„Das Richtige richtig tun!“
… ist gar nicht schwer.

GRC-Quick-Check

Gebrauchsanweisung, empirische Erhebung und Quick-Check zu „GRC“-Unternehmensführung in wenigen Minuten!

In Kooperation mit TIM Solutions / GRC Process Solutions

Autoren der Broschüre:

Prof. Dr. Jur. Josef Scherer

E-Mail:
josef.scherer@th-deg.de

☏ 01719960322

www.gmrc.de

Rechtsanwalt
Gründer und Leiter
des Internationalen Instituts für Governance, Management,
Risk- und Compliancemanagement
der Technischen Hochschule Deggendorf THD

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 Richter in Schiedsgerichtsverfahren. Von 2001 - 2015 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen / Körperschaften als Compliance-Ombudsmann sowie externer Compliancebeauftragter und 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 und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum. Außerdem ist er seit 2015 Mitglied des Beirates des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm) und seit 2016 Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement und seit 2017 Mitglied der Delegation ISO TC 309 Governance of organizations (Arbeitsausschuss Compliance NA 175-00-01-AA zur Erarbeitung von ISO/DIN-Standards im Bereich Unternehmensführung und –überwachung (Corporate Governance)).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Managerhaftung, Governance-, Compliance- und Risikomanagement sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht.

Zahlreiche Publikationen auf den Gebieten: Managerrisiko, Governance-, Risiko-. Chancen- und Compliancemanagement, Vertragsmanagement, Arbeitsrecht und Personalmanagement, Insolvenzrecht und Sanierung, Gläubigermanagement, Produkthaftungsrecht.

Die Veröffentlichungen (auch zum kostenlosen Download) finden Sie unter dem Link
http://www.scherer-rieger.de/index.php/wissenswertes/veroeffentlichungen.html

E-Mail:
klaus.fruth@t-online.de

www.gmrc.de

RiAG Klaus Fruth

Richter am Amtsgericht

**Leitung des Bereichs „Praxis“
des Internationalen Instituts für Governance, Management,
Risk- und Compliancemanagement
der Technischen Hochschule Deggendorf THD**

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 hauptsächlich als Strafrichter eingesetzt und dort Vorsitzender des Schöffengerichtes.

Seine Interessenschwerpunkte liegen im Bereich Governance und Compliance, des Manager-strafrechts und des Wirtschaftsstrafrechts.

Er ist Lehrbeauftragter an der Technischen Hochschule Deggendorf (THD) u.a. für Governance und Compliance, Produkthaftungsrecht, Unternehmensrecht und Geschäftsführer- Compliance.

Zugleich verantwortet er an der THD im Studiengang BWL Bachelor und Tourismusmanagement sowie bei den berufsbegleitenden Weiterbildungsstudiengängen die Durchgängigkeit eines geschlossenen Curriculums für Governance und Compliance.

Außerdem ist er Dozent u.a. für diverse Akademien ,im Rahmen von Inhouse-Schulungen und als Modulverantwortlicher und Referent im berufsbegleitenden Masterstudiengang Risiko- und Compliancemanagement an der THD tätig.

Seit 2014 übt er darüber hinaus die Funktion eines externen Compliance-Komitee-Mitglieds der THD (Zuständigkeit: Lehre) aus.

Er ist Leiter des Bereichs „Praxis“ am Internationalen Institut für Governance, Management, Risk & Compliance (GoMaRiCom).

Zusammen mit Prof. Dr. Scherer konzipierte er den weiterbildenden Zertifikatslehrgang „Zertifizierter Compliance-Officer“ der Haufe-Akademie und der Technischen Hochschule Deggendorf.

Inhaltsverzeichnis

7. **Tue Gutes und rede darüber: Intern oder extern: Reifegradmessung / Audit / Zertifizierung**

8. **Wir stellen uns vor: Das Internationale Institut für Governance, Management, Risk und Compliance der Technischen Hochschule Deggendorfs**

9. **Wer arbeitet noch im Zeitalter der Digitalisierung und was sind die Anforderungen?**

1. Einführung

1. 1 Hohe Anforderungen an Unternehmer!

Durch die kontinuierliche Zunahme und Verschärfung von Pflichten wird es für die Unternehmensleitung immer schwieriger, ein Unternehmen einerseits **rechtskonform**, andererseits aber **effizient** zu führen.

Schneller Wandel

Globalisierung, **Digitalisierung, wachsende Komplexität** in allen Bereichen erschweren unternehmerische Entscheidungsprozesse.

Unzureichendes Qualitäts-, Compliance- und Risikomanagement sowie fehlende Sensibilität sind häufig die Ursache für Schäden und Unternehmenskrisen.

Alleinstellungsmerkmale werden immer wichtiger!

Es ist entscheidend, durch Steuern **von Risiken und Realisieren von Chancen** einen Schritt voraus zu sein.

Effiziente, qualitativ hochwertige und (rechts-)sichere **Prozesse** in allen Unternehmensbereichen sind der Schlüssel zu **nachhaltigem unternehmerischen Erfolg und Unternehmenswertsteigerung.**

Lösungsansätze

Zur Erfüllung dieser vielfältigen Anforderungen durch den Unternehmer ist die Einführung eines **Integrierten Managementsystems mit Qualitäts-, Risiko-, Chancen-, und Compliance-Management** ein in der Praxis bereits bewährtes und äußerst erfolgreiches Instrument.

Gleichzeitig besteht nach der jüngsten Rechtsprechung sogar eine Pflicht für ein gelebtes („wirksames“) Managementsystem.

Was sagt die Praxis („good practice“)?

Um einen Überblick über die Präsenz der Themen:

- Digitalisierung/Industrie 4.0 in Prozessen,
- Risiko- Chancen- und Compliancemanagement

im Mittelstand zu bekommen, wird **auf Initiative des Instituts für Governance, Management, Risk & Compliance der Technischen Hochschule Deggendorf** eine **großflächige Befragung** von Geschäftsführern und sonstigen **Unternehmern** durchgeführt.

Haben Sie sich schon intensiver mit den Themen

- **Governance (Unternehmensführung), Risiko- und Compliancemanagement**
- **Internes Kontrollsystem**
- **Digitalisierung von Prozessabläufen**
- **Integriertes Managementsystem und**
- **Workflowmanagement**

befasst?

- ❑ Ja
- ❑ Durch Fachliteratur (Bücher, Fachzeitschriften, …)
- ❑ Teilnahme an Schulungen
- ❑ Sonstiges:_____

- ❑ Nein

1.2 Kleine Ursachen, große Probleme:

Es sind die kleinen Ursachen,

die große Probleme verursachen,

Zeit, Geld und Nerven kosten!

Kennen Sie Zeitfresser?

Eine **Studie**, bei der zahlreiche **Manager** tagelang unter Dokumentation ihrer „**Kommunikations-Aktivitäten**“ beobachtet wurden, ergab, dass Unternehmer sich im Schnitt zu **80%** ihrer Zeit mit der **Lösung (unnötiger) Probleme** beschäftigten und nur der Rest (20%), für Themen wie Strategie, Planung, Innovation zur Verfügung stand.[8]

„Verkehrtes Pareto-Prinzip“

8 Vgl. *Wimmer,* Kommunikation in Organisationen – Begleitung von 32 Führungskräften in drei erfolgreichen mittelständischen Industrieunternehmen, Masterarbeit im Masterstudiengang Philosophie-Politik-Wirtschaft der LMU München, 2010.

Probleme bei den Basics:

Falls nachfolgende Themen den Unternehmensalltag erheblich beeinflussen, liegt ein „systemisches“ Problem vor:

Bitte um Ihre Unterstützung!

Was in der Praxis alles nicht klappt: Bitte ankreuzen, falls eine Aussage auch auf Ihr Unternehmen, Ihre Abteilung zutrifft.

1	Nicht passende Tools / Methoden: Tool / Methode passt nicht zum Problem oder ist generell untauglich	☐
2	Fehlendes Generalgrundwissen mit einschlägigen Spezialwissen und mehrdimensionales Denken in diversen Fachdisziplinen (Recht / Technik / BWL / Psychologie / etc.)	☐
3	Zu wenig Blick in die Zukunft und über Tellerand / Planung (Business Plan / fehlende oder unzureichende Planungen in den relevanten Bereichen / etc.)	☐
4	Fehlende Softskills	☐
5	Zu wenig „Unternehmer im Unternehmen“ (Risiko- und chancenorientiertes unternehmerisches Denken / Entscheiden / Handeln)	☐

6	Fehlende Vorbildfunktion oder Fähigkeiten beim Management: "Der Fisch riecht vom Kopf weg" ("Tone from the Top")	☐
7	Inkonsequentes Führungsverhalten	☐
8	Bauchentscheidung statt schnelles *und* langsames Denken	☐
9	Abteilungsegoismus statt funktionierende Schnittstellen	☐
10	Falsche Leute auf falschen Posten (die Organisation richtet sich nach vorhandenen Personen, statt primär Schaffung optimaler Strukturen und danach Besetzung der Stellen mit den passenden Leuten)	☐

11	Schlechtes Zeitmanagement (Priorisierung der weniger wichtigen Dinge)	☐
12	Mangelhafte Kommunikation und fehlendes Verständnis für Begrifflichkeiten / Methoden / etc.	☐
13	Fehlendes Anreiz- und Sanktionssystem und geringe Motivation bzw. Loyalität	☐
14	Eigenmächtige Abweichung von vorgegebenen optimierten Prozessen aus unterschiedlichen Gründen (z.B. fehlendes Wissen, fehlende Akzeptanz) oder gar einfach fehlende oder schlechte Prozesse	☐
15	Unzureichende Kontrollmaßnahmen (If you can't measure it, you can't manage it)	☐

16	Mangelhafte Transparenz	☐
17	Unklare Zuständigkeiten	☐
18	Überwiegendes Lösen unnötiger Probleme (80%) statt Entwicklung von Innovationen, kreativen Strategien (20%) ("Pareto verkehrt")	☐
19	"Versumpfen" in Besprechungen / Erstellung von Konzepten und Fehlen einer stringenten Umsetzung (Steuerung): "Man müsste mal…"	☐
20	Etc.	☐

Sollten Sie mehr als 5 Kreuze gesetzt haben, besteht Bedarf für ein gelebtes, integriertes Managementsystem!

Damit Manager sich auf ihre (strategischen) Kernaufgaben konzentrieren können, sind **zuverlässige und fähige Mitarbeiter** sowie **gelebte Prozesse** wesentlich:

Ein Manager muss **delegieren**, aber sich gleichzeitig auch darauf verlassen können, dass **delegierte Aufgaben fristgerecht und qualitativ erledigt** werden.

Kommt es wiederholt zu Fristversäumnis oder Mängeln, übernimmt der Manager häufig selbst eigentlich delegierbare Aufgaben („alles an sich ziehen“) und vernachlässigt dadurch zwangsläufig seine Kernaufgaben.

Dies führt zu Frustration auf beiden Seiten.

Im übrigen bleibt er **trotz Delegation in der vollen Verantwortung!**

Daher sollte Management und Mitarbeiter ein **Integriertes „Kombi-Managementsystem on demand“ dabei unterstützen, „das „Richtige richtig“ zu tun“!**

1.3 Definitionen und Abgrenzungen

Was heißt eigentlich „GRC“?

„Complianceorientierte und risikobasierte Unternehmensführung und -überwachung“ erstreckt sich in Organisationen (private / public) auf *alle* Führungs-, Kern- und Unterstützungsprozesse.

Complianceorientierung
heißt, dass diese Prozesse sich an relevanten Gesetzen / Rechtsprechungen, „Anerkanntem Stand von Wissenschaft und Praxis“ und gegebenenfalls an einschlägigen Standards (ISO / IDW / etc.) orientieren.

Risikobasierung
bedeutet, dass – neben einem isolierten Risikomanagementprozess (vgl. Abbildung als Anlage) – an den relevanten Schritten in *jedem* Prozess (z.B. Vertriebs-/Einkaufs-/Personal-Prozesse) Risiko-Komponenten (z.B. prozessschritteigene Routinen (Identifikation / Bewerten / Steuern)), Risiko-Checks oder Risiko“-Steckbriefe“ enthalten sind.

Was heißt eigentlich „GRC“?

Abgrenzung zu Risk, Compliance und Qualitätsmanagement

- **Governance-Anforderungen sind umfassender** als Compliance-Anforderungen!

- **Compliance** kümmert sich um *pflichtgemäßes* Verhalten.
  Governance (Unternehmensführung) betrifft zusätzlich noch Themen mit Ermessensspielraum, z.B. strategische Entscheidungen

Abgrenzung von Compliance-Risiken und weiterem Risikomanagement

- **Risikomanagement** behandelt neben Compliance-Risiken auch sonstige Risiken, wie z.B. IT-Sicherheitsrisiken, Wegfall von Leistungsträgern, etc.

Abgrenzung zu „Qualitätsmanagement“

- Governance, Risk und Compliance kümmern sich idealerweise um alle Bereiche; Qualitätsmanagement (nach ISO 9001:2015) behandelt i.d.R. nur die Kernprozesse (F&E, Einkauf, Leistungserstellung, Vertrieb).

Mit einer Klappe mehrere Fliegen schlagen!

Idealerweise deckt sich pflichtgemäßes Verhalten mit „vernünftigem Verhalten“,

so, wie ein Bauarbeiter heutzutage von selbst und freiwillig Schutzkleidung (Helm / Sicherheitsschuhe / etc.) trägt und auf Alkohol auf der Baustelle verzichtet.

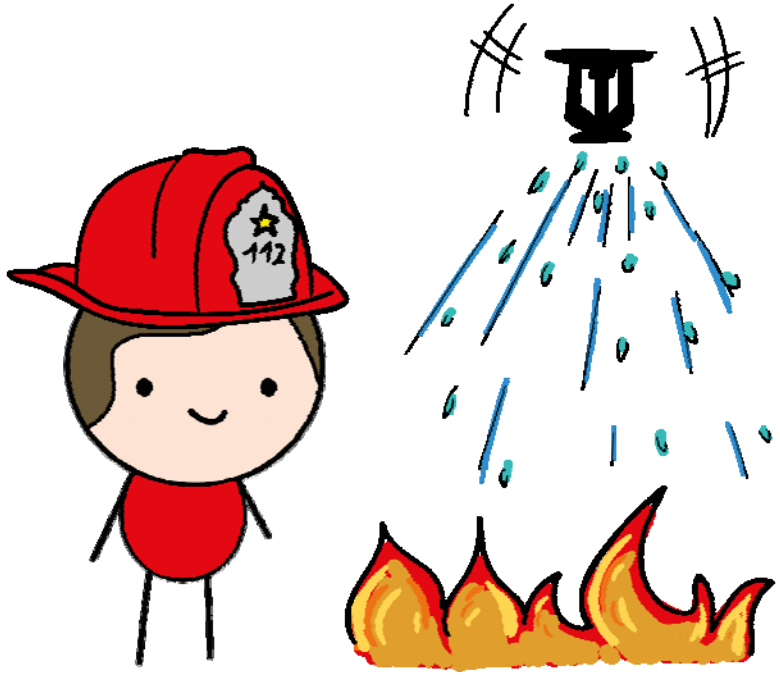
Oder ein Autofahrer sich angurtet.

Oder vor der Vergabe von Aufträgen die Vertragspartner (Lieferanten) „gecheckt“ werden in Hinblick auf Compliance, Qualität, Risiko, Nachhaltigkeit, etc. ….

