?

Indem der neue ISO-Standard zum Qualitätsmanagement verstärkt auch die sogenannten **„interested parties"** in den Focus rückt und den **risiko- und prozessorientierten Ansatz** betont, lässt sich feststellen, dass ein (kleiner) Schritt in Richtung „Industrie 4.0" gemacht wird: „Industrie 4.0" bedeutet in erster Linie Vernetzung und damit auch die Vernetzung von Prozessen. Bei den Vernetzungsobjekten reicht es nicht, lediglich intern die diversen Abteilungen und extern Kunden und Lieferanten miteinzubeziehen. Vielmehr erfordert eine moderne Vernetzung im Sinne von „Industrie 4.0" auch die Vernetzung mit sonstigen „interested parties" wie z. B. Behörden, Medien, Investoren, Mitarbeiter u.v.m. Insofern ist der neue Ansatz begrüßenswert. **Interessant ist, dass der neue QM-Standard auch eine „Vernetzung" mit anderen „Managementsystemen" wie Risiko- und Compliancemanagement auf den ersten Blick zwar nur implizit, aufgrund rechtlicher Vorgaben jedoch – wenn auch zwischen den Zeilen – explizit fordert.**

2. Exkurs: Was ist eigentlich ein Managementsystem?

Auch für Managementsysteme finden sich, da keine gesetzlich vorgegebenen Definitionen (Legaldefinitionen) existieren, unterschiedliche Bezeichnungen und Ansichten: ERP (Enterprise Resources Planning)-System, IMS (Integriertes Management System), „Führungssystem", etc. Zunächst der Versuch einer Definition von Managementsystem: Ein Managementsystem be-

steht aus formell vorgegebenen (idealerweise vernetzten und interagierenden) überwiegend standardisierten Grundsätzen und Komponenten, wie Aufbau- und Ablauforganisation mit dem Zweck, eine Organisation bei Zielsetzung und Planung, Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen.[2] Bzgl. eines Compliance-Managementsystems ließe sich darauf aufbauend definieren (auch hier gibt es bisher noch keine Legaldefinition, so dass die Definitionsfreiheit viele Vorschläge ermöglicht):

„Aufbau- und Ablauforganisation einer Institution mit interagierenden Komponenten (z. B. Prozessabläufe / Zuständigkeiten, etc.) mit dem Ziel der Sicherstellung von Pflichtenkonformität im Hinblick auf externe und interne verbindliche Vorgaben." Der IDW PS 980:2011 (Compliance-Managementsystem) definiert ein Compliance-Managementsystem folgendermaßen:

„Unter einem Compliance-Managementsystem sind die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele, eingeführten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie gegebenenfalls von Dritten abzielen, d. h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Verstößen (Regelverstößen). Ein CMS im Sinne des IDW-Prüfungsstandards kann sich insbesondere auf Geschäftsbereiche, auf Unternehmensprozesse (z. B. Einkauf) und auf bestimmte Rechtsgebiete (z. B. Kartellrecht) beziehen (abgegrenzte Teilbereiche)."

Anmerkung: Diese Ausführung ist zum einen fraglich, da sie lediglich von Zielen, Grundsätzen (Regelungen) und Maßnahmen spricht, jedoch die tragende Aufbau- und Ablauforganisation nicht erwähnt. Außerdem suggeriert sie möglicherweise den Verantwortlichen in der Praxis, sie hätten Ermessen bei der Frage, worauf sich das Compliance-Managementsystem erstrecken soll/kann. Das ist falsch und widerspricht der Rechtsprechung des Landgerichts München („Neubürger-Urteil"): Aufgrund der Legalitätspflicht sind alle rechtlichen Pflichten einzuhalten. Auch in zunächst nicht primär im Fokus des Interesses bestehenden Bereichen kann sich ein Compliance-Verstoß verheerend auswirken. Vergleiche hierzu die Insolvenz eines Lebensmittelherstellers in Freising aufgrund eines nicht abgestellten Hygienemangels.

2 Zuständigkeiten, Aufgaben- und Verantwortungsbereiche, beispielsweise abgebildet in Organigrammen, Stellenbeschreibungen, etc. sowie Prozessabläufe und Delegationen.
Die E DIN EN ISO 9001:2014 – 08 (Hinweis: Aus wissenschaftlichen Gründen wird hier bei einigen Standards mit den Entwurfsversionen gearbeitet) definiert unter Pkt. 3.4 ein Managementsystem als
„Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Politiken, Ziele und Prozesse zum Erreichen dieser Ziele festzulegen."
Anm. 1: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln, z. B. Qualitätsmanagement (3.30), Finanzmanagement (3.29) oder Umweltmanagement.
Anm. 2: Die Elemente des Managementsystems beinhalten die Struktur der Organisation (3.1), Rollen und Verantwortlichkeiten, Planung sowie Betrieb, Politiken (3.7), Praktiken, Regeln, Überzeugung, Ziele (3.8) und Prozesse (3.12) zum Erreichen dieser Ziele.
Anm. 3: Der Anwendungsbereich (...)"

Wie viele Managementsysteme gibt es im Unternehmen?

In der Praxis herrscht z. T. der Irrglaube vor, es gäbe im Unternehmen Raum für eine beliebige Vielzahl von Managementsystemen. Auch in diversen ISO-Standards wird bei der Definition von „Managementsystem"[3] festgestellt, dass es sich auf alle oder einzelne Themenbereiche (z.B. Compliance, QM, etc.) beziehen kann.

Genährt wird dieser alle Manager und Mitarbeiter abschreckende oder frustrierende Gedanke durch die „Erfindung" ständig neuer „Managementsysteme":

Qualitätsmanagement (ISO 9001 (2015)), für Automotive ISO TS 16949 (2009), für die Luftfahrt EN 9100 ff. (2009), für das Gesundheitswesen EN 15224 (2012), für Hochschulen 9001 i. V. m. ISO 29990 (2010), Umweltmanagement (Entwurf ISO 14000 (2015)), Arbeitssicherheitsmanagement (OHSAS 18001 (2007 – befindet sich in Revision)), IT-Sicherheitsmanagement (ISO 27001 (2008)), GoDV (Grundsätze ordnungsgemäßer Datenverarbeitung und DV-Revision, IT-Audits (IDW FAIT1 / IDW PS 330). - Der jüngst beschlossene Entwurf eines IT-Sicherheitsgesetzes soll bestimmten Branchen und Unternehmen 2 Jahre Zeit geben, um eigene Mindest-Standards zur IT-Sicherheit auf dem (fortschrittlichen) „Stand der Technik" vorzulegen. - Beschwerdemanagement (ISO 10002 (2010)), Risikomanagement (ISO 31000 (2009)), ONR 49000 (2014), COSO II (2004), IDW PS 340 (2000) (Risikofrüherkennungssystem), IDW PS 980 (2011) (Compliance Management), ISO 19600 (2014) (Compliance Management), ONR 192050 (2013) (Compliance) oder andere, z.B. US Sentencing Guidelines (2010), COSO I (2014) (Internal Control-Integrated Framework) und ISO / DIS 34001 (E) (2013) (Security), PAS 99 (2012) (Integriertes Managementsystem), ISO 22301 (2012) (Business Continuity), DCGK (2014) (Governance).

Internes (rechnungslegungsbezogenes) Kontrollsystem (IKS), IDW PS 261 (2012) und COSO I (2014), Interne Revision IDW PS 321 (2010) (vgl. auch DRS (Deutscher Rechnungslegungs-Standard) 20 (2012), DIIR Nr. 2 (2014) (Prüfung des Risikomanagements - mit / ohne Compliance-Risiken? - durch die Revision) und Abschlussprüfung IDW PS 300 (2013) uvm. ergänzen – mit jeweils unterschiedlichem Ansatz und Zielrichtung, aber etlichen Überschneidungen - diese "Systeme".

Nachteile einer Vielzahl einzelner Management-System (Insellösungen)

Ein Unternehmen, das nach und nach das eine oder andere System einführt, produziert damit fast unweigerlich **Insellösungen**, die nicht gelebt werden und deren Daten (sofern überhaupt eingepflegt) aufgrund fehlender Homogenität u.a. den „Segnungen" der **digitalen Datenanalyse nicht zur Verfügung** stehen.

3 **Aus ISO/WD 18386 [Working Draft] (2012) (Compliance-Management-Systems):**
"3.04 management system:
set of interrelated or interacting elements of an organization (3.01) to establish policies (3.07) and objectives (3.08) and processes (3.12) to achieve those objectives.
NOTE 1 to entry: **A management system can address a single discipline or several disciplines.**
NOTE 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc..
NOTE 3 to entry: **The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group or organizations. "**

Vorteile eines integrierten Managementsystems

Jedes lebende Unternehmen hat bereits per se ein Managementsystem: In jedem Unternehmen „bewegt sich was": Es gibt eine **Aufbau- und Ablauforganisation**, einen Regelkreislauf: Oft chaotisch, oft nicht dokumentiert, oft unbewusst, oft schon ganz passabel oder gar *„best practice"*.

Nachfolgend wird versucht, eine Vorgehensweise bzw. einen **modularen Aufbau** darzustellen, der das ganzheitliche Governance - *Management zusammen mit den unverzichtbaren Themen wie Strategie - Management, Organisations-Management, Finanz-Management, Personal-Management,* etc., in **ein einziges (integriertes) Managementsystem** einbettet.[4]

Auditoren, Abschlussprüfern aber auch den **Mitarbeitern** fällt es dadurch leichter, eine **Systematik** zu erkennen und zu sehen, dass sich viele **Themenbereiche überlappen.** Dadurch werden Insellösungen vermieden, **Transparenz** und Übersichtlichkeit jedoch erreicht.

Die Kunst, ein Managementsystem (inkl. IT-Unterstützung) nicht als Fluch, sondern als Segen zu sehen und entsprechend zu nutzen, besteht – wie immer – darin, zunächst Anforderungen und Zielvorgaben aufzustellen, ein erstelltes Konzept zu überprüfen, ob es geeignet ist, die Anforderungen zu erfüllen und die Zielerreichung sicherzustellen. Nach Definition und Sicherstellung der erforderlichen Ressourcen geht es an die Implementierung und Umsetzung im beruflichen Alltag (Wirksamkeit, *„gelebt werden"*) mit Überprüfung anschließender und kontinuierlicher Verbesserung.

Die **Anforderungen** der oben genannten **Standards** (QM, Umwelt, Arbeitssicherheit, Risiko- und Compliance, etc.) **müssen** lediglich als Komponenten **in die grundlegende Architektur und Bestandteile** der rechtssicheren Organisation **(Aufbau- und Ablauforganisation) eingefügt** werden. Positiv ist die großzügige Überschneidung dieser Standards, so dass beispielsweise die Implementierung der Anforderungen an QM, Umwelt- und Arbeitssicherheitsmanagement bereits ca. zwei Drittel des Risikomanagements abdecken mag.[5]

Die Rolle der IT-Lösungen für Managementsysteme

Die IT spielt hier nur eine sekundäre Rolle. Sie fungiert lediglich unterstützend. Insofern ist ein Gesamtkonzept für die unternehmensweite IT-Infrastruktur zu schaffen, das diverse Systeme oder Insellösungen vermeidet. Für große Unternehmen eignet sich beispielsweise SAP, für kleine nicht unbedingt:[6]

Wichtigste Voraussetzung für Mehrwert ist die konsequente „Fütterung" und Pflege des Systems und die einfache Handhabbarkeit für alle Mitarbeiter.

4 Vgl. zum Nachfolgenden: Scherer, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201-211.

5 Vgl. Scherer, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201-211.

6 Hier gibt es diverse Anbieter, bzw. Produkte (auch internetbasierte, mit und ohne Cloud-Lösung und z.T. frei verfügbar), z.B. „Pro Alpha", „AMS", „Navision" etc.

3. Was ist an der ISO 9001 (2015) (Qualitätsmanagement) neu?

Weniger erheblich scheinen die Auswechslung der Begriffe „Dokumente und Aufzeichnungen" durch **„dokumentierte Information"** und der **Wegfall** der Forderung, dass ein **Handbuch** angelegt werden muss. Auch der **Qualitätsmanagement-Beauftragte** fällt weg, indem die Verantwortung dem Top-Management zugeschoben wird. Dies ist nicht unbedingt im Sinne der Geschäftsleitung, da bisher nicht nur Aufgaben, sondern auch Verantwortung delegiert werden konnten. Ob sich diesbezüglich rechtlich in der Praxis etwas ändert steht, dahin.

Wie bereits erwähnt, ist die **Berücksichtigung der „interested parties"** in der ISO 9001 (2015) neu, wenngleich bereits die seit langem bestehende ISO 9004 diesen Ansatz längst im Focus hatte. Auch die „verstärkte" **Prozessorientierung** und die **Einbeziehung** von Risikomanagement ist neu.[7]

Neu bei dieser Norm ist auch, dass nicht mehr nur von Produkten, sondern **auch von Dienstleistungen** gesprochen und im Kontext weiterer ISO-Normen versucht wird, einen einheitlichen Aufbau zu berücksichtigen. Diese als **„high-level-structure"**[8] bezeichnete Un-

7 **Aus E DIN EN ISO 9001:2014-08:**

(…)

„Änderungen – Gegenüber DIN EN ISO 9001:2008-12 und DIN EN ISO 9001 Berichtigung 1:2009-12 werden folgende Änderungen vorgenommen:

a) **die Norm wurde grundlegend überarbeitet.** Eine Übersicht der wesentlichen Änderungen findet sich in Anhang A;

b) die Abschnittsreihenfolge wurde verändert, damit sie mit der in den ISO-Direktiven festgelegten Grundstruktur für Managementsystemnormen **(„High Level Structure"**) übereinstimmt."

c) **„Neu** sind in diesem Zusammenhang vor allem die folgenden Punkte:
- es wurde ein Abschnitt 4 zur Bestimmung des Kontexts der Organisation eingefügt, der die **Bestimmung der interessierten Parteien und ihrer für das Qualitätsmanagementsystem relevanten Anforderungen** umfasst; - es wurde der **„risikobasierte Ansatz"** hervorgehoben (siehe vor allem 6.1); - **„dokumentierte Information"** wurde als neuere Sammelbegriff der bisher bekannten „dokumentierten Verfahren" und „Aufzeichnungen" eingeführt, die Forderung nach einem **Qualitätsmanagementhandbuch** ist entfallen;

d) anstelle von „Produkten", was bislang „Dienstleistungen" umfasste, wird nun ausdrücklich **von „Produkten und Dienstleistungen" gesprochen,** um die Bedeutung der Norm für den Dienstleistungssektor hervorzuheben;

e) die für die Anwendung der ISO 9001 relevanten Begriffe und Definitionen aus der ISO 9000 wurden in das Dokument übernommen;

f) **der prozessorientierte Ansatz wurde gestärkt** und neue Anforderungen wurden formuliert (siehe vor allem 4.4);" (…).

8 **Aus E DIN EN ISO 9001:2014-08:**

(…)

„Nationales Vorwort – Dieses Dokument (prEN ISO 9001:2014) beinhaltet die deutsche Übersetzung des internationalen Norm-Entwurfes ISO/DIS 9001:2014, der vom technischen Komitee ISO/TC 176, Quality management und quality assurance, Unterkomitee SC 2, Quality sytems (Sekretariat: BSI, Vereinigtes Königreich) erarbeitet wurde."