Das war – zum Teil – früher anders!

Die letzten Jahre hat sich da viel verändert! Fallen Ihnen weitere (positive?) Beispiele ein?

Das „Neue“ an Governance, Risiko- und Compliancemanagement (GRC) ist, dass nicht – wie früher üblich – nur gelöscht wird, wenn es brennt und dann (reaktiv!) gewartet wird, bis es wieder brennt (-so werden bis heute noch Juristen ausgebildet).



„GRC“ kümmert sich gleich nach dem Brand um Brandschutz, damit es nicht nochmal brennt.

Oder noch viel besser: Gleich, bevor es überhaupt brennt, sorgt **es proaktiv für Brandschutz**.

Und:

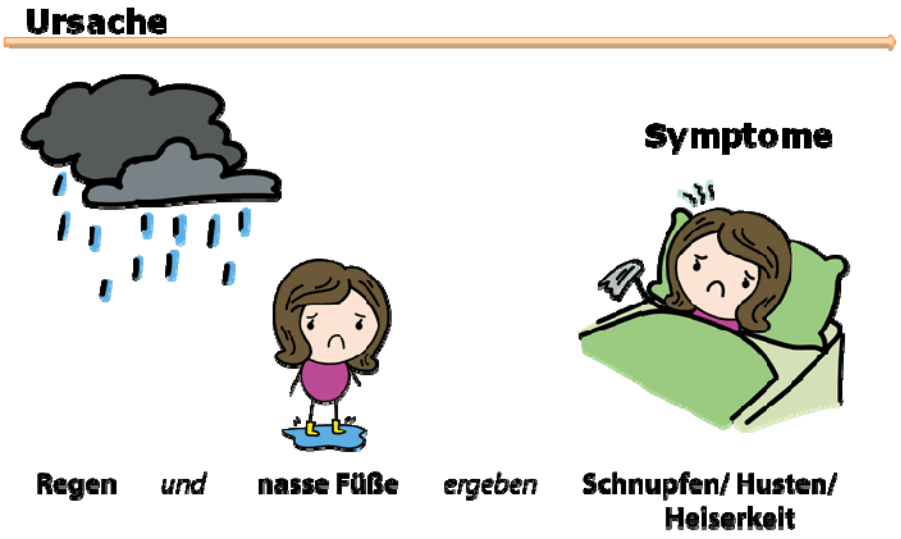
Ein funktionierendes „Brandschutzsystem“ (der Nachweis, dass gesetzliche, behördliche und interested-parties (z. B. Kunden, Aufsichtsfunktionen, etc.) -Anforderungen erfüllt werden) ist schließlich Voraussetzung für die Erlaubnis, das Unternehmen zu betreiben!

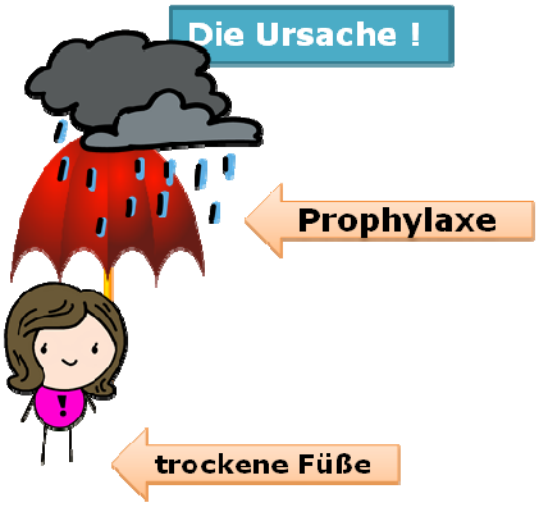
Governance, Risk und Compliance heißt, **durch Prophylaxe** den Eintritt von Pflichtverletzungen, Schadens- und Haftungsfällen zu **vermeiden** und den **Zugang zu Markt und Kunden und unternehmerische Tätigkeit an sich zu ermöglichen.**

1.4 Systemische Probleme erkennen und beheben!

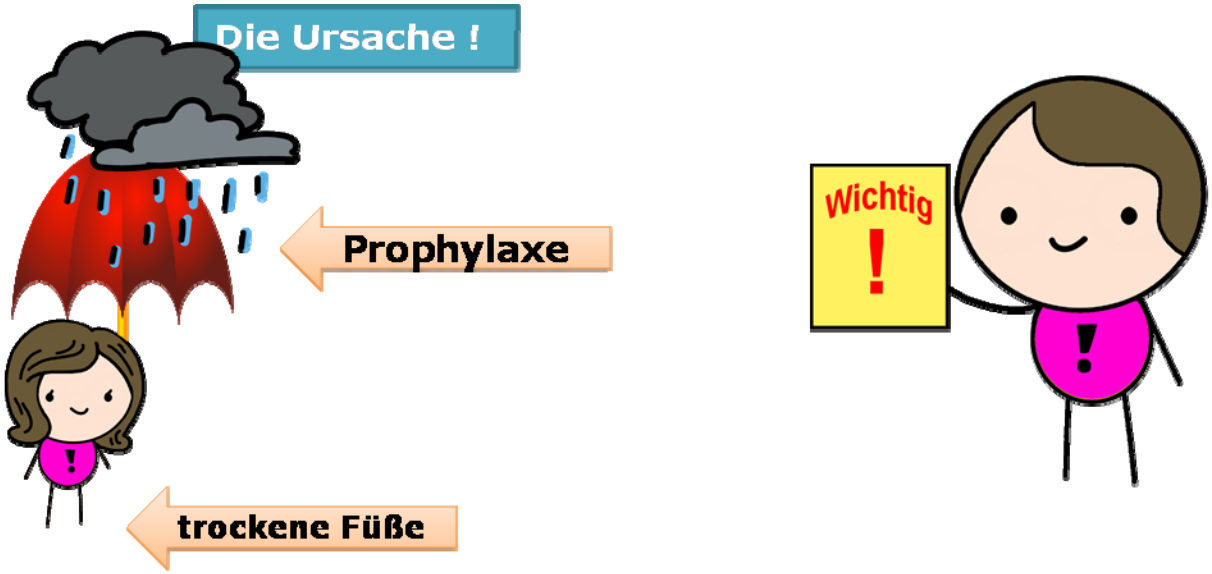
In vielen Unternehmen werden enorme **Ressourcen (Zeit / Geld / Nerven) verschwendet, um Symptome (Problemfälle) zu kurieren**.

Ziel ist, nicht – wie in der Praxis noch sehr häufig – mit viel Mühe die Symptome zu bekämpfen, sondern die Ursache





Die Lösung:



Ein wirksames (gelebtes) Integriertes Managementsystem mit GRC!

1.5 Neue „Spielregeln“ für Unternehmer!
Geänderte Umfeldbedingungen und Verunsicherung!

Die „gefühlte“ **Verschärfung von Haftungs- und Sanktionsgefahren für Vorstände, Geschäftsführer, Aufsichtsräte und sogar Gesellschafter** mit dem Vorwurf, pflichtwidrig gehandelt zu haben, ist objektiv **messbar:**

Im 10-Jahreszeitraum 1986-1995 gab es **genauso viele Urteile zur Managerhaftung wie in den letzten 100 Jahren zuvor.**

Für die nachfolgenden 10-Jahreszeiträume 1996-2005 und 2006-2015 wurde eine nochmalige Verdoppelung gemessen bzw. geschätzt!

Bayer [3] statuiert, der GmbH-Geschäftsführer sehe sich tatsächlich immens existenzbedrohender persönlicher Risiken ausgesetzt und hafte – faktisch – sogar viel schärfer als ein Vorstand, weil Geschäftsführer in Mittelstandsunternehmen nicht über *„vergleichbare Qualität an sachverständiger Beratung und Hilfestellung verfügen, die heute zur Abwehr rechtlich relevanter Sorgfaltsverstöße notwendig ist.*

Den Anforderungen, die heute an einen Geschäftsführer gestellt werden, lässt sich in der Praxis kaum gerecht werden".

Sogar der im Großen und Ganzen pflichtbewusst Agierende sehe sich nicht nur mit zivilrechtlichen Risiken, sondern auch der Gefahr der Strafbarkeit immer häufiger **bedroht**. [4]

[3] Vgl. *Bayer*, Die Innenhaftung des GmbH-Geschäftsführers, GmbHR 2014, S. 897 ff.

[4] Vgl. auch *Scherer/Fruth* (Hrsg.), Governance-Management, Band 1, 2014, Kap. 1.3.

Maßstab für Manager:

Der Entscheider hat sich nicht einmal zwingend auf dem „*neuesten Stand der Wissenschaft*“, sondern lediglich auf dem „*anerkannten Stand*“ als Mindestniveau zu bewegen:

Diese Aussage bezieht sich aber **nicht nur auf technisch physikalische Themen, sondern ebenso** u.a. **auf rechtliche und betriebswirtschaftliche Methoden und Werkzeuge.**

Das heißt, dass ***anerkannte und praktizierte Management-Methoden*** die **Messlatte für pflichtgemäßes Verhalten oder Pflichtverletzung** darstellen.

Beispiel:

Die Rechtsprechung sanktioniert **die Nichtabführung von Sozialversicherungsbeiträgen** (§ 266a StGB) sehr stark:

Dabei geht es **häufig** nicht um bewusst kriminell begangene Taten, sondern um **fehlende Sensibilität und Qualität der Organisation bei den Verantwortlichen**: So gibt es z.B. Grenzbereiche bzw. Unsicherheiten in der Praxis bei Scheinselbstständigkeit und Flexibilität bei „Gering-Verdiener-Jobs“, die zur Haftungsfalle für Manager werden:

Beispiel: „Scheinselbstständigkeits-Fall“:

Verurteilung eines 79-jährigen Senior-Chefs wegen Beschäftigung von Scheinselbstständigen zu Freiheitsstrafe („auf Bewährung“) durch *Landgericht Augsburg* als trauriger Abschluss eines arbeits- und erfolgreichen Berufslebens? [5]

Sind Sie sicher, dass Sie sicher sind?

ja ☐ ☐ nein

[5] Vgl. *SWP – Südwest Presse*, Pressemitteilung vom 14.10.2015, http://www.swp.de/ulm/lokales/alb_donau/IGericht-sieht-kein-System-hinter-Sozialbetrug;art1158552,3480598 [Abfrage am 10.06.2016].

Zahlreiche aktuelle **Problem-Fälle bei Konzernen, aber auch im Mittelstand** zeigen, dass die **Ursachen** für persönlich und unternehmensbezogen existenzielle Gefahren und Risiken **in nahezu jedem Bereich** / Prozess eines Unternehmens stecken können:

Fast jeden Tag finden sich sogar **in der Regional-Presse entsprechende Meldungen.**

BEISPIELE

Erstmalige (!) höchstrichterliche Rechtsprechung des Bundesgerichtshofes

***BGH*, Urteil vom 09.05.2017 – 1 StR 265/16 (Krauss Maffei Wegmann)**

Zur u.U. in der Einzelfallbetrachtung haftungsmindernden (!) Wirkung eines

- ❑ **in Anlehnung an anerkannte Standards (!)**

(IDW PS 980 / ISO 19600 / etc.: Vgl. Universal-Standard Compliance-Managementsystem des Internationalen Instituts für Governance, Management, Risk & Compliance)

- ❑ **zertifizierten (!) Compliance-Managementsystems**
- ❑ in Verbindung mit Wahrnehmung der Vorbildfunktion und
- ❑ vertrauensvoller Zusammenarbeit mit kompetenten Compliance-Beauftragten

durch die Geschäftsleitung:

- ❑ **Sowohl prophylaktisch,**
- ❑ **aber auch *nach (!)* dem Compliance-Vorfall** (zur Verhinderung von Wiederholungen)!

Vgl. auch:

***Raum* (Vorsitzender Richter des 1. Strafsenats des Bundesgerichtshofes), Compliance in Zusammenhang straf- und bußgeldrechtlicher Pflichten, S.48 ff., Rn. 56 ff., in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017**

Keine *„automatische" Haftungsbefreiung, aber:*

(Positive) Bedeutung der Standards für CMS und der Zertifizierung eines Compliance-Managementsystems

(in Kombination mit engagiertem „Tone from the Top" und Zusammenarbeit mit kompetenten Compliance-Officer)

in der *Einzelfallbetrachtung* des Gerichtes

- ❑ für Frage, *ob* Verletzung der Aufsichtspflicht vorliegt
- ❑ für Frage, *wie stark* eine Pflichtverletzung ist
- ❑ für Frage der *Höhe* der Geldbuße/Strafe
- ❑ für Frage, *wie* ein CMS aufzubauen und weiterzuentwickeln ist
- ❑ für Frage, *ob Strafbarkeit* vorliegt *(„strafbarkeitskonstituierend")* oder nicht!

Erste Entscheidung des Bundesgerichtshofes zu Compliance - Managementsystemen

„Erstmals hat der Bundesgerichtshof (BGH) im Urteil vom 9.5.2017 festgestellt, dass bei der Bußgeldbemessung gegen juristische Personen und Personenvereinigungen (§ 30 OWiG) sowohl die Existenz eines Compliance-Management-Systems (CMS), als auch die das CMS betreffenden Optimierungsmaßnahmen, welche nach Einleitung eines staatlichen Sanktionsverfahrens ergriffen wurden, von Bedeutung sind.“

„Unternehmen, insbesondere mittelständischen, die auch international tätig sind, ist daher dringend zu empfehlen, sich um die Einführung eines risikobasierten CMS bereits in Zeiten zu kümmern, in denen im Unternehmen aus Compliance-Sicht „die Welt noch in Ordnung ist“, d.h. sie sollten besser Vorsorge als Nachsorge betreiben. Wichtig ist dabei insbesondere, dass Compliance nicht nur auf dem Papier stattfindet, sondern, dass ein einmal eingeführtes CMS auch aktiv gelebt und stetig optimiert wird.“[1]

[1] *Malik, BGH:* Berücksichtigung Compliance-Management-System bei Bußgeldbemessung, www.haufe.de/compliance/recht-politik/vorteile-durch-compliance-management-system-bei-bussgeldbemessung_230132_422996.html

Die Aussagen des *Bundesgerichtshofes*[2]

zu:

- **1. Organ- (Manager-) Pflichten,**[3]
- **2. Ordnungsgemäße Delegation von Pflicht und Verantwortung,**[4]
- **3. Organ- (Manager-) Haftung,**[5]
- **4. Voraussetzungen der Befreiung von strafrechtlicher Haftung bei ordnungsgemäßer Einrichtung eines Compliance-Managementsystems (CMS),**[6]
- **5. Rechtliche Bedeutung von CMS in Verstoßfällen,**[7]
- **6. Bedeutung und Auswirkung von *Standards* (ISO / IDW / etc.) und *Zertifizierungen* auf die Manager- und Unternehmenshaftung,**[8]
- **7. Wertbeitrag eines CMS:**[9]

[2] Vgl. *Bundesgerichtshof* vom 09.05.2017 Az. 1 StR 265/16, Rn. 118 sowie *Raum* im Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017 in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017, auf den in der *BGH*-Entscheidung verwiesen wird.
[3] A. a. O. (Fn.1), Rn. 2.
[4] A. a. O. (Fn.1), Rn. 6 ff.
[5] A. a. O. (Fn.1), Rn. 3 ff.
[6] A. a. O. (Fn.1), Rn. 5 ff. und Rn. 28 – 32
[7] A. a. O. (Fn.1), Rn. 33 ff.
[8] A. a. O. (Fn.1), Rn. 56 ff.
[9] A. a. O. (Fn.1), Rn. 4 ff.a

Tipp:

1. Installieren Sie ein angemessenes Compliance- Managementsystem!

2. Optimieren Sie bei eingetretenen Problemfällen / eingeleiteten staatlichen Sanktionsverfahren Ihre betrieblichen Abläufe!