„Dieser Text wurde mithilfe **der von ISO eingeführten Grundstruktur für Managementsystemnormen („High Level Structure")** erarbeitet. **Die Grundstruktur,** die in Anhang SL, Anlage 2 der ISO/IEC-Direktives, Part 1, consolidated ISO Supplement, 2014, angegeben ist, **enthält neben der Struktur auch einheitlichen Basistext, gemeinsame Benennungen und Basisdefinitionen für den Gebrauch in Managementsystemnormen.** Die deutsche Übersetzung der Grundstruktur wurde zwischen Deutschland, Österreich und der Schweiz abgestimmt und gilt für alle Übersetzungen von Managementsystemnormen die vollständig oder teilweise der ISO-Grundstruktur folgen." (…).

terteilung der Standards soll gewährleisten, dass die diversen Standards leichter verstanden werden. Auch künftig **einheitliche Definitionen** in den diversen Standards sollen dies fördern.

Ob der **Aufbau mit den 10 Unterpunkten:**
1. Anwendungsbereich, **2.** Normative Verweisungen, **3.** Begriffe, **4.** Kontext der Organisation, **5.** Führung, **6**. Planung für das Qualitätsmanagementsystem, **7.** Unterstützung, **8.** Betrieb, **9.** Bewertung der Leistung, **10.** Verbesserung
eine tatsächlich optimale Struktur darstellt, ist zu diskutieren, vgl. die Empfehlung eines auch mit COSO und IDW, etc. harmonisierten Standard-Aufbaus in Scherer / Fruth (Hrsg.) Governance-Management, Band II (Audit), (2015).
Insbesondere werden die Phasen P/D/C/A mit Inhalten vermischt, wobei übersehen wird, dass sich die P/D/C/A-Phasen auf sämtliche Inhalte zu erstrecken haben.
Auch ist fraglich, ob die Ausdrucksweise des neuen Standards für jeden verständlich und umsetzbar gestaltet wurde.

4. Was fehlt noch?

Beim neuen QM-Standard fehlt meines Erachtens - wie bei vielen anderen Standards auch - zunächst die Erklärung, ob diese Norm den „Anerkannten Stand von Wissenschaft und Praxis" widerspiegelt oder den „Stand der Technik" oder den „Neuesten Stand von Wissenschaft und Technik". Auch über die Rechtsqualität eines Standards und die Art des Zusammenkommens wird nichts ausgeführt, was über Verweisungen auf ein allgemeines ISO-Werk möglich wäre. [9]

Diese Fragen werden ausführlich in einer demnächst erscheinenden Sonderveröffentlichung des Berufsverbandes der Compliance-Manager (BCM) e. V. behandelt.

Die „gestärkte" **Prozessorientierung** könnte weiterhin auch noch dahingehend ergänzt werden, dass künftig nicht funktions-, sondern auch prozessorientiert auditiert werden soll/muss, da in diesem Falle die Schnittstellen funktionsübergreifend deutlich heraustreten würden.

Viel wichtiger wäre es m. E. jedoch, klar auszudrücken, was der neue QM-Standard unter dem neuen, „gestärkten" prozessorientierten Ansatz versteht:[10]

9 Vgl. hierzu 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 (2015) Compliance-Managementsystem", Corporate Compliance Zeitschrift 2015, S. 9 ff.

10 **Aus E DIN EN ISO 9001:2014-08**
(. .)
„0.3 Prozessorientierter Ansatz
Konsistente und vorhersehbare Ergebnisse werden wirksamer und effizienter erzielt, wenn **Tätigkeiten** als miteinander in Wechselbeziehung stehende **Prozesse verstanden sowie geleitet und gelenkt werden**, die als **zusammenhängendes System** funktionieren. **Diese Internationale Norm fördert die Wahl eines prozessorientierten Ansatzes** für die Entwicklung, Verwirklichung und Verbesserung der Wirksamkeit eines Qualitätsmanagementsystems, **um die Kundenzufriedenheit** durch die Erfüllung der Kundenanforderungen **zu erhöhen.** In 4.4 der vorliegenden Internationalen Norm sind spezifische Anforderungen enthalten, die bei der Einführung eines prozessorientierten Ansatzes als unverzichtbar gelten.

Der prozessorientierte Ansatz beruht auf einer systematischen Festlegung und Steuerung von Prozessen und deren Wechselwirkungen, so dass die angestrebten **Ergebnisse mit der Qualitätspolitik, sonstige Anforderungen an Prozesse** und der strategischen Ausrichtung der Organisation übereinstimmen. **Die Steuerung der Prozesse und des Systems als Ganzes** kann **durch** die Methode „Planen-Durchführen-Prüfen-Handeln" (en: **Plan-Do-Check-Act, PDCA**) (siehe 0.4) erreicht werden, deren Hauptaugenmerk auf **„risikobasiertem Denken"** liegt, wodurch unerwünschte Ergebnisse (siehe 0.5) verhindert werden sollen.".

Aus E DIN EN ISO 9001:2014-08:
„Kommt der prozessorientierte Ansatz innerhalb eines Qualitätsmanagementsystems zum Einsatz, **so stellt er Folgendes sicher:**
a) Verstehen der Anforderungen und deren fortlaufende Einhaltung;
b) Berücksichtigung der Prozesse aus Sicht der Wertschöpfung;
c) Erreichen einer wirksamen Prozessleistung;
d) Verbesserung von Prozessen basierend auf der Beurteilung von Daten und Informationen."

Aus E DIN EN ISO 9001:2014-08:
(…)„B.5 QMP 4 – Prozessorientierter Ansatz
a) **Aussage:** Konsistente und vorhersehbare Ergebnisse werden wirksamer und effizienter erzielt, **wenn Tätigkeiten als miteinander in Wechselbeziehung stehende Prozesse**, die als kohärentes System funktionieren, verstanden, geleitet und gelenkt werden.
b) **Begründung**: Das Qualitätsmanagementsystem setzt sich aus miteinander in Wechselbeziehung stehenden Prozessen zusammen. Das Verständnis, wie Ergebnisse durch dieses System erzielt werden, einschließlich all seiner Prozesse, Ressourcen, Lenkungen und Wechselwirkungen, ermöglicht einer Organisation, ihre Leistung zu optimieren." (. .):

Der neue QM-Standard definiert Prozesse als *„Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse (3.46) umwandelt."* ***„Prozessmanagement" wird nicht definiert!*** *Anders bei Buhl*[11]*, der - sich wesentlich näher am „Stand der Technik" orientierend (fortschrittlicher) – wertorientiertes Prozessmanagement* beschreibt:

*„Dabei ist ein **Prozess** ein ereignisgesteuerter, inhaltlich abgeschlossener, zeitlicher und sachlogischer Ablauf von Aufgabendurchführungen, in denen unter Nutzung von Ressourcen betriebliche Leistungen erstellt werden oder die Leistungserstellung koordiniert wird. Das **Prozessmanagement** umfasst die Planung, Steuerung, Kontrolle und Weiterentwicklung von Prozessen typischerweise mittels einer zyklischen Abfolge mehrerer Teilaufgaben:(1) Identifikation, Definition und Modellierung, (2) Implementierung und Ausführung, (3) Überwachung und Steuerung sowie (4) Kontinuierliche Weiterentwicklung. Die Begriffe **Geschäftsprozess** und **Geschäftsprozessmanagement** sind sprachliche Spezialisierungen, die den direkten Bezug zur betrieblichen Leistungserstellung und die Abgrenzung von anderen Prozesstypen (z. B. Hilfs- oder Führungsprozessen) hervorheben.".*

11 Vgl. Buhl / Röglinger / Stöckl / Braunwarth, Wertorientierung im Prozessmanagement- Forschungslücke und Beitrag zu betriebswirtschaftlich fundierten Prozessmanagement - Entscheidungen, 2011, F/M - Kernkompetenzzentrum Finanz- & Informationsmanagement Universität Augsburg).