BGH, Urteil vom 09.05.2017 – 1 StR 265/16, Rn. 118 (Beck RS 2017, 114548)

„Für die Bemessung der Geldbuße ist zudem von Bedeutung, inwieweit die Nebenbeteiligte[10] ihrer Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt ***und ein effizientes Compliance-Management installiert hat****[11], das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss*

(vgl. Raum in Hastenrath, Compliance - Kommunikation, 2. Aufl., S. 31 f.).

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

[10] das betroffene Unternehmen, Anmerkung des Verfassers
[11] Hervorhebung durch Verfasser
[12] Hervorhebung durch Verfasser

Aussagen des Bundesgerichtshofes

Zu 1.

□ Organ- (Manager-) Pflichten:

Tipp:

1. Installieren Sie eine Unternehmens-, Umfeld- und interested parties – Analyse als Voraussetzung für eine angemessene Risiko-Analyse!

2. Führen Sie regelmäßig angemessene (Compliance-) Risikoanalysen durch!

3. Unterbinden Sie Rechtsverletzungen aus der Späre des Unternehmens durch ein angemessenes Compliance-Managementsystem!

4. Optimieren Sie Ihre internen Richtlinien und Prozessabläufe!

Aussagen des Bundesgerichtshofes

Zu 1.

□ Organ- (Manager-) Pflichten:

Zitat Raum:[13]

„(...) Wohl aber gibt es allgemeine Pflichten der Organe, die sich der Sache nach als relevante Compliance-Pflichten verstehen lassen. Ziel eines Compliance-Systems ist es, die Einhaltung dieser Pflichten möglichst optimal sicherzustellen.“[14]

„Die ***permanent zu aktualisierende Risikoanalyse***[15] ***setzt voraus, dass Vorkehrungen getroffen sind****, die es erlauben, den Markt ständig im Blick auf mögliche Gefahrensituationen zu beobachten.“*

---

[13] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 40 Rn. 29, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.
[14] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 31, Rn. 2, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.
[15] Hervorhebung durch Verfasser

*„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 („effektiv“)[16] **Compliance-Management installiert** hat, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss*

*(**vgl. Raum** in Hastenrath, Compliance – Kommunikation, 2. Aufl., S. 31 f.).*

*Dabei kann auch eine Rolle spielen, ob die Nebenbeteiligte **in der Folge dieses Verfahrens***

***entsprechende Regelungen optimiert** und*

***ihre betriebsinternen Abläufe so gestaltet hat**,[17] dass vergleichbare Normverletzungen zukünftig jedenfalls deutlich erschwert werden.“[18]*

[16] Anmerkung des Verfassers
[17] *Anmerkung: Fettdruck durch Verfasser*
[18] *BGH,* Urteil vom 09.05.2017 – 1 StR 265/16, Rn. 118 (Beck RS 2017, 114548)

„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****."*[19]

[19] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 31, Rn. 2, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

Zu 2.
□ Ordnungsgemäße Delegation von Pflicht und Verantwortung

Tipp:

1. Implementieren Sie einen kompetenten (internen / externen) Compliance-Beauftragten!

2. Überprüfen Sie regelmäßig die Funktionsfähigkeit Ihre Compliance-Managementsystems!

Zu 2.
□ Ordnungsgemäße Delegation von Pflicht und Verantwortung

Zitat Raum:[20]

2.1. „Ordnungsgemäße Delegation und Übertragung von Compliancebefugnissen“

„Maßgeblich ist das Bestellungsverhältnis [bzgl. des Compliance-Beauftragten] und wie es in der Praxis ausgeführt wird. (...)
Durch die Delegation darf daher keine Verantwortlichkeitslücke entstehen.
(...) Es muss (...) ein angemessener Informationsaustausch zwischen Organ und Compliance-Beauftragten stattfinden, der die gemeinsame Risikoanalyse im Blick auf das Unternehmen umfasst.“

2.2. „Auswahl der Compliance-Beauftragten“ [21]

2.3. „Überwachung“ [22]

„Das Organ muss vielmehr die Funktionsfähigkeit seines Compliance-Systems ebenso überprüfen wie seine Effizienz.“

[20] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 33, Rn. 6 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.
[21] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 37, Rn. 18 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.
[22] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 38, Rn. 22 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

Zu 3.

□ Organ- (Manager-) Haftung: [23]

Tipp:

1. Vermeiden Sie persönliche zivil-, straf- und bußgeldrechtliche Haftung: Vermeiden Sie Pflichtverstöße, indem Sie Ihre Organisation und Prozesse rechtssicher ausgestalten!

[23] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 31, Rn. 3., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017

Zu 3.

- **Organ- (Manager-) Haftung:**

  Unterscheidung zwischen Innen- und Außenhaftung sowie Zivil-, Wettbewerbs- sowie Straf- und Bußgeldrecht bei Compliance-Verstößen:

  Bei schuldhafter Pflichtverletzung durch die Organperson:

  - **3.1. I. d. R. keine zivil- oder wettbewerbsrechtliche Außenhaftung gegenüber Dritten**
  - **3.2. Zivilrechtliche persönliche Haftung i. d. R. nur gegenüber der Gesellschaft**
  - **3.3. Persönliche straf- und bußgeldrechtliche Haftung.**

Zu 4.

- **Voraussetzung der Befreiung von strafrechtlicher Haftung bei ordnungsgemäßer Einrichtung eines Compliance-Managementsystems:**

  Zitat *Raum:* [24]

  „[…] Für das Organ kann dies bedeuten, dass es sich ***im Falle einer ordnungsgemäßen Einrichtung entsprechender Compliance-Systeme jedenfalls im Grundsatz von einer strafrechtlichen Haftung (teilweise) befreien kann****. […]“*

  „[…] Dafür sind regelmäßig ***folgende Voraussetzungen*** *erforderlich:“*

[24] *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, S. 33, Rn. 5, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

Zu 4.

- **Voraussetzung der Befreiung von strafrechtlicher Haftung bei ordnungsgemäßer Einrichtung eines Compliance-Managementsystems:**

Tipp:

1. Befreien Sie sich von (strafrechtlicher) Haftungsgefahr durch:

   - ☐ Auswahl und organisatorisch richtige Einsetzung eines kompetenten (internen / externen) Compliance-Beauftragten!
   - ☐ Delegation der Compliance-Pflichten und Befugnisse auf den Compliance- Beauftragten
   - ☐ Überwachung des Compliance-Managementsystems
   - ☐ Vorbildfunktion in Sachen Compliance („Tone from the top“)
   - ☐ Überprüfung, ob Ihr Compliance-Managementsystem die wesentlichen Komponenten aufweist (vgl. unten 4.5)

Zu 4.

□ Voraussetzung der Befreiung von strafrechtlicher Haftung bei ordnungsgemäßer Einrichtung eines Compliance-Managementsystems:

Zitat *Raum:* [24]

„[…] Für das Organ kann dies bedeuten, dass es sich ***im Falle einer ordnungsgemäßen Einrichtung entsprechender Compliance-Systeme jedenfalls im Grundsatz von einer strafrechtlichen Haftung (teilweise) befreien kann****. […]“*

„[…] Dafür sind regelmäßig ***folgende Voraussetzungen*** *erforderlich:“*

[24] *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, S. 33, Rn. 5, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

4.1

□ ***„Ordnungsgemäße Delegation und Übertragung von Compliance-Befugnissen“:***

Zitat *Raum:* [25]

„[…] Eine der entscheidenden Schlüsselfragen lautet, ***wo und wie der Compliance-Verantwortliche*** *in der Unternehmensstruktur* ***verortet sein muss****.“*

[25] *Raum*, Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten, S. 33, Rn. 6, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

4.2

- ***„Auswahl der Compliance-Beauftragten“:***

  - Angemessene Rechtskenntnisse
  - Kommunikative Fähigkeiten
  - Konsequenz bei der Wahrnehmung seines Amtes
  - Persönlicher Charakter
  - Sachliche Ausstattung

4.3

□ *„Überwachung“:*

Zitat *Raum*: [26]

„[…] Das Organ muss vielmehr die Funktionsfähigkeit seines Compliance-Systems ebenso überprüfen wie seine Effizienz“ [Effektivität].

4.4

□ *„Positive Gesamteinstellung zur Compliance“*

(Tone from the Top)

[26] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 38, Rn. 22, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

4.5

□ *„Inhaltliche Maßgaben* für Angemessenheit / Ordnungsmäßigkeit eines CMS“:[27]

Tipp:

2. Überprüfen Sie, ob Ihr Compliance-Managementsystem folgende Basis-Elemente aufweist:

- ☐ Regelmäßige Risikoanalyse
- ☐ Kompetente, geschulte und motivierte Mitarbeiter auch in Bezug auf Compliance
- ☐ Anonymitätswahrendes Hinweisgebersystem
- ☐ Prozesse, um Compliance-Verstoße frühzeitig zu erkennen und konsequent und angemessen zu reagieren

[27] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 40, Rn. 27 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

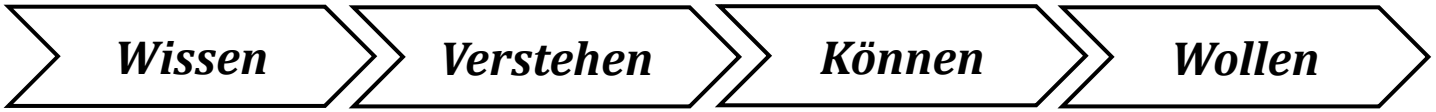
4.5.1

□ ***„Permanent zu aktualisierende Risikoanalyse“***

4.5.2

□ **Fortbildung der Mitarbeiter**

Vermittlung der für die Mitarbeiter *in ihrem Tätigkeitsfeld* maßgeblichen Normen:



[27] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 40, Rn. 27 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

4.5.3

□ Anonymitätswahrendes Hinweisgebersystem:

„Wichtig ist die Vertraulichkeit, […]“

4.5.4

□ Konsequente Ahndung von Verstößen

(Compliance-Verstoß-Erkennungs- und Reaktionsprozess)

Zu 5.

□ Rechtliche Bedeutung eines Compliance-Managementsystems in Verstoßfällen

Tipp:

1. Leiten Sie noch bei etwaigen persönlichen Sonderkenntnissen über Compliance- Risiken bzw. –Verstößen unverzüglich angemessene Maßnahmen ein!

„Eine wesentliche Wirkung eines Compliance-Systems ist die straf-/bußgeldrechtliche Entlastung der Geschäftsleitung“

„Liegt ein ordnungsgemäßes [!] Compliance-System vor, ist das Organ straf- und bußgeldrechtlich exkulpiert, *wenn ihm auch im Blick auf etwaige persönliche Sonderkenntnisse kein Schuldvorwurf gemacht werden kann.“*[28]

[28] *Raum*, „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 41, Rn. 34, in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

Zu 6.

- **Bedeutung und Auswirkung von Standards (ISO / IDW / etc.) und Zertifizierungen auf die Manager- und Unternehmenshaftung [29]**

Tipp:

1. Orientieren Sie die Ausgestaltung Ihres (Compliance-) Managementsystems an den Inhalten der geläufigen Standards (ISO / IDW / COSO / ...).

2. Sorgen Sie für Zertifizierungs-Reifegrad Ihres Managementsystems!

3. Nehmen Sie engagiert eine Vorbildfunktion auch in Richtung Compliance wahr!

4. Arbeiten Sie eng und vertrauensvoll mit einem konsequenten (internen / externen) Compliance-Beauftragten zusammen!

[29] *Raum* (Vorsitzender Richter des 1. Strafsenats des Bundesgerichtshofes), „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", 2017, S. 48 ff., Rn. 56 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017, Zitate:

Zu 6.

□ Bedeutung und Auswirkung von Standards (ISO / IDW / etc.) und Zertifizierungen auf die Manager- und Unternehmenshaftung

„Richtlinien und Zertifizierung

*In diesem Zusammenhang ist zu erörtern, welche **Bedeutung** den in jüngerer Zeit erarbeiteten **IDW (PS 980) und ISO (19600) Richtlinien/Normen** bzw. den von wirtschaftsberatenden Unternehmen angebotenen **Zertifizierungen** zukommen kann.“*

*„[…] Der Sache nach **gehören diese Fragen** im obigen Prüfungsschema **an die Stelle, an der geprüft wird, ob eine Verletzung der Aufsichtspflicht** vorliegt.*

*Die **Richtlinien/Normen können nämlich Standards setzen**, die wiederum die Entscheidung, ob das Zumutbare getan wurde, um solche Verstöße zu vermeiden, beeinflussen können.*

*Sie **helfen** aber auch – im Falle der Annahme einer Aufsichtspflichtverletzung – **das Maß der Pflichtwidrigkeit zu bestimmen**, das für die Bemessung der Geldbußen zu Lasten der Leitungspersonen und des Unternehmens selbst ein entscheidendes Kriterium ist.“*

*„Weder Richtlinien noch Zertifizierungen ersetzen **im Verletzungsfall die gebotene Einzelfallbetrachtung**. Die standardisierten Normen können die eigenverantwortliche Prüfung der Gerichte nicht ersetzen.*

*Eine **Zertifizierung** (auf welcher Grundlage auch immer) hat **für sich genommen weder** für das Organ **noch** für das Unternehmen eine **exkulpierende Wirkung**.*

*Insoweit kann die Zertifizierung **allenfalls eine individuelle Bedeutung** dafür haben, dass sich die Verantwortlichen um die Verhinderung von Rechtsverletzungen aus ihrem Unternehmen heraus bemüht haben.“*

*„Ebenso stellt **der kommunikative Prozess**, der mit der Zertifizierung verbunden ist, **einen Wert an sich** dar.*

*Hierdurch wird **Problembewusstsein geschaffen** und regelmäßig auch eine **Verbesserung der vorhandenen Strukturen** herbeigeführt.*

*Jedenfalls können die auf dem Markt befindlichen **Richtlinien** gerade im unternehmerischen Bereich ein **wichtiger Leitfaden für den Aufbau und die Weiterentwicklung eines Compliance-Systems** sein.“*

„Derartige Leitlinien können *deshalb* ***faktisch strafbarkeitskonstituierend sein****.*

Die mit der ISO 19600 geschaffenen Regeln *(…) können einen* ***Orientierungsrahmen*** *schaffen.*

Generell lässt sich anmerken, dass die von den Unternehmensleitungen erwünschten haftungsrechtlichen Persilscheine nicht durch eine Zertifizierung anhand irgendwelcher Richtlinien erreichen lassen wird, sondern ***in erster Linie*** *durch*

eine ***engagierte Wahrnehmung der Vorbildfunktion***

und einer ***ambitionierten und vertrauensvollen Zusammenarbeit mit kompetenten Compliance-Beauftragten****.“*

Zu 7.