Exkurs: Von „Wertorientierter Unternehmensführung“ zu „Wertorientiertem Prozessmanagement“:

„Um im betriebswirtschaftlichen Sinn „wertorientiert“ zu sein, muss ein Steuerungskonzept (…) folgende Anforderungen erfüllen: [12]

1 ***Planung und Kontrolle von Wertbeiträgen:*** *Entscheidungsalternativen müssen einerseits ex ante hinsichtlich ihres erwarteten Beitrags zur Unternehmenswertsteigerung bewertet werden* ***(Planung)****. Andererseits muss ex post überprüfbar sein, ob der geplante Wertbeitrag tatsächlich realisiert wurde* ***(Kontrolle)****.*

2 ***Zukunftsorientierung, Risikoadäquanz und Zahlungsstromorientierung: Planungs- und Kontrollwerte müssen*** *den Zeitwert des Geldes und die* ***Risikoeinstellung*** *der involvierten* ***Entscheidungsträger widerspiegeln*** *sowie auf* ***Zahlungsstrom größen basieren.***

3 ***Zielbezug zur langfristigen, nachhaltigen (Gesamt-) Unternehmenswertsteigerung:*** *Planungs- bzw. Kontrollwerte müssen in sachlogischem Z****usammenhang mit den Unternehmenszielen****, insbesondere der langfristigen, nachhaltigen Unternehmenswertsteigerung, stehen.*

4 ***Anreizverträglichkeit und Kommunikationsfähigkeit:*** *Planungs- und Kontrollwerte werden i. d. R. zur verhaltenssteuernden Leistungsbeurteilung verwendet. Dazu muss ein Steuerungskonzept anreizverträglich und kommunikationsfähig sein. Anreizverträglichkeit bedeutet, dass sich ein* ***Steuerungskonzept für den Einsatz im Rahmen einer leistungsorientieren Entlohnung eignet****, also z. B. manipulationsresistent ist. Kommunikationsfähigkeit ist dann gegeben, wenn* ***die verwendeten Kennzahlen für Stakeholder verständlich sind*** *und eine transparente Grundlage zur Ermittlung der Entlohnungshöhe bilden.“*

Anmerkung des Verfassers: Die Themengebiete / Bereiche / Prozessabläufe / „Managementsysteme“ eines Unternehmens könnten und sollten mit entsprechenden **Wertbeitrags-Kennzahlen** (vgl. z.B. SAM-Sustainability-Report von Siemens) ausgestattet werden. Mit diesen Kennzahlen mag unter Berücksichtigung der Vorgaben der Entscheidungsträger (Shareholder / Aufsichtsgremium / Stakeholder und der Unternehmensvision) geplant und die Zielerreichung kontrolliert werden.
Die Kennzahlen ließen sich auch für ein Anreizsystem verwenden und auch als Basis für Transparenz, sowie in- und externe Kommunikation dienen.

Buhl stellt in seiner (äußerst lesenswerten) Abhandlung dar, dass sich seit Rappaport

12 Zitate aus Buhl / Röglinger / Stöckl / Braunwarth, Wertorientierung im Prozessmanagement- Forschungslücke und Beitrag zu betriebswirtschaftlich fundierten Prozessmanagement –Entscheidungen, 2011, F/M – Kernkompetenzzentrum Finanz- & Informationsmanagement Universität Augsburg

(1986) zwar viele wissenschaftliche Antworten mit ***wertorientierter Unternehmensführung*** beschäftigen und sich die Wertorientierung als ***„Leitbegriff der Unternehmensführung grundsätzlich durchgesetzt“*** habe.

Im Bereich „Prozessmanagement“ dagegen haben nach Buhl im Jahr 2011, zum Zeitpunkt des Abschlusses seiner Untersuchung, die **Erkenntnisse der wertorientierten Unternehmensführung kaum Einzug** gehalten. Lediglich elf (!) einschlägige Beiträge fand er, wobei lediglich vom Brocke et al. mit zwei Aufsätzen ***„value-oriented process modelling“ (2009)*** und ***„Wertorientiertes Prozessmanagement: State-of-the-Art und zukünftiger Forschungsbedarf“ (2010)*** zufriedenstellten.

Buhl stellt damit eine noch **erhebliche Forschungslücke** u. a. bzgl. der Integration von Ertrags- und Risikogrößen zu Wertbeiträgen, der Ex-post-Kontrolle von Prozessmanagemententscheidungen und **des expliziten Zielbezuges auf den langfristigen, nachhaltigen Unternehmenswert** als Spitzenkennzahl fest.

Die Wichtigkeit des Themas wird bestätigt durch die geplante **Neufassung der ISO 9001:2015 (Qualitätsmanagement) für 2015**: Dort wird an vielen Stellen der **risikobasierte Ansatz** betont und der **Prozessansatz** gegenüber der Version 2008 erheblich verstärkt:

Zu ermitteln sind künftig Inputs, Outputs, Wechselwirkungen, Leistungskennzahlen, Verantwortlichkeiten, Chancen und Risiken. Ein explizierter Bezug auf die Anforderungen des „wertorientierten Prozessmanagements“ fehlt jedoch!

Sowohl bei ***Buhl*** als auch in entsprechenden ISO-Standards fehlt m. E. darüber hinaus die systematische Erarbeitung von Pflicht-Anforderungen an Prozesse, vgl. dazu unten „Anforderungen an Produkte, Leistungen, Prozesse, Systeme“:

Wie im Ansatz „Complianceorientiertes Governance-Management“[13] generell ausgeführt, sollten zunächst die

- **Obligatorischen Anforderungen mit Sanktionsrisiken**
  (effektiv, qualitativ, fristgerecht, sicher, rechtssicher (compliant), dem „Anerkannten Stand von Wissenschaft und Praxis“ entsprechend, effizient, gewissenhaft und ordentlich sowie aus der Wertorientierung : risikoorientiert) erfüllt werden. Danach sind – bei Anwendung der Business Judgment Rule – die

- **fakultativen Anforderungen des wertorientierten Prozessmanagements**
  (wertbeitrags-, nachhaltigkeits-, zukunfts-, chancen-, zahlungsstromorientiert, messbar, transparent und kommunikationsfähig, anreiz- und sanktionsfähig) „als Kür“ zu erfüllen.

Wieder zeigt sich, dass die **BWL ohne Berücksichtigung von Recht (§§) etc. nicht** unbedingt ganzheitlich und **komplett** die verpflichtenden Anforderungen abbilden kann / mag: So wird

13 Vgl. Scherer / Fruth (Hrsg.), Governance-Management Band I, 2014.

in Lehre und Beratung seit Jahren das **Prozessdreieck der Ablauforganisation** mit lediglich den drei Anforderungen Kosten (effizient), Zeit (fristgerecht) und Qualität vor- und nachgebetet. Und die **ISO 9001 (2015)** stellt auch in der neuen Version überwiegend Qualität und Service als Kundenanforderungen bzw. neue (oder nicht neu, vgl. ISO 9004) Anforderungen der „interested parties" dar. Mayrhofer14 fordert daher zu recht, das Prozess-Dreieck in ein **Vieleck („Prozess-Polygon", („Prozess-Pentagramm" Mayrhofer))** zu transformieren, um den heutigen Governance-Anforderungen u. a. mit Risiko- und Compliance-Management, gerecht zu werden.