□ Wertbeitrag eines CMS

Tipp:

1. Messen Sie den Reifegrad Ihres (Compliance-) Managementsystems!
2. Erzielen Sie mit einem gelebten (Compliance-) Managementsystem Wertbeiträge und Reputationsgewinne
3. Tue Gutes und rede darüber – intern und extern mit „interessierten Gruppen“

„Zwischenzeitlich ist eine funktionierende und glaubhafte Compliance **für das Image des Unternehmens selbst zu einem wichtigen Faktor geworden.**

Compliance hat einen **erheblichen Werbewert** für Kapitalgesellschaften.“[30]

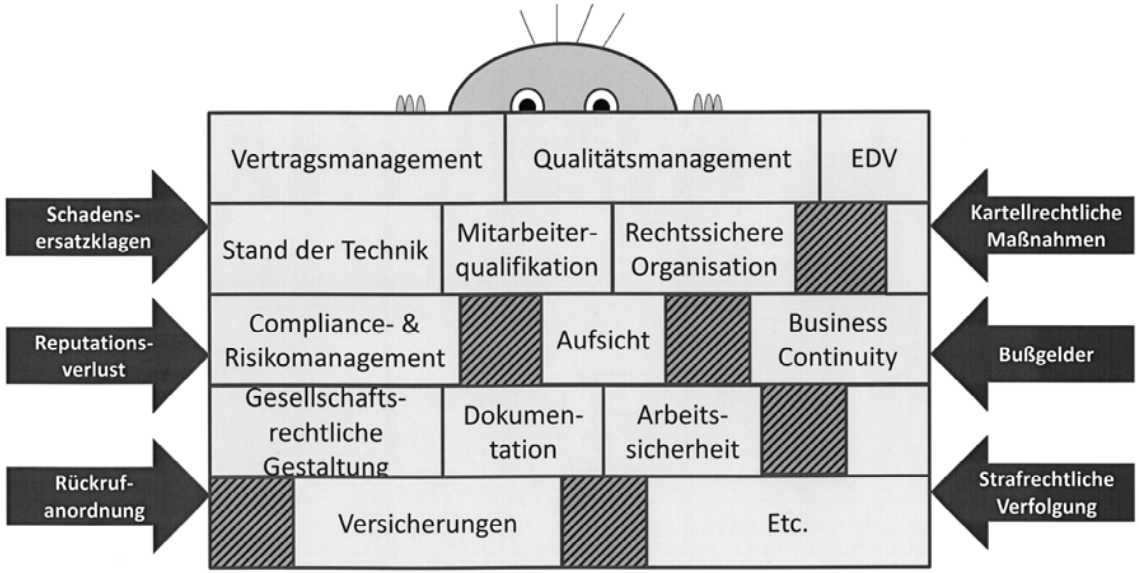
[30] Vgl. *Raum* „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, 2017, S. 32, Rn. 4 ff., in *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017

Anmerkung des Verfassers:

Tipp:

Berücksichtigen Sie den „gesunden Menschenverstand und das Pareto-Prinzip!“

1.6 Die „Manager-Haftungs-Firewall“



Die „**Manager-Haftungs-Firewall**“ gibt es nicht „von der Stange“ zu kaufen.

Sie **besteht aus einzelnen Bausteinen** /Komponenten, die in **gelebte (!) Prozessabläufe** integriert werden. Am besten wird sie unter fachkundiger Anleitung mit Profis von Ihnen und Ihren Mitarbeitern geformt.

Dann hält sie auch!

Fragen und Unsicherheit bzgl. rechtssicherer, effektiver und effizienter Organisation:

- Was ist „gute Unternehmensführung“ nach anerkanntem Stand von Wissenschaft und Praxis?

- Was ist dabei konkret wie zu erfüllen („das Richtige richtig tun“)?

- Wie kann das – mit überschaubarem Aufwand – umgesetzt werden?

- Welche integrierten (IT)-Lösungen sind einzusetzen, um den neuen und künftigen Anforderungen gerecht zu werden und um Management und Mitarbeiter zu unterstützen, pflichtgemäß, nachhaltig und erfolgreich zu agieren?

Checkfragen:

Spielen bei Ihnen im Unternehmen das Thema „Überregulierung“ / „hohe Kosten mit hohem Ressourceneinsatz aufgrund ausufernder Bürokratie“ eine Rolle?

- ❑ Ja
- ❑ Nein

Fordern Geschäftspartner (z.B. Großkunden) vermehrt Zertifikate oder Nachweise bezüglich Qualitätsmanagement, Risikomanagement, Compliancemanagement oder Nachhaltigkeit?

- ❑ Ja
- ❑ Nein

Gibt es im Bereich „Prozessoptimierung“ und Digitalisierung (workflow-Management) noch Nachholbedarf?

- ❑ Ja
- ❑ Nein

Sind Sie sich unsicher, ob Sie, das Unternehmen und Ihre Mitarbeiter durch eine rechtssichere und effiziente Organisation tatsächlich vor (*persönlicher)* Haftung/Sanktion geschützt sind?

- ❑ Ja
- ❑ Nein

Tragen Sie sich mit dem Gedanken, Qualitätsmanagement nach der neuen ISO 9001:2015 zu rezertifizieren oder erstmalig einzuführen?

- ❑ Ja
- ❑ Nein

Halten Sie die Implementierung (und (Re-)Zertifizierung) der in Anzahl wachsender „Managementsystem-Inseln“ (Qualitätsmanagement-, Arbeitssicherheit-, Umwelt-, Risiko-, Compliance-, Nachhaltigkeits-, etc.-Managementsystem) für ineffektiv, ineffizient und nicht zielführend?

- ❑ Ja
- ❑ Nein

Ist Ihr System eine Anhäufung von nicht abgestimmten Inseln?

- ❑ Ja
- ❑ Nein

Vermuten Sie, dass dies viel Geld, Zeit, Nerven verbrennt?

- ❑ Ja
- ❑ Nein

Unterstützt Sie bereits ein (Integriertes) Managementsystem zur vollen Zufriedenheit?

- ❑ Ja
- ❑ Nein

Sind Sie interessiert an Kosteneinsparung durch Integration von Qualitätsmanagement mit Risiko-, Compliancemanagement und Internem Kontrollsystem?

- ❑ Ja
- ❑ Nein

Ist Gesellschafter oder Aufsichtsgremium Ihres Unternehmens verantwortlich für die „Governance"-Funktionen Risikomanagement, Compliance, Internes Kontrollsystem und Revision und möchte nun von Ihnen als Unternehmer entsprechende Nachweise?

- ❑ Ja
- ❑ Nein

Haben Sie bereits ein Managementsystem im Unternehmen implementiert?

- ❑ Qualitätsmanagement DIN ISO 9001:2015
- ❑ Arbeits- und Gesundheitsschutzmanagement (neu)
  DIN EN ISO 45001:2017, OHSAS 18001:2007
- ❑ Umweltmanagement DIN ISO 14001:2015
- ❑ IT Sicherheitsmanagement DIN ISO 27001:2015
- ❑ Internes Kontrollsystem (IKS) IDW PS 982:2017 /
  IDW PS 261
- ❑ Internes Revisionssystem DIIR Nr. 3 / IDW PS 983:2017
- ❑ Datenschutz-Managementsystem
- ❑ Personal-Managementsystem ISO 30400 ff :2016
- ❑ Sonstige:_____

- ❑ Nein

Unterhalten Sie ein Compliance-Managementsystem entsprechend ISO 19600:2014 und IDW PS 980:2011?

- ❑ gelebt und zertifiziert
- ❑ implementiert und zertifiziert
- ❑ implementiert
- ❑ gerade im Aufbau
- ❑ nicht geplant
- ❑ Nein

Unterhalten Sie ein Risiko- und Chancen-Managementsystem nach DIN ISO 31000:2009 bzw. ONR 49000 im Unternehmen?

- ❑ gelebt und zertifiziert
- ❑ implementiert und zertifiziert
- ❑ implementiert
- ❑ gerade im Aufbau
- ❑ nicht geplant
- ❑ Nein

2. Lösungen:

Integriertes „Kombi-Managementsystem on demand“

- die Basis für Zielerreichung, Workflow-Management, Digitalisierung und Industrie 4.0

1. Was ist das?

Geschäftsleitung (Geschäftsführer / Vorstand), **Gesellschafter** und u. U. **Aufsichtsgremium** (Aufsichtsrat / Beirat / etc.) haben höchstes **Interesse an ordnungsgemäßer und erfolgreicher Unternehmensführung.**

Das *Richtige* muss *richtig* gemacht werden, **um die vielfältigen Ziele zu erreichen.**

Workflow-Management, Digitalisierung und Industrie 4.0 sind ein „*Muss*“ für verantwortungsvolle, zukunftsorientierte Unternehmer.

Dabei unterstützt ein *Integriertes „Kombi-Managementsystem on demand“*:

Nach der P/D/C/A-Methode werden in einer „**prozessorientierten Organisation**“ über ein:

1. Zielemanagement
die richtigen Ziele gesetzt, Anforderungen bestimmt und geplant / projektiert.

↓

Das
2. Organisationsmanagement

schafft die erforderlichen Rahmenbedingungen, wie beispielsweise implementierte Prozessabläufe und stellt input / Ressourcen bereit.

↓

In der
3. Umsetzungsphase wandeln diverse Aktivitäten den input in output / Zielerreichung.

↓

Das
4. Steuerungs- und Überwachungs- sowie

↓

5. Verbesserungsmanagement

gewährleistet die Zielerreichung.

Für den Unternehmer stellt sich die Frage, **worum** er sich **kümmern** sollte und **welche** Ziele er setzen muss.

Für eine **Vielzahl von Themen**, wie Qualitäts-, Risiko-, Compliance-, Umwelt-, Nachhaltigkeits-, etc.-Management stehen **diverse Standards** (ISO, COSO, IDW, etc.) und **Insel-Systeme** zur Verfügung.

Die über eine ***Unternehmensanalyse*** ermittelten relevanten Themen können jedoch auch **integriert** abgebildet werden.

Dabei findet sich aufgrund zahlreicher **Redundanzen** ein **enormes Einsparungspotenzial.**

2. Was bringt das?

Eine Organisation, die sich an Prozessabläufen orientiert, die diverse Anforderungen erfüllen, sorgt für **Rechtssicherheit**, Transparenz, Effizienz, **Zielerreichung und hohe Wertbeiträge**.

- Und sie legt den **Grundstein für Workflow-Management, Digitalisierung und Industrie 4.0.**

Erstmalige (!) höchstrichterliche Rechtsprechung des Bundesgerichtshofes

***BGH*, Urteil vom 09.05.2017 – 1 StR 265/16 (Krauss Maffei Wegmann)**

Zur u.U. in der Einzelfallbetrachtung haftungsmindernden (!) Wirkung eines

- ❑ **in Anlehnung an anerkannte Standards (!)**

(IDW PS 980 / ISO 19600 / etc.: Vgl. Universal-Standard Compliance-Managementsystem des Internationalen Instituts für Governance, Management, Risk & Compliance)

- ❑ **zertifizierten (!) Compliance-Managementsystems**
- ❑ in Verbindung mit Wahrnehmung der Vorbildfunktion und
- ❑ vertrauensvoller Zusammenarbeit mit kompetenten Compliance-Beauftragten

durch die Geschäftsleitung:

- ❑ **Sowohl prophylaktisch,**
- ❑ **aber auch *nach (!)* dem Compliance-Vorfall** (zur Verhinderung von Wiederholungen)!

Vgl. auch:

***Raum* (Vorsitzender Richter des 1. Strafsenats des Bundesgerichtshofes), Compliance in Zusammenhang straf- und bußgeldrechtlicher Pflichten, S.48 ff., Rn. 56 ff., in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017**

Keine *„automatische" Haftungsbefreiung, aber:*

(Positive) Bedeutung der Standards für CMS und der Zertifizierung eines Compliance-Managementsystems

(in Kombination mit engagiertem „Tone from the Top" und Zusammenarbeit mit kompetenten Compliance-Officer)

in der *Einzelfallbetrachtung* des Gerichtes

- ❑ für Frage, *ob* Verletzung der Aufsichtspflicht vorliegt
- ❑ für Frage, *wie stark* eine Pflichtverletzung ist
- ❑ für Frage der *Höhe* der Geldbuße/Strafe
- ❑ für Frage, *wie* ein CMS aufzubauen und weiterzuentwickeln ist
- ❑ für Frage, *ob Strafbarkeit* vorliegt *(„strafbarkeitskonstituierend")* oder nicht!

3. Besteht eine (rechtlich verbindliche) Pflicht?

Rechtsprechung und in einigen Branchen neuerdings sogar der **Gesetzgeber** stellen **verpflichtende Anforderungen an die Geschäftsorganisation** auf.

So ist beispielsweise ein (Compliance-)Risiko-Managementsystem oder Internes Kontroll-System (IKS) rechtlich verpflichtend.

Der Nachweis eines (zertifizierten) Qualitäts- oder corporate social responsibility (CSR)-Managementsystems wird immer häufiger **von Kundenseite gefordert**.

4. Wird die Einrichtung eines (Integrierten) Managementsystems von Standards / Auditoren gefordert?

Mit einer Klappe mehrere Fliegen schlagen!

Es gibt derzeit **nahezu für jedes (Prozess-) Themenfeld eines Unternehmens** (Strategie, Personal, Risk, Compliance, Einkauf, Leistungserstellung und Vertrieb, IT, Qualitätsmanagement, IKS, etc.) **Standards** von ISO / DIN / COSO / IDW / DIIR / etc..

Diese sehen überwiegend **Insel-Systeme** vor.

Von Insel-Systemen „profitieren“ nicht alle: Insbesondere für Geschäftsleitung und Mitarbeiter **bedeuten viele parallele „Insel-Welten“ eine nicht lebbare (wirksame) und teuere Bürokratie**.

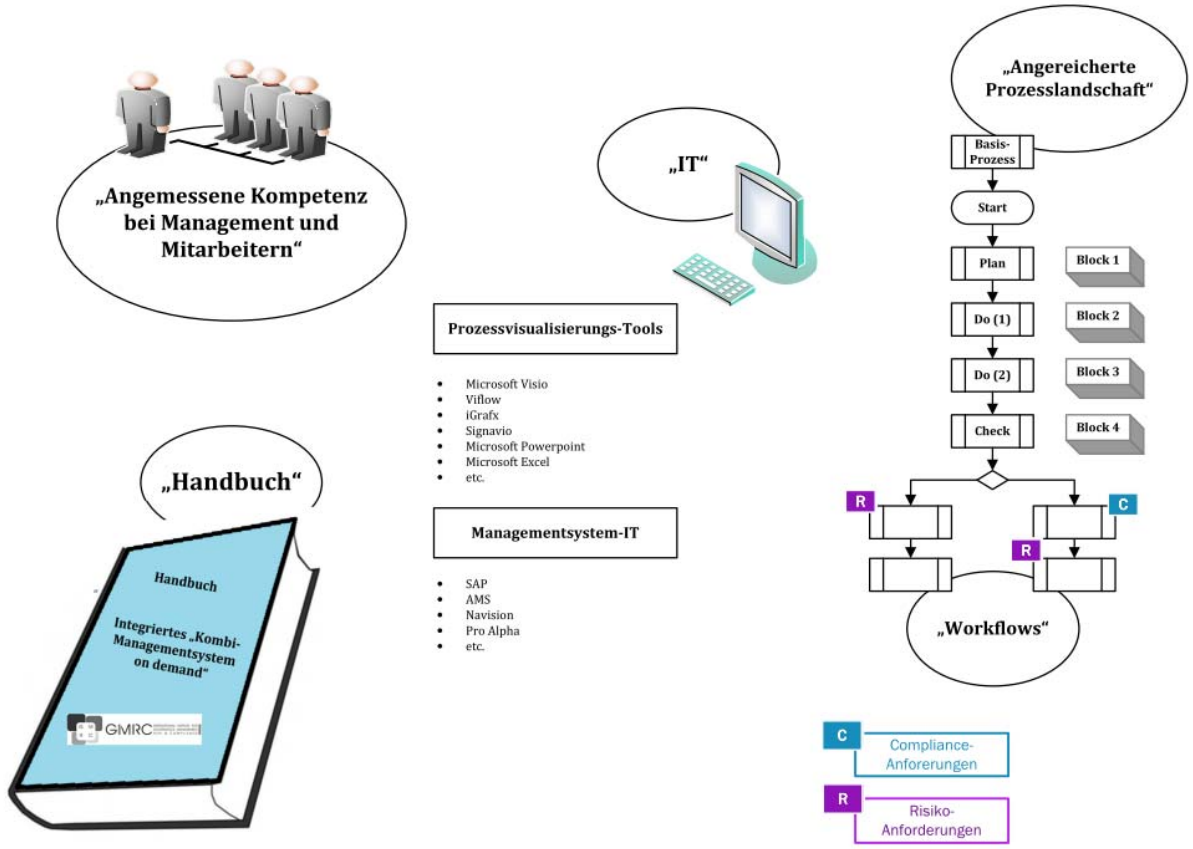
Ein **Integriertes Managementsystem sieht** dagegen z. B. der britische Standard PAS 99:2012 vor.

5. Gibt es Arbeitshilfen?

Ja, z. B.

- ☐ Risikoworkshop und Unternehmens-, Umfeld- und interested parties- Analyse zur Feststellung, welches „System“ zwingend und / oder nützlich ist.
- ☐ Konzeptionierung eines an den relevanten Standards orientierten Integrierten Managementsystems inkl. eines Kataloges erforderlicher Einzelkomponenten (z. B.
  - Prozessabläufe,
  - Stellenbeschreibungen,
  - Kennzahlensystem, etc.)
- ☐ Implementierung (Anreicherung der Prozesslandschaft)
- ☐ Hinführung zur „Wirksamkeit“ (gelebt werden) durch die Mitarbeiter
- ☐ Audit
- ☐ Zertifizierungsmöglichkeit

6. Wie sieht das Produkt aus?



Das „Produkt“ besteht aus diversen Komponenten

3. P/D/C/A: „Plan“: Ziele-Management

Wofür sind Geschäftsleitung, Aufsichtsgremium und das weitere Management verantwortlich?

Bitte auf nachfolgender Matrix ankreuzen:

Was ist Pflicht bzgl. „ob“?

(Müssen Sie sich grundsätzlich um dieses Thema kümmern?)

Ist auch vorgegeben, „wie“? Sie den jeweiligen Prozess-Themenbereich auszugestalten haben (z.B. über Standards)?

Ernüchterndes Ergebnis: Sie sollten sich um fast alles in einer *grundsätzlich* vorgegebenen Art und Weise kümmern!

„Plan“: Ziele-Management

Nr.	Themengebiet	Muss sich die gewissenhafte Geschäftsleitung zwingend um diesen Themenbereich kümmern?		Existieren zwingende Vorgaben, "wie?" dieser Themenbereich auszugestalten ist? Existieren "Good Practice-Standards" (z.B. ISO / IDW / COSO / etc.)		Falls bzgl. "ob?" oder "wie?" keine Pflicht besteht, sondern Ermessensspielraum: Anwendung der Business Judgment Rule und Entscheidung:	
		Pflicht bzgl. "Ob?"		Vorgaben bzgl. "wie?"		Was ist gewünscht?	
		+	-	+	-	+	-
1	Analyse von Unternehmen, Umfeld, Anforderungen der interested parties						
2	Management (Fachliche und persönliche Kompetenzen)						
3	Governance I Zusammenspiel der Organe						
	Governance II Unternehmensführung (GoU)						
	Governance III Unternehmensüberwachung (GoÜ)						
4	Managementsystem						
5	Vision / Ziele / Strategie / Planung						
6	Organisation						
7	Finanzen / Steuern / Versicherung						
8	Personal						
9	Risiko-Management						
10	Compliance & Legal / (Externe) Rechtsabteilung						

Ermittlung der relevanten (Prozess-) Themenbereiche über Unternehmensanalyse mit Risiko- und Chancen-Bewertung

Wofür ist Geschäftsleitung, Aufsichtsgremium und das weitere Management verantwortlich?

Quelle: *Scherer / Fruth* (Hrsg.), Governance-Management, Band I, 2014, S. 69

11	Forschung und Entwicklung						
12	Beschaffung / Einkauf						
13	Leistungserbringung						
14	Marketing / Vertrieb						
15	IT						
16	Information / Kommunikation / Berichtswesen						
17	Wissens- und Dokumentations-management						
18	Rechnungswesen / Controlling						
19	Qualitätsmanagement						
20	Security / Safety						
21	Business Continuity / Restrukturierung / Sanierung						
22	Sonstige (Logistik / Projektmanagement / etc.)						

Quelle: *Scherer / Fruth* (Hrsg.), Governance-Management, Band I, 2014,S. 69

Egal, in welchem (Prozess-)Themenbereich (Finanzen, Einkauf, Personal, Vertrieb, Leistungserstellung, IT, QM, etc.):

Der Ablauf sollte stets gleich sein:
Ziele und deren Anforderungen bestimmen **(Ziele- und Planungsmanagement)** und die erforderlichen Ressourcen **(Input)** bereitstellen:

Dann können Mitarbeiter und IT im Rahmen der von den Prozessabläufen vorgegebenen Leitplanken agieren **(„line of action“)** und mithilfe interner und externer **Steuerung und Überwachung**

die Ziele (Output) erreichen:

3.1 Was wollen Geschäftsleitung, Gesellschafter, Aufsichtsgremium und sonstige interested parties? Das Gleiche!

Alle wollen das Gleiche! Was?

1. Angemessene Ziele und Kennzahlen (Plan)

Beispiele: Pflichtziele (Compliance) und fakultative Ziele (business-judgment-rule):
Z. B. Wertsteigerung, Wertbeiträge, Nachhaltigkeit, Social responsibility, Innovationsführerschaft

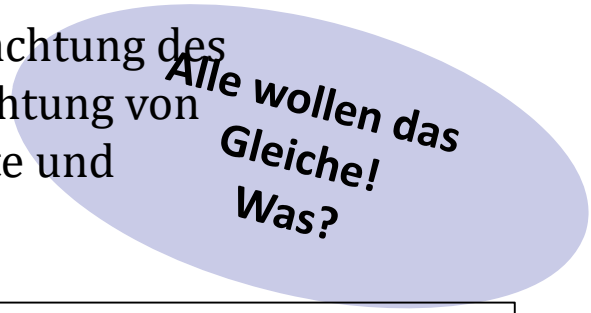
2. Angemessene Planung (Plan)

Beispiele: Wirtschaftsplan, Finanzplan, Personalplan, Produktionsplanung, Liquiditätsplanung, Investitionsplanung, etc.

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement, 2016, S. 42 ff.

3. Sorgfältige Umsetzung: Wirksame (gelebte) angemessene Prozesse (Do)

Beispiele: Beachtung der Gesetze (Compliance) und Beachtung des anerkannten Standes von Wissenschaft und Praxis, Beachtung von Standards (?), Beachtung der Anforderungen an Produkte und Leistungen (effektiv, qualitativ, sicher, rechtssicher usw.)



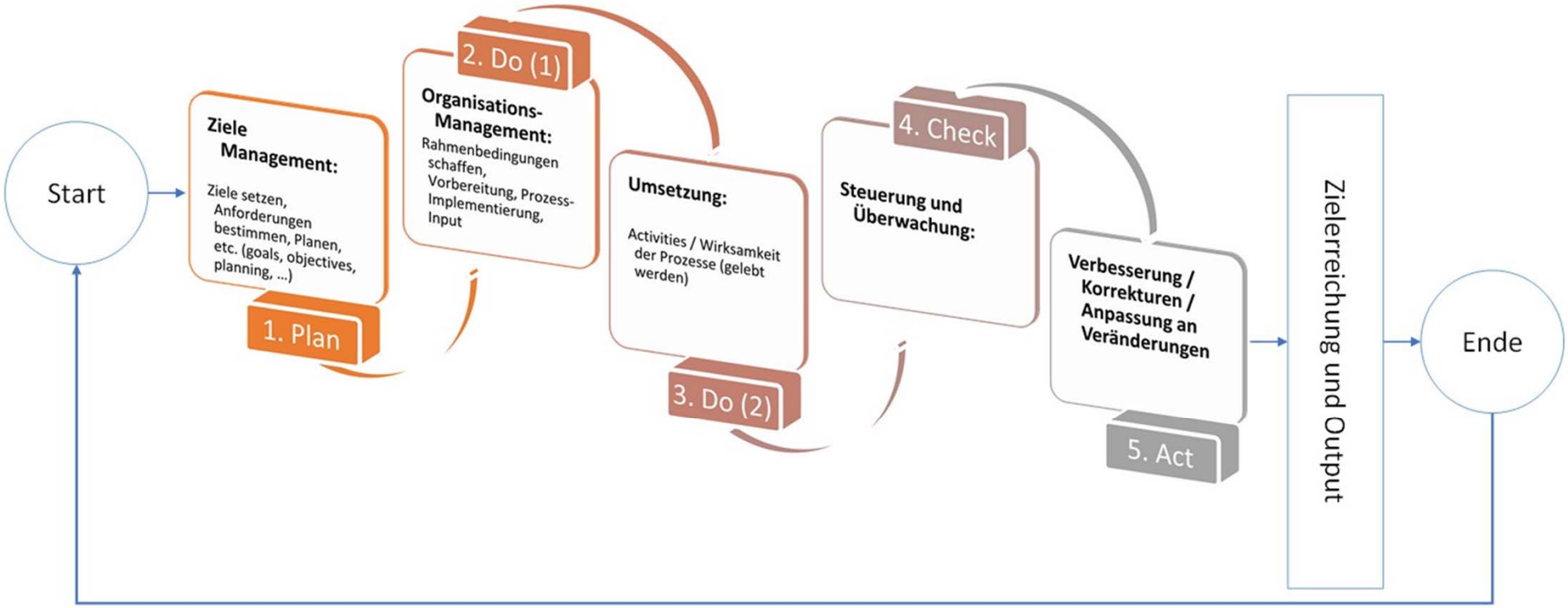
4. Angemessenes und wirksames Steuerungs- und Überwachungssystem (Check)

Beispiele: Das „lines of defense-Modell“

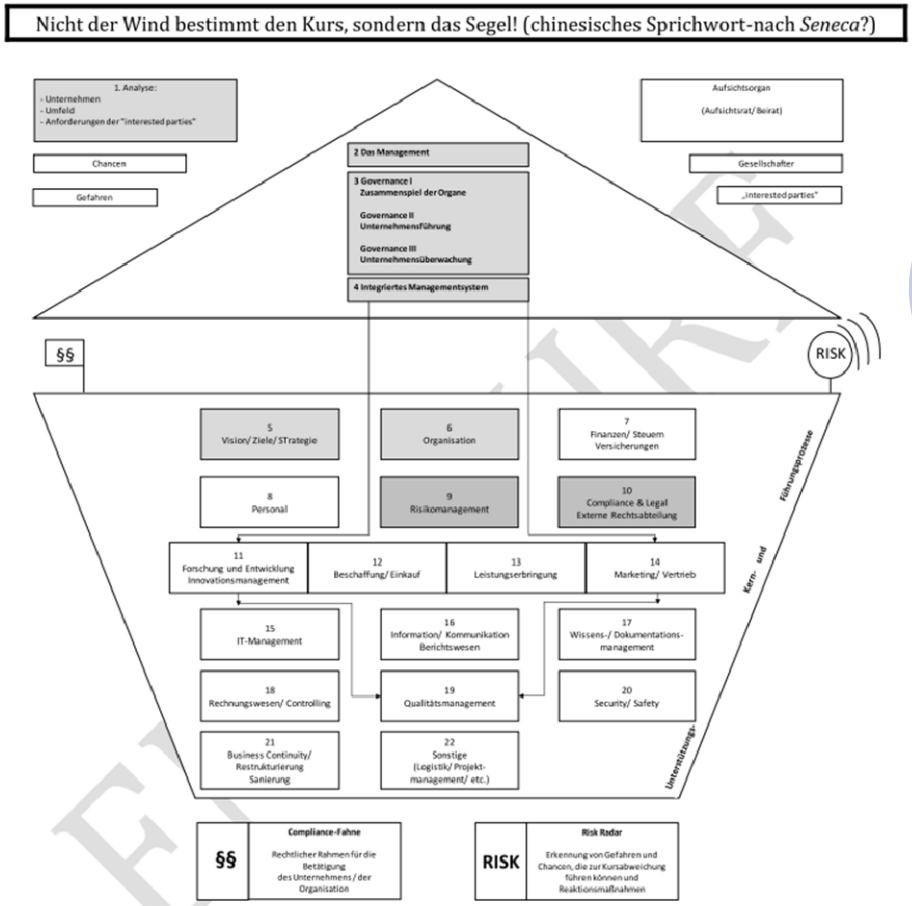
5. Grad der Zielerreichung (über Kennzahlen / KPI‘s)

Beispiele: Finanzkennzahlen, Personalkennzahlen (Human Capital Metrics), Compliancekennzahlen, Innovations-, Nachhaltigkeits-, Social Responsibility-Kennzahlen, usw.

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement, 2016, S. 42 ff.


Start
Ziele Management:
Ziele setzen, Anforderungen bestimmen, Planen, etc. (goals, objectives, planning, ...)
1. Plan
2. Do (1)
Organisations-Management:
Rahmenbedingungen schaffen, Vorbereitung, Prozess-Implementierung, Input
Umsetzung:
Activities / Wirksamkeit der Prozesse (gelebt werden)
3. Do (2)
4. Check
Steuerung und Überwachung:
Verbesserung / Korrekturen / Anpassung an Veränderungen
5. Act
Zielerreichung und Output
Ende

Ihr „Unternehmenssschiff“ mit ca. 20 Führungs-, Kern- und Unterstützungs-Prozessen, Compliance-Fahne und Risiko/Chancen-Radar



„Ein kleiner Schritt in der Unternehmensorganisations -Strategie

- ein großer Schritt zu Workflow-Management, Digitalisierung und Industrie 4.0!

Gibt es diese Prozess-Themenbereiche auch in Ihrem Unternehmen?

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement mit GRC, 2016,S. 25 ff.

3.2 Risiko-Kurz-Check für Ihr „Unternehmens-Schiff“:

Top-Risiken im Prozess-Themenfeld 1: „Externe Risiken“

	relevant?	
▪ Naturkatastrophen und höhere Gewalt (Feuer, Blitzschlag, Explosion, Schäden durch Sturm, Hagel, Erdbeben, Krieg, Terrorismus, soziale Unruhen, Seuchen – auch bei wichtigen Lieferanten?)	❑ Ja	❑ Nein
▪ Konjunkturschwankungen (Rezession)	❑ Ja	❑ Nein
▪ Mehr Wettbewerber durch globale Märkte	❑ Ja	❑ Nein
▪ Unternehmensschädliche Gesetzgebung und Rechtsprechung	❑ Ja	❑ Nein
▪ Demographische Entwicklung (z. B. Überalterung)	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 1: „Externe Risiken“

- Fachkräftemangel ❑ Ja ❑ Nein
- Wachsende Komplexität ❑ Ja ❑ Nein
- Neue Anforderungen durch Digitalisierung ❑ Ja ❑ Nein

- Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 2: „Management“

	relevant?	
▪ Persönliche zivil- und strafrechtliche Haftung wegen Pflichtverstoß bei unternehmerischer Tätigkeit (Managerhaftung)	❑ Ja	❑ Nein
▪ Unternehmensblockade: bei Konzentration der Kernfunktionen auf wenige Leistungsträger und fehlender Vertretungsregelung mit Wissensmanagement	❑ Ja	❑ Nein
▪ Persönliche Verluste bei Unternehmenskrise (Verlust von Arbeitsplatz, Reputation, Wohnung, Altersvorsorge wegen fehlender insolvenzsicherer Vermögensanlage etc.)	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 2: „Management“

relevant?