Nur, wenn zunächst die von Prozessgestaltungen zu erfüllenden Anforderungen vollständig bekannt sind und um fakultative, aber gewünschte Anforderungen / Ziele (z. B. Wertorientierung oder Akzeptanz beim Prozesseigner) ergänzt werden, lassen sich diese unter Berücksichtigung ihrer Wechselwirkungen integrativ beachten. Erst in diesem Stadium ist es angezeigt, unter einer Vielzahl von Tools und Methoden aus dem Prozessmanagement (Six Sigma, TQM, Lean Management, Prozesskostenrechnung, usability engineering, Balanced Scorecard, Reifegradmodelle, etc.) die angemessenen (erforderlich und ausreichend: geeignet zur Zielerreichung) auszuwählen und entsprechend einzusetzen.

Wenn dadurch „das Richtige richtig getan" wird, sind nicht nur wirtschaftliche Ziele zu erreichen, sondern auch **Haftungsgefahren für Prozesseigner, -modellierer und Geschäftsleitung reduziert.** Der dafür erforderliche angemessene **Reifegrad** lässt sich beispielsweise mit einem **Scoring-Modell** berechnen und einer Excel-basierten **„Prozessspinne"**, an deren Eckpunkte sich die diversen Anforderungen finden, visualisieren. Eine mathematische Formel zur Berechnung des Wertes des „process-capital" (analog der „Saarbrücker Formel" für das human capital) und **des Wertbeitrages des „Compliance-orientierten Prozessmanagements"** steht wohl noch aus.

Ende Exkurs

Auch die **generellen Anforderungen an Prozesse / (Management-) Systeme / Produkte / Dienst- oder Werkleistungen / Funktionen** / etc. werden in neuem QM-Standard nicht genannt. Sie gehen weit über Qualitätsanforderungen hinaus[15] Prozesse, Produkte, Management-Systeme, etc. müssen sicher, rechtssicher, effektiv, qualitativ, effizient, risikogesteuert und sollten wertorientiert, etc. sein.

14 Quelle: RiskNet https://www.risknet.de/themen/risknews/governance-prozess-pentagramm/a5a0dcb3f503fe9264b-352f336b845f7/ (letzter Zugriff: 25.03.2015).

15 Vgl. Scherer / Fruth (Hrsg.), Governance-Management, Band I, 2014, Kap. 1.

Anforderung:	Folge bei Fehlern:
✓ Effektiv (Ziel wird erreicht)	Unmöglichkeit (§§)
✓ Qualitativ	Mängelhaftung (§§)
✓ Fristgerecht	Verzug (§§)
✓ Sicher	Nebenpflichtverletzung § 823 BGB, § 280 BGB (§§)
✓ Rechtssicher (compliant)	Vielfältige Sanktionen (§§)
✓ Dem „Anerkannten Stand von Wissenschaft und Praxis" entsprechend (Standards)	Mängelhaftung / Sonstige Haftung bei Schäden / Beweislastumkehr (§§)
✓ Effizient (wirtschaftlich)	Liquiditätsprobleme / Ergebnisprobleme (§§) (Haftung für finanzielle Einbußen, Krisen- und Insolvenzverursachung, etc.)
✓ Gewissenhaft	Fehlende Gewissenhaftigkeit der Geschäftsführung § 43 GmbHG, § 93 AktG.: Pflichtverstoß und persönliche Haftung (§§)
✓ Wertorientiert:	
Wertbeitragsorientiert (Planung u. Messung von Wertbeiträgen)	
Nachhaltig und zukunftsorientiert	Teils nur suboptimales Wirtschaften
Chancen- und risikoorientiert	**Durchschnittliche Lebensdauer von Unternehmen: 12 Jahre !**
Messbar	
Transparent und kommunikationsfähig	Teils Pflichtverstoß (z. B. fehlende Risikoorientiertheit) (§§)
Zahlungsstromorientiert	
Anreizfähig und sanktionsfähig	
…	

Außerdem fehlt in der neuen ISO Norm eine deutliche Erwähnung eines erheblichen Grundsatzes an einführender, exponierter Stelle, nämlich dass „das Agieren im Rahmen dieses Standards durch rechtliche Rahmenbedingungen eingeschränkt ist".

In verstreuten Abschnitten finden sich jedoch zahlreiche Hinweise, dass beispielsweise Produkte und Dienstleistungen **rechtliche (gesetzliche und behördliche) Anforderungen zu beachten** haben.[16] Dass jedoch das gesamte unternehmerische Agieren aufgrund des Legalitätsprinzips in den aktuellen rechtlichen Rahmenbedingungen zu erfolgen hat, wird – wie in den ersten anderen Standards auch - nicht herausgestellt, führt bei Missachtung jedoch zu empfindlichen Sanktionen.

16 **Aus E DIN EN ISO 9001:2014-08:**
(…)
„Einleitung
0.1 Allgemeines zum Qualitätsmanagementsystem"
„Diese Internationale Norm kann von internen und externen Parteien verwendet werden, um die Fähigkeit der Organisation zur fortlaufenden Erfüllung der Anforderungen der Kunden sowie der gesetzlichen und behördlichen Anforderungen, die auf die von ihr bereitgestellten Produkte und Dienstleistungen anwendbar sind, sowie der Anforderungen der Organisation selbst und deren Ziel, die Kundenzufriedenheit zu verbessern, **zu bewerten"** (…)

Aus E DIN EN ISO 9001:2014-08:
(…)
„1 Anwendungsbereich
Diese Internationale Norm **legt Anforderungen an ein Qualitätsmanagementsystem** fest, wenn eine Organisation
a) ihre Fähigkeit darlegen muss, fortlaufend **Produkte oder Dienstleistungen** bereitstellen zu können, **die die Anforderungen der Kunden** und **die zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen**, und
b) danach strebt, die Kundenzufriedenheit durch wirksame Anwendung des Systems zu erhöhen, einschließlich der Prozesse zur fortlaufenden Verbesserung des Systems **und der Zusicherung der Einhaltung von Anforderungen der Kunden** (Anm. des Verfassers: Sehr aktuell! In der Praxis fordern derzeit sehr viele Unternehmen von ihren Geschäftspartnern und sogar wiederum deren Lieferanten die Zusicherung von **Compliance** und auditieren sogar vor Ort die Einhaltung der Versprechen) und von **zutreffenden gesetzlichen und behördlichen Anforderungen.**
ANMERKUNG 2 Gesetzliche und behördliche Anforderungen können auch als rechtliche Anforderungen bezeichnet werden." (…)

Aus E DIN EN ISO 9001:2014-08:
(…)
„5.1.2 Kundenorientierung
Die oberste Leitung muss in Bezug auf die Kundenorientierung Führung und Verpflichtung zeigen, indem sie sicherstellt, dass
a) die Anforderungen des Kunden und **geltende gesetzliche sowie behördliche Anforderungen bestimmt und erfüllt werden,**
b) die Risiken und Chancen, die die Konformität von Produkten und Dienstleistungen beeinflussen können, sowie die Fähigkeit zur Verbesserung der Kundenzufriedenheit bestimmt und berücksichtigt werden,
c) der Fokus der fortlaufenden Bereitstellung von Produkten und Dienstleistungen, die die **Anforderungen der Kunden** und die **zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen,** aufrechterhalten wird,
d) der Fokus der Verbesserung der Kundenzufriedenheit aufrechterhalten wird." (…)

Aus E DIN EN ISO 9001:2014-08:
(…)
„8.2.3 Überprüfung von Anforderungen in Bezug auf Produkte und Dienstleistungen
Die Organisation **muss**, soweit zutreffend, Folgendes überprüfen:
a) die vom Kunden festgelegten Anforderung einschließlich der Anforderungen hinsichtlich der Lieferung und der Tätigkeiten nach der Lieferung;
b) die vom Kunden nicht angegebenen Anforderungen, die jedoch für den festgelegten oder den beabsichtigten Gebrauch durch den Kunden, soweit bekannt, notwendig sind;
c) **weitere gesetzliche und behördliche Anforderungen, die für die Produkte und Dienstleistungen gelten;"** (…).