- Unternehmenskrise durch Nachfolgestreit oder Ausgleichszahlungen aufgrund fehlender Nachfolgeplanung, fehlender Abstimmung von Ehe-, Gesellschafts- und Erbverträgen bzw. Testament
  ❑ Ja ❑ Nein
- Unzureichende Altersvorsorge
  ❑ Ja ❑ Nein
- Ausfall durch burn out, Krankheit, Unfall, Tod
  ❑ Ja ❑ Nein
- Sonstiges: _____
  _____

Passauer Neue Presse, 09.03.2015:

"Unwissenheit schützt vor Strafe nicht“

von Stefan Holzinger

"Auf unseren Anklagebänken landen viele Geschäftsleute, die ins kalte Wasser geworfen werden",** sagte **Richter Klaus Fruth.

Sichtlich mitgenommen erschien am Amtsgericht eine 50-jährige Witwe. Ihr wird vorgeworfen, die Sozialversicherung um 23346,94 Euro geprellt zu haben – verteilt über einen Zeitraum von zwei Jahren habe sie keine Abgaben für einen ihrer Firmenmitarbeiter bezahlt. "Ich habe das nicht gewusst und dachte mir, das passt so", beteuerte die Frau immer wieder. Wie sich im Laufe der Verhandlung herausstellte, basiert das Vergehen auf sehr tragischen Umständen und Schicksalsschlägen:

Gatte stirbt an Herzinfarkt (…)
Er war es, der die Firma gegründet hatte. Sie bewegte sich stets im Hintergrund. (…) übernahm sie die Geschäftsführung nach dem Tod ihres Mannes .
Zu ihren Arbeitern gehörte ein Mann, der als Gewerbetreibender Aufträge für die Firma der Frau annahm. Allerdings ausschließlich für ihre Firma und in einem solchen Rahmen, dass er als regulärer Arbeitnehmer der Firma anzusehen sei.

"Ich war mir der Verantwortung nicht bewusst. (…) Er sagte mir, er sei selbstständig und habe auch auch andere Baustellen. Auch von einem eigenen Lastwagen war einmal die Rede. Das habe ich alles geglaubt, ohne es zu überprüfen“. (…)

Anschließend zogen sich Richter Fruth, Rechtsanwalt (…) und Staatsanwalt (…) zur Rechtsberatung zurück und kamen mit einer Einigung wieder: "Bei Geständnis verhängt das Gericht eine Gesamtstrafe zwischen sechs und zwölf Monaten − zur Bewährung", teilte Fruth mit. (…)

Weil sie auch noch nie im Konflikt mit dem Gesetz war und die Umstände, die zur Tat führten, sehr sehr schwierig gewesen seien, ist für Fruth die Strafe trotz des hohen finanziellen Schadens durchaus vertretbar. ***"Unwissenheit schützt leider vor Strafe nicht",*** *belehrte der Amtsrichter.*

Top-Risiken im Prozess-Themenfeld 3: „Governance“ (Unternehmensführung und –überwachung, Zusammenspiel der Organe)

	relevant?	
1. Interaktion der Organe (Gesellschafter, Geschäftsführer, Vorstand, Aufsichtsrat):	❑ Ja	❑ Nein
▪ Die Interaktion der Organe geschieht nicht mit einheitlichem Blick auf die Unternehmensstrategieentwicklung		
▪ Die Interaktion der Organe ist nicht harmonisch	❑ Ja	❑ Nein
2. Unternehmensführung:		
▪ Pflichtaufgaben der Unternehmensleitung ohne Ermessen werden nicht ermittelt und ausgeführt.	❑ Ja	❑ Nein
▪ Bei fakultativen Themen (mit Ermessenspielraum) wird die Business Judgment Rule nicht beachtet.	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 3: „Governance“ (Unternehmensführung und –überwachung, Zusammenspiel der Organe)

	relevant?	
▪ Die Unternehmensleitung überwacht das Unternehmen nicht in geeigneter und wirksamer Weise.	❑ Ja	❑ Nein
▪ Maßgebliche Schnittstellen (wie z.B. zu Internem Kontrollsystem/Risikomanagement) werden nicht sinnvoll bedient.	❑ Ja	❑ Nein
▪ Es gibt keine den Bedürfnissen des Unternehmens/ Konzerns entsprechende Überwachungsfunktion ("lines of defenses"), (z.B. IKS, Risk, Compliance, Controlling, QM, Interne Revision/Konzernrevision)	❑ Ja	❑ Nein
▪ Mangelnde Konsequenzen aus den Feststellungen und Empfehlungen der Überwachungsfunktion	❑ Ja	❑ Nein
▪ Fehlendes integriertes GRC-System	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 4: „Managementsystem(e)“ (QM, Risk, Compliance, etc.)

	relevant?	
• Insellösungen statt ein integriertes Managementsystem	❑ Ja	❑ Nein
• Unzureichendes Schnittstellenmanagement	❑ Ja	❑ Nein
• Unzureichende Analyse auf Schwachstellen	❑ Ja	❑ Nein
• Fehlende Kenntnis/Analyse, welche "Managementsysteme" Pflicht und welche freiwillig sind (z.B. Risiko-, Compliance-, Qualitäts-, Arbeitssicherheits-, Umwelt-, Personal, -etc.- Managementsystem)	❑ Ja	❑ Nein
• Unzureichende prozessorientierte Organisation	❑ Ja	❑ Nein
• Unzureichende IT-Unterstützung des Managementsystems	❑ Ja	❑ Nein
• Fehlendes Workflowmanagement / Digitalisierung der Prozesse	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 5: „Ziele, Strategie, Planung“

	relevant?	
▪ Unrealistische, nicht vorhandene, falsch formulierte oder verfehlte Ziele	❑ Ja	❑ Nein
▪ Fehlende oder fehlerhafte Strategie	❑ Ja	❑ Nein
▪ Fehlende oder nicht passende Kennzahlen (KPI‘s)	❑ Ja	❑ Nein
▪ Fehlentscheidungen durch „Bauchentscheidungen“	❑ Ja	❑ Nein
▪ Strategische Ausrichtung des Unternehmens wird von den Mitarbeitern nicht getragen / beachtet	❑ Ja	❑ Nein
▪ Nichtbeachtung der formulierten Leitlinien	❑ Ja	❑ Nein
▪ Unzureichende Kommunikation von Zielen und Strategie	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 6: „Organisation“

	relevant?	
▪ Differenz zwischen vorgegebener Organisationsstruktur und dem realen Aufbau und Ablauf im Unternehmen	❑ Ja	❑ Nein
▪ Abteilungsegoismus	❑ Ja	❑ Nein
▪ Verlangsamung der Prozesse durch zu viele Entscheidungswege und unflexiblen Organisationsaufbau	❑ Ja	❑ Nein
▪ Unzureichende Abstimmung von Aufgaben und Zuständigkeiten im Unternehmen (“Schnittstellenproblem“)	❑ Ja	❑ Nein
▪ Haftung wegen „Organisationsverschuldens“	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 7: „Finanzen / Steuern / Versicherungen“

	relevant?	
▪ Schlechte Kapitalstruktur (hoher Fremdkapitalanteil)	❑ Ja	❑ Nein
▪ Mangelhafte Liquiditätsplanung, Investitionsplanung und Fehlinvestitionen	❑ Ja	❑ Nein
▪ Fehlende „Tax-Compliance“	❑ Ja	❑ Nein
▪ Abhängigkeit von Gläubigern (Banken)	❑ Ja	❑ Nein
▪ Persönliche Mithaftung (z.B. über Bürgschaft)	❑ Ja	❑ Nein
▪ Veruntreuung / Unterschlagung	❑ Ja	❑ Nein
▪ Mangelhaftes Forderungsmanagement	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 8: „Personal“

	relevant?	
▪ Hohe Fluktuation	❑ Ja	❑ Nein
▪ Zu hohe Personalkosten	❑ Ja	❑ Nein
▪ Kriminelles Verhalten von Mitarbeitern	❑ Ja	❑ Nein
▪ Fehlende Motivation der Mitarbeiter	❑ Ja	❑ Nein
▪ Haftungs- und Prozessrisiken aufgrund des komplexen und sich ständig ändernden Arbeitsrechts	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 8: „Personal“

	relevant?	
▪ Zu wenig qualifizierte Mitarbeiter	❑ Ja	❑ Nein
▪ Austritt von Leistungsträgern	❑ Ja	❑ Nein
▪ Sonstiges: _____		
_____		

Top-Risiken im Prozess-Themenfeld 9: „Risikomanagementsystem“

	relevant?	
• Kein integriertes Risiko-Managementsystem	❑ Ja	❑ Nein
• Es existiert kein effektiver Risikomanagement-Prozess	❑ Ja	❑ Nein
• Maßnahmen zur Risikobewältigung werden nicht nachgehalten	❑ Ja	❑ Nein
• Top-Risiken des Unternehmens sind nicht bekannt	❑ Ja	❑ Nein
• Unzureichende Definition von Frühwarnsignalen und Maßnahmen, mit deren Hilfe bestandsgefährdende Risiken rechtzeitig erkannt und gesteuert werden können	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 10: „Compliance-Anforderungen“ (rechtliche / gesetzliche / behördliche)

	relevant?	
• Fehlendes integriertes Compliance-Managementsystem	❑ Ja	❑ Nein
• Compliance wird nicht gelebt	❑ Ja	❑ Nein
• Legalitätspflichten und/oder freiwillig gesetzte Regelungen sind nicht bekannt	❑ Ja	❑ Nein
• Legalitätspflichten und/oder freiwillig gesetzte Regelungen werden nicht (vollständig) eingehalten	❑ Ja	❑ Nein
• Es existiert keine passende Überwachung	❑ Ja	❑ Nein
• Es existiert keine passende Reaktion bei Verstößen	❑ Ja	❑ Nein
• Kunden, Behörden oder Sonstige fordern vermehrt den Nachweis von Compliance	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 10: „Compliance-Anforderungen“ (rechtliche / gesetzliche / behördliche)

	relevant?	
• Es gibt keine verbindlichen Anweisungen/ Informationsflüsse bzgl. Compliance an die Mitarbeiter	❑ Ja	❑ Nein
• Es gibt keine Vorkehrungen zur Korruptionsprävention	❑ Ja	❑ Nein
• Es existiert kein passendes (anonymes) Meldewesen/Hinweisgebersystem	❑ Ja	❑ Nein
• Prozessabläufe sind nicht mit Compliance-Komponenten angereichert	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 11: „Forschung & Entwicklung/Innovation/Anpassung an Umfeld-Veränderungen“

	relevant?	
▪ Fehlende Leistungsfähigkeit und Zuverlässigkeit neu entwickelter Produkte/Leistungen	❑ Ja	❑ Nein
▪ Nichteinhaltung von Terminen bei Entwicklungen	❑ Ja	❑ Nein
▪ Mangelnde Abstimmungen von F&E mit Abteilung Vertrieb und Einkauf	❑ Ja	❑ Nein
▪ Fehlendes Verständnis des Kundenwunsches/ der Marktanforderungen	❑ Ja	❑ Nein
▪ Verletzung von Patenten	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 11: „Forschung & Entwicklung/Innovation/Anpassung an Umfeld-Veränderungen“

	relevant?	
▪ Unzureichende Innovation	❑ Ja	❑ Nein
▪ Fehlende Alleinstellungsmerkmale (unique selling points (usp‘s))	❑ Ja	❑ Nein
▪ Unzureichende Maßnahmen für Umstellung auf Digitalisierung und „4.0“	❑ Ja	❑ Nein

▪ Sonstiges: _____

_____

Top-Risiken im Prozess-Themenfeld 12: „Beschaffung“

	relevant?	
▪ Qualitätsdefizite der gelieferten Produkte/Leistungen, Falschlieferungen oder verspätete Lieferungen	❑ Ja	❑ Nein
▪ Negative Preisentwicklung	❑ Ja	❑ Nein
▪ Keine ausreichende Abstimmung mit Abteilung Produktion/F&E/Vertrieb	❑ Ja	❑ Nein
▪ Lieferantenabhängigkeit	❑ Ja	❑ Nein
▪ Zu hoher Lagerbestand	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 12: „Beschaffung“

	relevant?	
▪ Lieferantenausfall	❑ Ja	❑ Nein
▪ Fehlende Sicherstellung von Compliance und Nachhaltigkeit beim Lieferant	❑ Ja	❑ Nein
▪ Unzureichende Überwachung bei Delegationen auf Externe	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 13: „Leistungserbringung / Produktion / Handel / etc.“

	relevant?	
▪ Qualitätsprobleme	❑ Ja	❑ Nein
▪ Betriebsunterbrechung (z. B. Maschinenausfall)	❑ Ja	❑ Nein
▪ Zu kostenintensive Produktion / Unzureichende Standardisierung / Digitalisierung	❑ Ja	❑ Nein
▪ Betriebsunfälle	❑ Ja	❑ Nein
▪ Produkthaftungsfälle	❑ Ja	❑ Nein
▪ Terminprobleme	❑ Ja	❑ Nein
▪ Probleme mit rechtlichen Anforderungen („Product Compliance“)	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 14: „Marketing / Vertrieb“

	relevant?	
▪ Fehlende Übereinstimmung zwischen Unternehmenszielen / Strategie und Marketingstrategien	❑ Ja	❑ Nein
▪ Zielgruppenverfehlung	❑ Ja	❑ Nein
▪ Verlust von Marktanteilen bzw. keine Marktanteilserweiterung durch fehlendes oder wirkungsloses Marketing	❑ Ja	❑ Nein
▪ Haftung für rechtswidrige Werbung	❑ Ja	❑ Nein
▪ Transportrisiko	❑ Ja	❑ Nein
▪ Abnehmende Kundenzufriedenheit	❑ Ja	❑ Nein
▪ Verlust eines Schlüsselkunden	❑ Ja	❑ Nein
▪ Rechtsstreitigkeiten	❑ Ja	❑ Nein
▪ Kundenbedürfnisse werden nicht erkannt	❑ Ja	❑ Nein
▪ Umsatzrückgänge	❑ Ja	❑ Nein
▪ Sonstiges: _____		
_____		

Top-Risiken im Prozess-Themenfeld 15: „IT“

	relevant?	
▪ Unternehmensblockade und Datenverlust durch Serverausfall	❑ Ja	❑ Nein
▪ Fehlende Zugriffskontrollen	❑ Ja	❑ Nein
▪ Datenverlust	❑ Ja	❑ Nein
▪ IT-Missbrauch durch die Mitarbeiter	❑ Ja	❑ Nein
▪ Missbrauch durch betriebsfremde Personen	❑ Ja	❑ Nein
▪ Fehlende Verschlüsselung	❑ Ja	❑ Nein
▪ Unzureichende Datensicherung	❑ Ja	❑ Nein
▪ Sicherheitsrisiken im Bereich Information und Kommunikation IuK (VoIP, Handy etc.)	❑ Ja	❑ Nein
▪ Verseuchung durch Viren, Würmer, Trojaner	❑ Ja	❑ Nein
▪ „Cyber-Risks“ (IT-Sicherheit / Datenschutz / …)	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 16: „Wissens-/ Informationsmanagement, Kommunikation“

	relevant?	
▪ Sammlung unnötiger / falscher Informationen	❑ Ja	❑ Nein
▪ Unzureichende Pflege (Inputs) der Daten	❑ Ja	❑ Nein
▪ Fehlende bzw. unpassende technische Grundlage	❑ Ja	❑ Nein
▪ Datenklau (Betriebsspionage)	❑ Ja	❑ Nein
▪ Fehlende oder fehlerhafte Festlegung der Zugriffsrechte	❑ Ja	❑ Nein
▪ Unterbrochener Informationsfluss	❑ Ja	❑ Nein
▪ Zurückhaltung von Informationen	❑ Ja	❑ Nein
▪ Sonstiges: _____	❑ Ja	❑ Nein
_____		

Top-Risiken im Prozess-Themenfeld 17: „Dokumentation“

	relevant?	
• Unzureichendes Dokumentations-Managementsystem	❑ Ja	❑ Nein
• Unübersichtliche/unklare Dokumentenverwaltung	❑ Ja	❑ Nein
• Unzureichende Dokumentenlenkung (inkl. Freigabe-, Zugriffsrechte, etc.)	❑ Ja	❑ Nein
• Veraltete Daten/Informationen	❑ Ja	❑ Nein
• Datenklau (Betriebsspionage)	❑ Ja	❑ Nein
• Fehlende oder fehlerhafte Festlegung der Zugriffsrechte	❑ Ja	❑ Nein
• Fehlende Integrität oder fehlende Verfügbarkeit der Daten	❑ Ja	❑ Nein
• Fehleranfällige Speichermedien	❑ Ja	❑ Nein
• Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 18: „Rechnungswesen / Controlling“

	relevant?	
▪ Controlling nicht auf die Größe des Unternehmens abgestimmt	❑ Ja	❑ Nein
▪ Fehlende / geringe Aussagekraft und Verständlichkeit von Controllinginstrumenten	❑ Ja	❑ Nein
▪ Fehlende Transparenz bei der Kostenaufstellung	❑ Ja	❑ Nein
▪ Unzureichende Nachkalkulation	❑ Ja	❑ Nein
▪ Fehlendes oder mangelhaftes Controlling	❑ Ja	❑ Nein
▪ Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 19: „Qualitätsmanagement“

	relevant?	
• Fehlendes integriertes Qualitäts-Managementsystem	❑ Ja	❑ Nein
• Falsch bzw. nicht gelebtes Qualitätsmanagement im Unternehmen	❑ Ja	❑ Nein
• Überzogenes, zu teures, nicht praxisbezogenes Qualitätsmanagement	❑ Ja	❑ Nein
• Fehlende Kontrollen über den kompletten QM-Prozess	❑ Ja	❑ Nein
• Verlust von Marktanteilen/Kunden durch schlechte Produkt- oder Servicequalität	❑ Ja	❑ Nein

Top-Risiken im Prozess-Themenfeld 19: „Qualitätsmanagement“

	relevant?	
• Persönliche zivil- und strafrechtliche Haftung von Unternehmern und Mitarbeitern sowie unvorhersehbare Schadenersatzforderungen aufgrund eines Haftungsfalles	❑ Ja	❑ Nein
• Qualitäts-Managementsystem weist nicht die inzwischen geforderten Komponenten von Risiko- und Compliancemanagement auf	❑ Ja	❑ Nein
• Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 20: „Security / Safety“

	relevant?	
• Fehlendes (integriertes) Security-/ Safety-Managementsystem	❑ Ja	❑ Nein
• Unzureichender Datenschutz	❑ Ja	❑ Nein
• Unzureichender Gebäudeschutz	❑ Ja	❑ Nein
• Unzureichender Brandschutz	❑ Ja	❑ Nein
• Unzureichender Arbeitsschutz/ Arbeitssicherheit	❑ Ja	❑ Nein
• Unzureichende Produktionssicherheit	❑ Ja	❑ Nein
• Cyber/IT-Sicherheits-Risiken	❑ Ja	❑ Nein
• Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 21: „Business Continuity“

	relevant?	
• Unzureichendes Notfall-, /Krisen- und Kontinuitätsmanagementsystem	❑ Ja	❑ Nein
• Fehlende, aktuelle Business-Impact-Analyse	❑ Ja	❑ Nein
• Fehlende Notfallpläne in den diversen Prozessthemenbereichen (IT, Leistungserstellung, Personal, Finanzen, etc.)	❑ Ja	❑ Nein
• Unzureichende Risiko-Früherkennungssystem	❑ Ja	❑ Nein
• Sonstiges: _____ _____		

Top-Risiken im Prozess-Themenfeld 22: „Sonstige“

- Welche sonstigen (Prozess-) Themenbereiche sind in Ihrem Unternehmen wichtig/relevant (z.B. Logistik, Projektmanagement, etc.)?

  _____
  _____
  _____

- Welche möglichen Risiken oder Chancen sehen Sie in diesen weiteren (Prozess-) Themenbereichen?

  _____
  _____
  _____

relevant?

- Projektmanagement ❑ Ja ❑ Nein
- Logistik ❑ Ja ❑ Nein

- Welche Themen spielen bei Ihnen außerdem eine Rolle?

  _____
  _____

- Sonstiges:

  _____
  _____

Bewerten Sie bitte die folgenden Bereiche Ihres Unternehmens in Bezug auf das Gefahren- und Chancenpotenzial:

	Gefahren		Chancen	
	hoch	**gering**	**hoch**	**gering**
1 Externe Risiken (z. B. Rezession, Globalisierung)	❑	❑	❑	❑
2 Unternehmerrisiko (z. B. plötzlicher Ausfall, Managerhaftung)	❑	❑	❑	❑
3 Governance (Unternehmensführung und -überwachung, Zusammenspiel der Organe)	❑	❑	❑	❑
4 Managementsystem(e) (QM, Risk, Compliance, etc.)	❑	❑	❑	❑
5 Strategie (z. B. fehlende oder nicht konsequent umgesetzte Strategie)	❑	❑	❑	❑
6 Organisation (z. B. Organisationsverschulden / ineffiziente Abläufe)	❑	❑	❑	❑
7 Finanzen (z. B. Kreditverknappung / Forderungsausfälle)	❑	❑	❑	❑
8 Personal (z. B. Ausfall des Leistungsträgers)	❑	❑	❑	❑
9 Risikomanagementsystem	❑	❑	❑	❑
10 Compliance-Anforderungen	❑	❑	❑	❑

	Gefahren		Chancen	
	hoch	**gering**	**hoch**	**gering**
11 F & E (z. B. geringes Innovationspotenzial)	❑	❑	❑	❑
12 Beschaffung (z. B. Lieferantenaufsfallrisiko)	❑	❑	❑	❑
13 Leistungserbringung (z. B. Produktqualitätsprobleme)	❑	❑	❑	❑
14 Vertrieb (z. B. sinkende Umsätze)	❑	❑	❑	❑
15 IT (z. B. Serverausfall)	❑	❑	❑	❑
16 Wissens-/Infomanagement (z. B. fehlendes bzw. nicht umgesetztes Konzept)	❑	❑	❑	❑
17 Dokumentation	❑	❑	❑	❑
18 Controlling (z. B. fehlende konsequente Umsetzung)	❑	❑	❑	❑
19 Qualitätsmanagement	❑	❑	❑	❑
20 Security/Safety	❑	❑	❑	❑
21 Business Continuity	❑	❑	❑	❑
22 Sonstige	❑	❑	❑	❑

Ziele-, Organisations-, sowie Steuerungs- und Überwachungssystem

Ziele

Bzgl. der **Ziele unternehmerischen Handelns** sind die

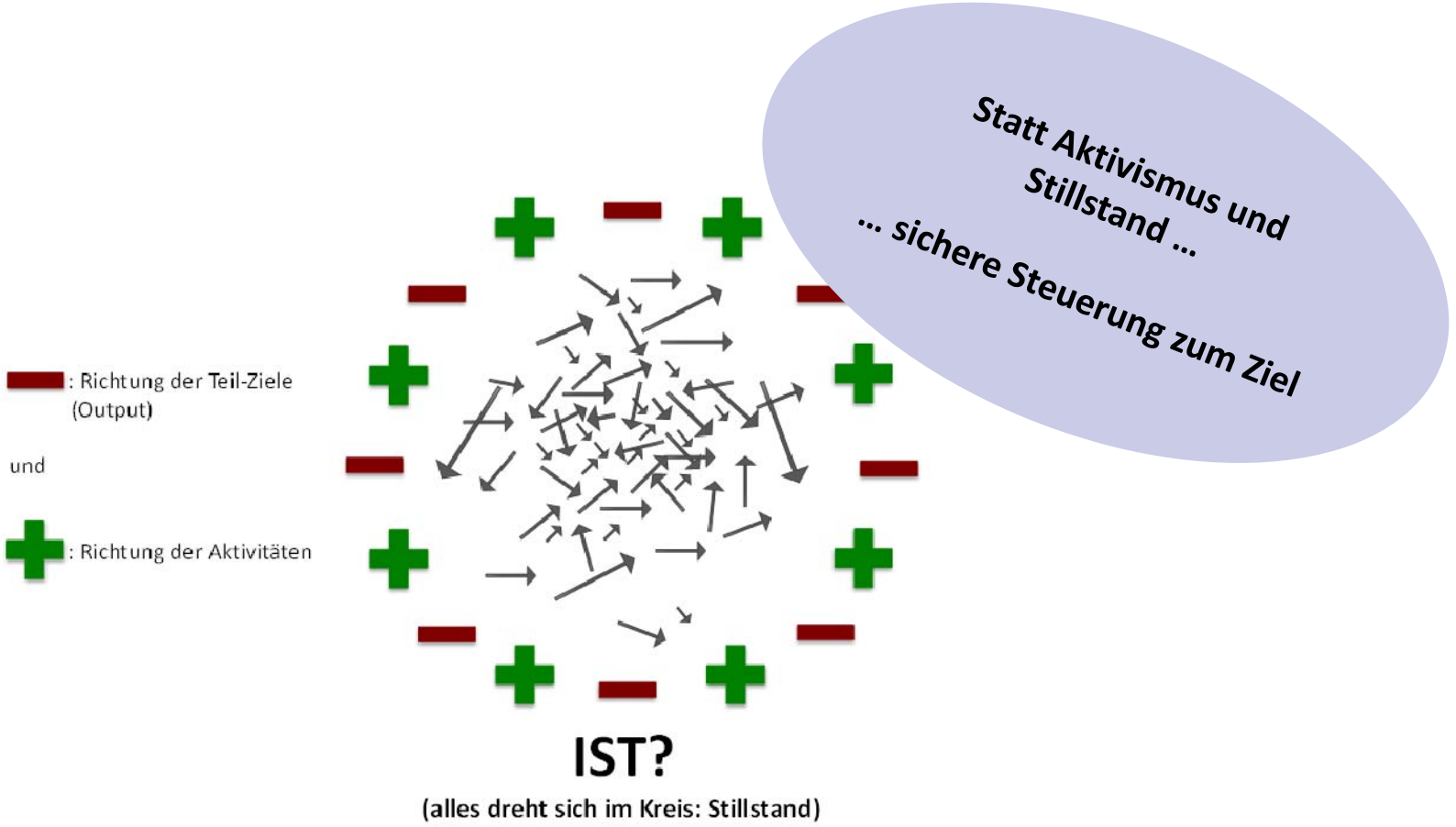
- (gemeinsamen) unternehmerischen Ziele der Organe (Geschäftsführer / Vorstand, Gesellschafter, Aufsichtsgremium), Mitarbeiter und sonstigen „interested parties“

zu differenzieren von den

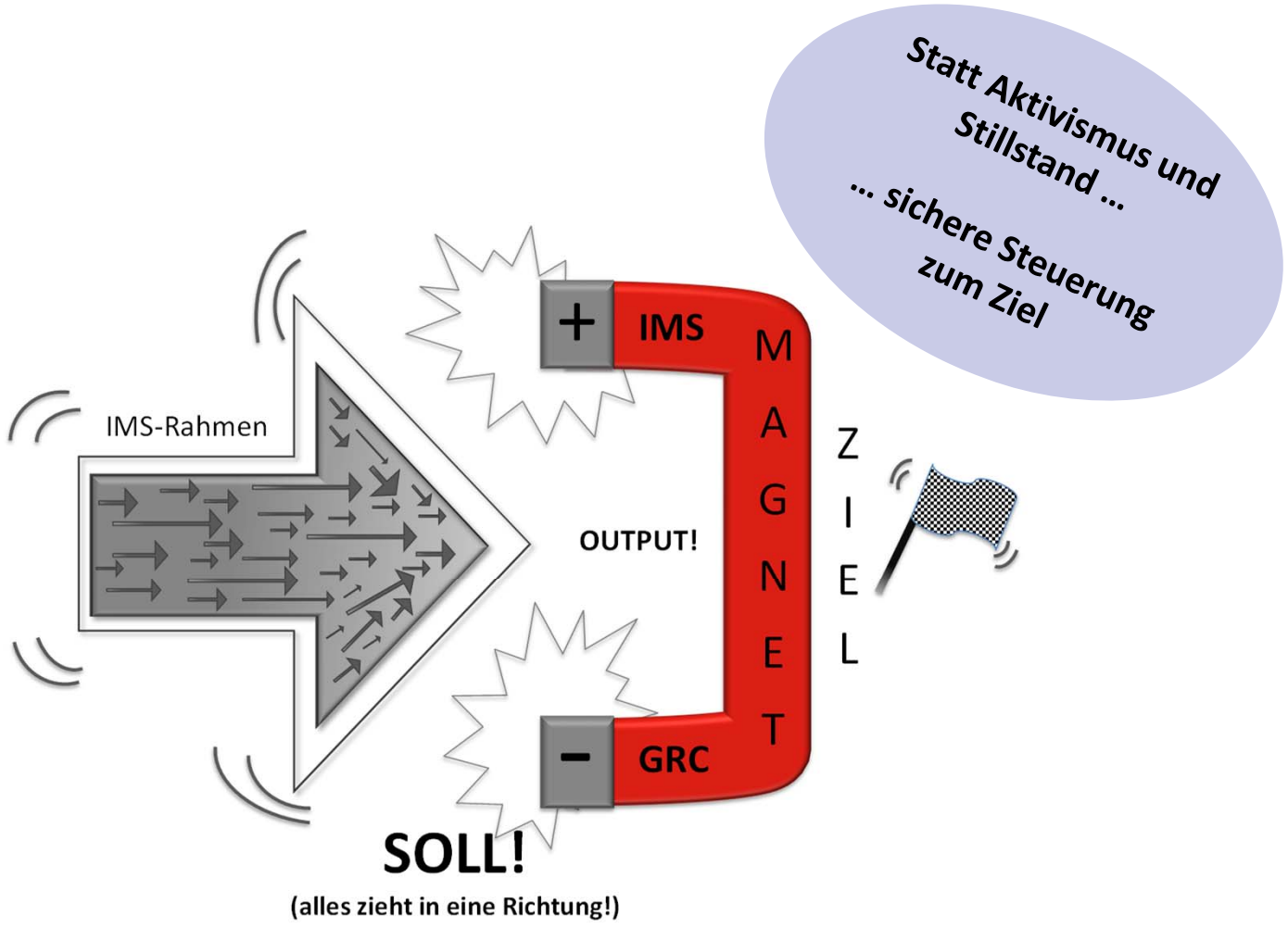
- persönlichen (beruflichen) Zielen der jeweils Agierenden.