Bei der Nennung von **Risikomanagement-Bestandteilen** fehlt ein angemessener, zielführender Hinweis, wie der QM-Standard sich zur Risikomanagement-Norm ISO 31000 verhalten soll.[17]

17 **Aus E DIN EN ISO 9001:2014-08:**
(…)
„0.5 „Risikobasiertes Denken"
Risiko ist die Auswirkung von Unsicherheit auf ein erwartetes Ergebnis und das Konzept des risikobasierten Denkens **war schon immer in ISO 9001** inbegriffen. Die vorliegende Internationale Norm bringt das risikobasierte Denken **noch deutlicher zum Ausdruck** und bindet es in die Anforderungen an die Einführung, Verwirklichung, Aufrechterhaltung und fortlaufende Verbesserung des Qualitätsmanagementsystems ein. **Organisationen können sich für einen umfangreicheren risikobasierten Ansatz** als den in der vorliegenden Internationalen Norm enthaltenen **entscheiden; ISO 31000** enthält Leitlinien zum formellen Risikomanagement, **das in bestimmten Kontexten von Organisationen geeignet sein kann.**
Nicht alle Prozesse des Qualitätsmanagementsystems verkörpern den gleichen Risikograd bezüglich der Fähigkeit der Organisation, **ihre Ziele zu erreichen,** und Konsequenzen aus den Nichtkonformitäten von Prozessen, Produkten, Dienstleistungen oder des Systems sind nicht in allen Organisationen die gleichen. In einigen Organisationen kann die Lieferung nichtkonformer Produkte und die Erbringung nichtkonformer Dienstleistungen eine **geringfügige Unannehmlichkeit** für Kunden bedeuten; in anderen Organisationen kann dies jedoch **weitreichende und schwerwiegende Konsequenzen** mit sich bringen. Bei der Festlegung der Strenge und des Formalitätsgrads, die/der zur Planung und Lenkung des Qualitätsmanagementsystems, der Teilprozesse und der Tätigkeiten benötigt wird, **wird das „risikobasierte Denken" deshalb in qualitativem Sinne (und, je nach Kontext der Organisation, auch in quantitativem Sinne)** berücksichtigt." (…)

Aus E DIN EN ISO 9001:2014-08:
(…)
„4.4 Qualitätsmanagementsystem und dessen Prozesse (…)
Die Organisation muss die Prozesse bestimmen, die für das Qualitätsmanagementsystem benötigt werden, sowie deren Anwendung innerhalb der Organisation festlegen, und muss außerdem Folgendes bestimmen:
f) (…)
die Risiken und Chancen in Übereinstimmung mit den Anforderungen nach 6.1 und die Planung und Umsetzung geeigneter Maßnahmen, um diese zu berücksichtigen;(…)

Aus E DIN EN ISO 9001:2014-08:
6.1.2 Die Organisation **muss planen:**
Anm. d. Verf.: Sehr verwirrend! Muss die Organisation nur „planen" oder auch umsetzen (implementieren / leben), überwachen, verbessern (nur „Plan" oder auch „Do, Check, Act")? Antwort: Natürlich auch Do/Check/Act!

a) Maßnahmen zum **Umgang mit Risiken und Chancen,**
b) **wie**
1) **die Maßnahmen in die Qualitätsmanagementsystem-Prozesse der Organisation integriert und dort umgesetzt werden** (siehe 4.4),
2) die Wirksamkeit der Maßnahmen bewertet wird.
Maßnahmen zum Umgang mit Risiken und Chancen müssen proportional zum möglichen Einfluss auf die Konformität von Produkten und Dienstleistungen sein.
ANMERKUNG **Zu den Möglichkeiten zum Umgang mit Risiken und Chancen** kann Folgendes zählen: Vermeiden von Risiken, ein Risiko auf sich zu nehmen, um eine Chance wahrzunehmen, Beseitigen der Risikoquelle, Ändern der Wahrscheinlichkeit oder der Konsequenzen, Risikoteilung oder Beibehaltung des Risikos durch verantwortungsbewusste Entscheidung." (…)

Aus E DIN EN ISO 9001:2014-08:
(…)
6 **Planung für das Qualitätsmanagementsystem**
6.1 Maßnahmen zum Umgang mit Risiken und Chancen
6.1.1 Bei Planungen für das Qualitätsmanagementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie **die Risiken und Chancen bestimmen**, die betrachtet werden müssen, um
a) sicherzustellen, dass das Qualitätsmanagementsystem seine beabsichtigten Ergebnisse erzielen kann, (…).

Zu den „Risiken" gehören zwingend auch Compliance-Risiken, da es keinen sachlichen Grund gibt, ein so großes Feld mit potenziell existenzbedrohenden Risiken „auszuklammern". Dies wäre zudem auch pflichtwidrig i. S. der §§ 43 GmbHG, 93,107 AktG, vgl. LG München („Neubürger-Urteil"). Wenn also „Maßnahmen zum Umgang mit Risiken und Chancen" gefordert werden, muss dies auch Compliance-Risiken umfassen.

Geradezu paradox ist die Forderung nach einem risikobasiertem Ansatz einerseits und andererseits die falsche und „gefährliche" Aussage: **„Obwohl Risiken und Chancen bestimmt und behandelt werden müssen, gibt es keine Anforderung für ein formelles Risikomanagement oder einen dokumentierten Risikomanagementprozess. (…)"**
Diese Aussage ist wohl der Angst vor der Konkurrenz der Risikomanagement-Standards oder vor der für Qualitätsmanagement völlig neuen Materie, insbesondere, wenn man Compliance-Risiken miteinbezieht, geschuldet.[18]

5. Die Lösung: Ein integriertes (GRC-) Managementsystem

Da nahezu alle Standards (ISO / COSO / IDW / …) für …-Managementsysteme auf einen einheitlichen, zum großen Teil redundanten Aufbau und Inhalt komprimiert werden können, sollte die Praxis die Gelegenheit nutzen, das vorhandene (Qualitäts-)Managementsystem auf ein integriertes, ganzheitliches Führungssystem „umzurüsten", das nicht nur einzelne Themenfelder, sondern die Anforderungen der Grundsätze ordnungsgemäßer Unternehmensführung (GoU) und -überwachung (GoÜ) (Corporate Governance) insgesamt einzuhalten ermöglicht. Der Aufwand ist überschaubar. Nachfolgend ein Beispiel:[19]

Die Anreicherung von aufbau- und ablauforganisatorischen Komponenten (z.B. eines Prozessablaufs) mit Anforderungen diverser Standards am Beispiel des Angebotsmanagementprozesses im Vertrieb.

18 **Aus E DIN EN ISO 9001:2014-08**:
(…)
„A.4 Risikobasierter Ansatz
Diese Internationale Norm **fordert von der Organisation, dass sie ihren Kontext versteht** (siehe 4.1) **und die Risiken und Chancen** (siehe 6.1), **die zu berücksichtigen sind, bestimmt.**
Es ist eine Kernaufgabe eines Qualitätsmanagementsystems, als vorbeugendes Instrument zu wirken. Aus diesem Grund enthält diese Internationale Norm keinen separaten Abschnitt oder Unterabschnitt mit der Überschrift „Vorbeugende Maßnahmen". Das Konzept der vorbeugenden Maßnahmen wird durch einen risikobasierten Ansatz bei der Formulierung von Anforderungen des Qualitätsmanagementsystems zum Ausdruck gebracht.
Der risikobasierte Ansatz bei der Erarbeitung dieser Internationalen Norm hat eine teilweise Reduzierung der vorschreibenden Anforderungen und deren Ersatz durch leistungsbasierte Anforderungen ermöglicht.
Obwohl Risiken und Chancen bestimmt und behandelt werden müssen, gibt es keine Anforderung für ein formelles Risikomanagement oder einen dokumentierten Risikomanagementprozess." (…).

19 Zum „Gesamtbild" vgl. Scherer / Fruth (Hrsg.), Governance-Management, Band II (Audit), 2015

Der **Einbau** von Risiko- oder Compliance - Komponenten **in vorhandene Prozessabläufe** ist sehr schön **am Beispiel der Kundenprüfung:** Identitäts-, Bonitäts- und Legalitätsprüfung (z.B. Außenwirtschaftskontrolle und Geldwäsche beim Kunden) als zeitnaher Prozessschritt im Angebotsprozess darzustellen, der nicht nur Gefahren reduziert und persönliche Haftung vermeidet[20], sondern auch zeigt, dass Governance mit Risiko- und Compliance - Management hilft, viel Geld zu sparen:

Angebotsmanagement als Teil des Vertriebsprozesses

Der Vertriebsprozess ist in vielen Unternehmen bereits – oft sogar dokumentiert – aufgrund der Prozessdokumentationsobliegenheit aus dem Qualitäts- und Prozessmanagement vorhanden:

Dieser Vertriebsprozess wird nun – auch – mit Risiko-, Chancen- und Complianceelementen angereichert und damit optimiert. Dazu ist bei allen Prozessschritten nach Risiko-, Chancen- und Complianceanforderungen mittels Checkliste, Brainstorming, Interviews, etc. (Eruierungsphase) zu suchen. Diese sind anschließend zu bewerten (Evaluation) und bei Überschreitung der von der Geschäftsleitung festgelegten Wesentlichkeitsgrenze als Prozessschritte oder Kontrollpunkte in den Prozessablauf einzubauen. Beispielhaft wird nun der Angebotsmanagementprozess als Teil des Vertriebsprozesses untersucht:

Der Einbau des Prozessschrittes „Kundenprüfung" in den Angebotsmanagementprozess

Die **Identitätsprüfung** klärt die Frage, wer tatsächlich Vertragspartner ist (Hans Maier oder Hans Maier Bau-GmbH oder Hans Maier Holding GmbH & Co. KG oder Hans Maier Bauleistungen AG: Häufig wird nur mit „Fa. Maier" oder gar mittels unterschiedlicher Briefbögen kommuniziert: Ansprüche gegen den Vertragspartner wären wegen der ungeklärten Frage, wer tatsächlich Partner ist, kaum durchsetzbar). Auch die **Vertretungsmacht** der für den Vertragspartner handelnden Person kann an dieser Stelle gleich ebenso geklärt werden: Ist die für den Vertragspartner handelnde Person überhaupt ausreichend legitimiert (Prokura, Handlungs- oder Einzelvollmacht)? Die **Bonitätsprüfung** zeigt, ob die Wahrscheinlichkeit, auch an das Entgelt zu kommen, hoch genug ist, um ein Angebot stellen zu wollen (z.B., wenn zwar die Zahlen der anfragenden GmbH gut sind, diese GmbH aber Teil eines kriselnden Konzerns ist: Infektionsgefahr!). Die **Legalitätsprüfung** (Außenwirtschaftsgesetz, Geldwäsche, etc.) gibt Auskunft, ob ein Angebot überhaupt abgegeben werden darf, usw. In der **Praxis fehlen** entsprechende **Prüfschritte häufig** völlig, werden oft nur bei Neukunden durchgeführt **oder** befinden sich im Prozessablauf **an ungünstiger Stelle** (z.B. erst nach Durchführung

20 Risikomanagement und Compliance: Nach BGH **haftet ein Geschäftsführer,** der pflichtwidrig eine **Bonitätsprüfung nicht installiert** hat (Organisationspflichtverletzung), **persönlich** für den der Gesellschaft durch den Forderungsausfall entstandenen Schaden, BGH, WM 1981, S. 440.

von technischer / kaufmännischer Prüfung und den Vertragsverhandlungen, wodurch viel Zeit und Geld verschwendet wird).

Also hat bzgl. einer Bonitäts-, Identitäts- und Legalitätsprüfung des Kunden der erstmalige **Einbau oder die Versetzung des Prozessschrittes** an erste Stelle in den Angebotsprozess **finanzrisiko- und haftungsreduzierende Wirkung:**
Es ist beispielsweise zu verhindern, dass durch einen wesentlichen Forderungsausfall eines Kunden mit schlechter Bonität das Unternehmen im Bestand gefährdet wird. Außerdem würde bei einem wesentlichen finanziellen Verlust wegen fehlender Bonitätsprüfung der Geschäftsführer der Gesellschaft (wegen Organisationspflichtverletzung) persönlich haften:

Das Unterlassen einer Bonitätsprüfung wurde bereits in der Rechtsprechung als Pflichtverstoß der Geschäftsführung angesehen und demzufolge wurde ein Schadensersatzanspruch aus § 43 Abs. 2 GmbHG gegen den Geschäftsführer konstruiert![21]

Durch die **Ergänzung** des Prozesses um den **Schritt „Kundenprüfung" (Identitäts-,Bonitäts- und Legalitätsprüfung** (Außenwirtschaftsrecht und Geldwäschegesetz, etc.) an der optimalen Stelle (gleich, nachdem dem Kunden, der ein Angebot nachgefragt hat, der Eingang seines Schreibens bestätigt wurde), ergeben sich **positive Auswirkungen: Bei negativer Auskunft**[22] wird eine zeit- und geldaufwändige technische und kaufmännische, Prüfung nebst Vertragsvorbereitung nicht durchgeführt **(x Tausend Euro Einsparung!).** Stattdessen wird aufgrund der freien Kapazität das Angebot für einen „positiven" Kunden, der möglicherweise aufgrund der im früheren Normalfall langsamen Bearbeitung zum Wettbewerber abgewandert wäre, zeitnah bearbeitet und erfolgreich umgesetzt (nochmals x Tausend Euro!). **Und entsprechend gehts weiter: Analyse und Optimierung durch Anreicherung mit Schritten zur Erfüllung der Anforderungen aus Risiko- und Compliancemanagement, etc. aller wichtigen weiteren Prozesse.**

21 Vgl. Fußnote oben.
22 Z.B.: Vertrag darf wegen Außenwirtschaftskontrolle oder fehlender Bonität bzw. nicht eindeutiger Identität oder Konzernzugehörigkeit des Anfrageunternehmens mit Krise bei Muttergesellschaft, etc. nicht geschlossen werden.

6. Bedeutet Vernetzung der Managementsysteme i. S. v. „Industrie 4.0" nicht auch exponentielle wechselseitige Auslagerung / Outsourcing?

Da „Industrie 4.0" wohl davon ausgeht, Leistungen (inklusive Produkte, etc.) nicht mehr alleine im eigenen Unternehmen, sondern im Rahmen von gemeinschaftlicher vernetzter Leistung vieler auch externer Leistungserbringer (Kunden / Lieferanten / Subunternehmer / etc.) zu erstellen, liegt auf der Hand, dass das Thema Outsourcing eine wesentlich verstärkte Betrachtung verdient.

Anforderungen bei Auslagerungen (Delegation / Überwachung)[23]

Bei Outsourcing / Auslagerungen oder Delegationen ist darauf zu achten, dass der Hersteller von Endprodukt/-leistung oder ein Systemverantwortlicher i.d.R. die Gesamtverantwortung für alle in dem System oder dem Endprodukt befindlichen Leistungen oder Komponenten trägt. Die Anforderungen an eine rechtssichere Delegation bestehen nach wie vor in der Auswahl von geeigneten Delegationsempfängern, einer entsprechenden Instruktion und einer Überwachung, dass die Leistungen der Delegationsempfänger die Anforderungen Effektivität, Sicherheit, Rechtssicherheit, Qualität, Termintreue, etc., beachten.

(Prüfungs-)Standards bei Auslagerungen

Für Auslagerungen gibt es bereits **spezielle Prüfstandards, um den Delegationsempfänger zu bewerten.** Beispielsweise im Bereich der IT-Dienstleistungen oder für rechnungslegungsrelevante Geschäftsprozesse zum Nachweis eines funktionierenden internen Kontrollsystems nach dem international anerkannten Prüfungsstandard ISAE 3402, SSAE 16 (früher SAS 70) oder IDW PS 331 bzw. 951.

In der Praxis zeigt sich, dass Lieferanten häufig in jüngster Zeit auch im Hinblick auf das Leben von Compliance- und Risikomanagement schon sehr gut auditiert und überwacht werden, jedoch sonstige Dienstleister, z.B. Berater, etc. noch unüberwacht ausgewählt und beschäftigt werden. Hier sollte sich ein Gesinnungswandel durchsetzen, da Fehlleistungen von Beratern genauso schwerwiegende Folgen haben könnten, wie fehlerhaft gelieferte Komponenten.

23 Vgl. auch Scherer / Fruth (Hrsg.), Governance-Management, Band II (Audit), 2015, zur Haftung von Management bei nicht ausreichender Überwachung Externer.

7. Neue Anforderungen an „Managementsysteme“, Manager und Mitarbeiter im Zeitalter „Industrie 4.0“

Mitarbeiter und Geschäftsleitung sowie Aufsichtsorgane sollten sich mit den neuen Anforderungen von „Industrie 4.0“ verstärkt beschäftigen. Insbesondere muss ein **Verständnis für die Architektur der erforderlichen Vernetzung** diverser „Managementsystem-Disziplinen“, wie hier am Beispiel von Qualitäts-, Risiko- und Compliancemanagement dargestellt, herbeigeführt werden. Das heißt aber auch, dass eine gewisse **Generalistenausbildung**, die über diverse Wissenschaftsdisziplinen und Fachfakultäten hinausgeht, erforderlich wird. Qualitätsmanagement erfordert nun - endlich - auch Risiko- und Compliancemanagement: Da sich beispielsweise der Kernbereich eines Compliance-Managementsystems mit dem prophylaktischen und reaktiven Management von Compliance-Risiken befasst, ist für Compliance-Verantwortliche Know-how im Risikomanagement inkl. der Fähigkeit, die angemessenen Methoden und Tools zum sachgerechten Einsatz zu bringen, unverzichtbar. Umgekehrt muss das Risikomanagement sich auch mit Compliance-Risiken beschäftigen, die gerade auch im Compliance-Bereich existenzielle Gefahren für Unternehmen und Mitarbeiter schlummern. Leider finden sich in der Praxis häufig eher nicht gut kommunizierende Inseln, die dadurch oft weder effektiv noch effizient arbeiten können. Auch die herkömmlichen Ausbildungsangebote weisen diese übergreifenden und vernetzten Ansätze noch nicht auf.

Die **Fähigkeit, Prozessmanagement und Workflows zu begreifen,** sowie Schnittstellen und Vernetzungen bedienen zu können, ist ebenso wichtig, wie die Herbeiführung von weltweit einheitlichem Verständnis von Begrifflichkeiten, Tools, Methoden, etc..

Entsprechende Anforderungen mögen zum einen auch in Stellenbeschreibungen derjenigen Mitarbeiter aufgenommen werden, die sich mit der Umstellung auf „Industrie 4.0“ zu beschäftigen haben. Ein weiteres Mittel, die entsprechende fachliche und persönliche Qualität für „Industrie 4.0“ darzustellen, wären entsprechende **Personenzertifizierungen.** Auch hierzu gibt es bereits **Standards** z.B. nach **DIN ISO 17024,** nach der Zertifizierungen durch von der deutschen **Akkreditierungsstelle (DAkkS)** akkreditierten Zertifizierer durchgeführt werden. Diese bisher für z. B. QM-Beauftragte vorgesehenen Zertifizierungen sollten nun im Lichte der ISO 9001:2015 auch die Themen Risiko- und Compliance-management-Kompetenzen beleuchten.

Literaturverzeichnis

Monographien:

Scherer, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012

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 (2015) Compliance-Managementsystem“, Corporate Compliance Zeitschrift 2015, S. 9 ff.

Buhl / Röglinger / Stöckl / Braunwarth, Wertorientierung im Prozessmanagement - Forschungslücke und Beitrag zu betriebswirtschaftlich fundierten Prozessmanagement - Entscheidungen, 2011, F/M -Kernkompetenzzentrum Finanz- & Informationsmanagement Universität Augsburg
Scherer / Fruth (Hrsg.), Governance-Management Band I, 2014.

Scherer / Fruth (Hrsg.), Governance-Management, Band II (Audit), 2015.

BGH, WM 1981, S. 440

Standards:

E DIN EN ISO 9001:2014-08:

Entwurf der Norm Qualitätsmanagementsysteme – Anforderungen

ISO/WD 18386 [Working Draft] (2012) (Compliance-Management-Systems)

IDW PS 980:2011

Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen

Internetquellen:

RiskNet https://www.risknet.de/themen/risknews/governance-prozess-pentagramm/a5a0dcb3f503fe9264b352f336b845f7/ (letzter Zugriff: 25.03.2015)

Autoren

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (Compliance), insbesondere Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf.
Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und Richter am Landgericht in einer Zivilkammer.
Neben seiner Tätigkeit als Seniorpartner der Kanzlei Prof. Dr. Scherer, Dr. Rieger & Partner erstellt er wissenschaftliche Rechtsgutachten und agiert als vorsitzender Richter in Schiedsgerichtsverfahren. Von 2001 - 2014 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken. Prof. Dr. Scherer fugiert in diversen Unternehmen / Körperschaften als Compliance Ombudsmann. Prof. Dr. Josef Scherer ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha. In Kooperation mit TÜV konzipierte er als Studiengangsleiter und Referent den akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement an der Technischen Hochschule Deggendorf. Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum. Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten der Managerhaftung, Governance, Compliance- und Risikomanagement sowie des Vertragsrechts, Produkthaftungsrechts, Sanierungs-und Insolvenzrechts.
Zahlreiche Publikationen auf den Gebieten: Managerrisiko, Governance-, Risiko-. Chancen- und Compliancemanagement, Vertragsmanagement, Arbeitsrecht, Insolvenzrecht und Sanierung, Gläubigermanagement, Produkthaftungsrecht.

Richter am Amtsgericht Klaus Fruth studierte Jura an der Universität Passau. Nach dem Staatsexamen arbeitete er in der Insolvenzverwaltung Professor Dr. Scherer. Anschließend war er mehrere Jahre Staatsanwalt bei den Staatsanwaltschaften in Deggendorf und Passau. Seit 2007 ist er Richter am Amtsgericht. Derzeit ist er beim Amtsgericht Freyung als Strafrichter eingesetzt und dort Vorsitzender des Schöffengerichtes. Seine Interessenschwerpunkte liegen im Bereich des Wirtschaftsrechts. Er ist Lehrbeauftragter der Technischen Hochschule Deggendorf u.a. für Governance, Produkthaftungsrecht, Unternehmensrecht und Geschäftsführer- Compliance. Außerdem ist er Dozent u.a. für die TÜV-SÜD Akademie, die Hans-Lindner-Stiftung und das Volkswagen Bildungsinstitut. Seine Publikationen befassen sich mit Technik- und Healthcare-Governance und Manager-Compliance.