Während in **der Praxis sehr viele Aktivitäten in unterschiedliche Ziel-Richtungen** zu dem Ergebnis führen, dass sich „alles im Kreise dreht“ oder sogar zu **Stillstand bzw. Rückschritt,** sollte idealerweise ein **Integriertes Managementsystem wie ein „starker Magnet“ die Aktivitäten gebündelt in die richtige Zielrichtung** ziehen: Vgl. nachfolgende Abbildung:

Homogenes Ziel-Kennzahlensystem, heruntergebrochen auf Prozessziele



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand, -Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017, <IMS>

Zum Thema zukunftsorientierte Unternehmensführung und Digitalisierung

Erstellen Sie regelmäßig (mindestens 1x im Jahr) eine dokumentierte **Umfeld- und Interested Parties-Analyse** für Ihr Unternehmen, in der Rahmenbedingungen, Trends und Branchenentwicklungen, wie z.B. demografische Entwicklung, Ressourcen-verknappung, Globalisierung, volatile Märkte, wachsende und sich ändernde Kunden-bedürfnisse weltweit, etc. berücksichtigt werden?

- ❑ Ja
- ❑ Nein

Haben Sie eine dokumentierte und regelmäßig den ex- und internen Veränderungen und den Herausforderungen des Wandels **angepasste Vision und Strategie?**

- ❑ Ja
- ❑ Nein

Zum Thema zukunftsorientierte Unternehmensführung und Digitalisierung

Kennen Sie die **Erfolgspotenziale** Ihres Unternehmens und sind die Risiken sowie Chancen, welche die Erfolgspotenziale negativ bzw. positiv beeinflussen können, dokumentiert?

- ❑ Ja
- ❑ Nein

Kennen und erfüllen Sie die aktuellen Anforderungen an eine **rechtssichere Unternehmensorganisation** (Compliance)?

- ❑ Ja
- ❑ Nein

Zum Thema zukunftsorientierte Unternehmensführung und Digitalisierung

Sind Sie der Meinung, dass sich die **rechtlichen Anforderungen** an Unternehmen und Managern in den letzten 5 Jahren stark **verschärft** haben?

- ❑ Ja
- ❑ Nein

Finden Sie die **„Compliance-Diskussion“**

- ❑ förderlich
- ❑ rein theoretisch
- ❑ nicht förderlich

Zum Thema zukunftsorientierte Unternehmensführung und Digitalisierung

Versuchen Sie konzeptionell, die **Chancen und Risiken möglicher künftiger Entwicklungen und/oder Trends** zu erkennen, zu bewerten und Maßnahmen daraus abzuleiten?

- ❑ Ja
- ❑ Nur sporadisch
- ❑ Nein

Kennen/nutzen Sie ausreichend **Informationsquellen** bezüglich der Sie / Ihr Unternehmen betreffenden Zukunftstrends?

- ❑ Ja
- ❑ Nein

Zum Thema zukunftsorientierte Unternehmensführung und Digitalisierung

Fühlen Sie sich von Ihrem **Fachverband** (z.B. VDI, VDA, VDMA, BayME, ...) ausreichend unterstützt?

- ❑ Ja
- ❑ Nein

Fühlen Sie sich von den **Industrie- und Handelskammern** bzw. **Handwerkskammern** ausreichend unterstützt?

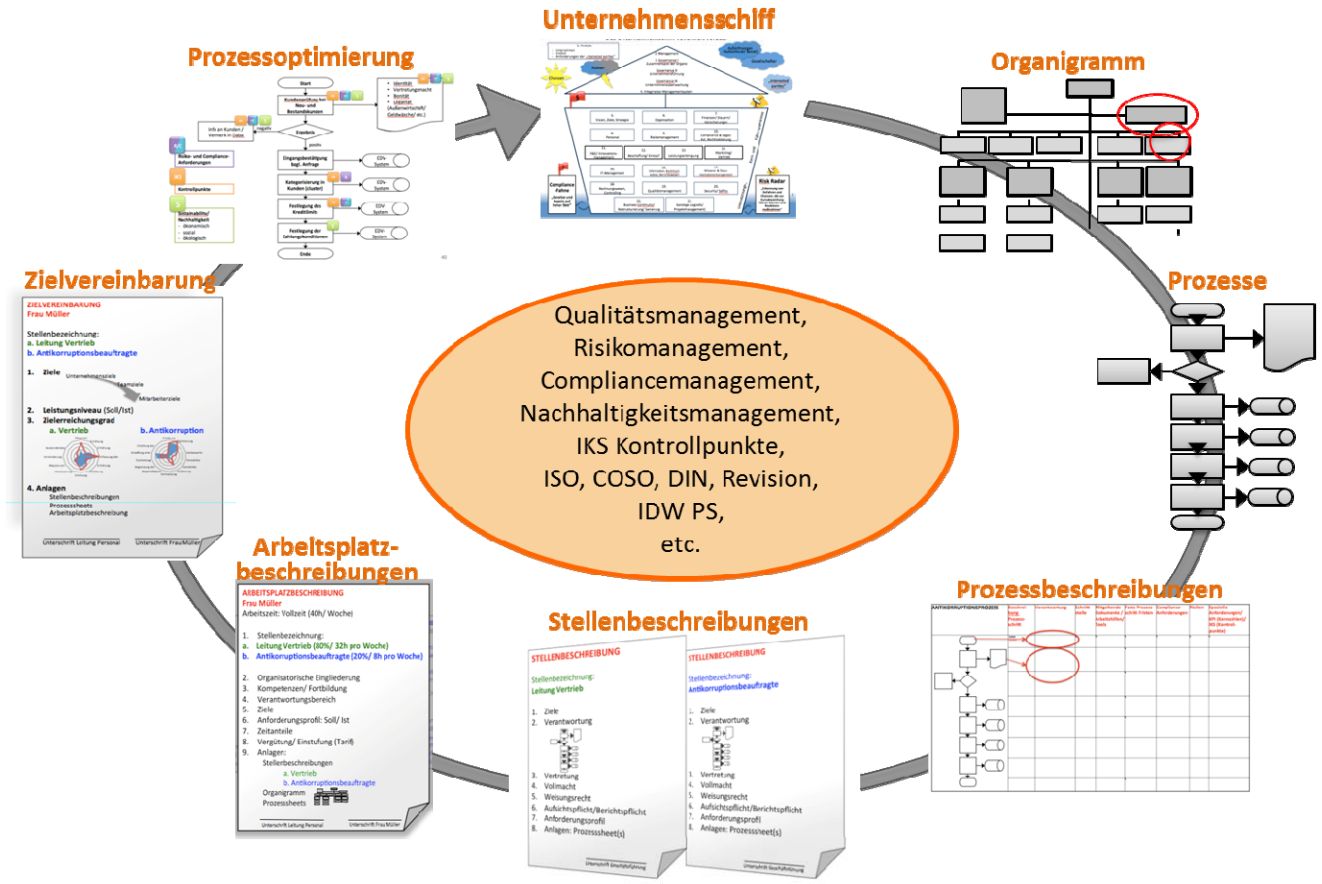
- ❑ Ja
- ❑ Nein

Sehen Sie den Wald vor lauter Bäumen nicht mehr so richtig?

Quelle: *Scherer / Fruth* (Hrsg.), Governance-Management Band II, 2016, S. 34

4. Prozessorientierte Organisation / Die Evolution des Prozessmanagements

Integriertes Qualitätsmanagement mit GRC



Haben Sie

Rechtssichere Organisation?

ja ☐ ☐ nein

Rechtssichere Delegation?

ja ☐ ☐ nein

Rechtssichere Stellenbeschreibungen?

ja ☐ ☐ nein

Haben Sie

Rechtssichere Arbeitsplatzbeschreibungen?

ja ☐ ☐ nein

Rechtssichere Zielvereinbarungen?

ja ☐ ☐ nein

Rechtssichere Prozessabläufe?

ja ☐ ☐ nein

Lösungen:

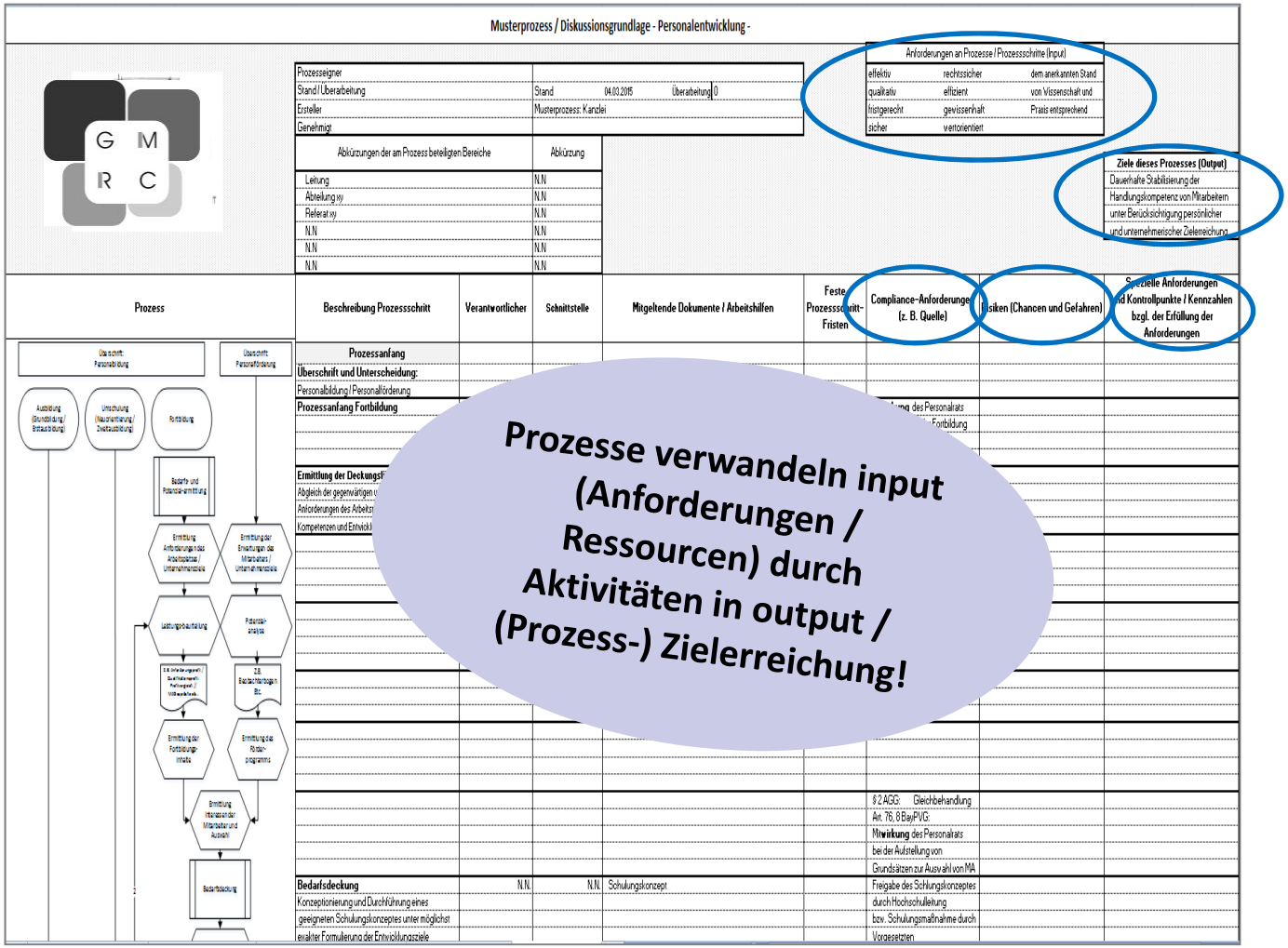
Rechtssichere Organisation:

❑ Einzelne Komponenten

Z. B.

1. Stellenbeschreibungen ❑
2. Zielvereinbarungen ❑
3. Aufsichtsratsfunktion im Prüfungsausschuss gem. § 107 AktG (Überwachung der Wirksamkeit von Risk / Compliance / IKS / Revision) ❑
4. Hinweisgebersystem / Ombudsmannsystem ❑
5. Prozessabläufe ❑
6. Etc. ❑

Prozesse: Ziele setzen, Input, Aktivitäten, Output, Ziele erreichen!



Erklärung: Neu! *Der Standard für Qualitätsmanagement 9001:2015 fordert im Rahmen des „Prozessmanagements" die Berücksichtigung diverser Komponenten, wie z.B. aus Compliance und Risk. Das Muster-Prozesssheet erfüllt diese Anforderungen.*

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 66 ff.

DIN EN ISO 9001:2015-11
EN ISO 9001:2015 (D/E)

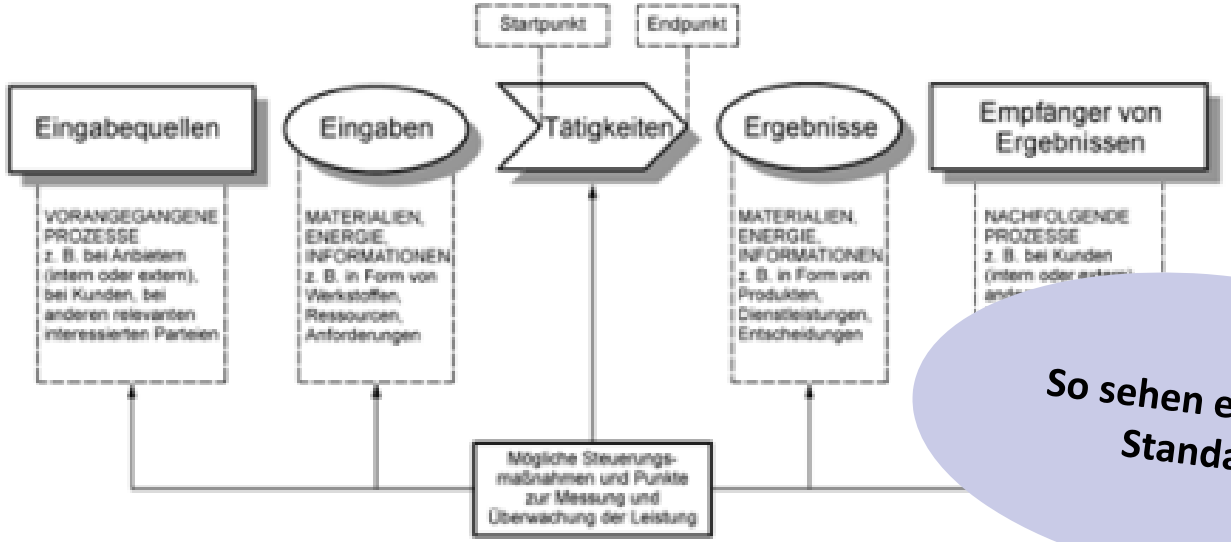


Bild 1 — Schematische Darstellung der Elemente eines Einzelprozesses

So sehen es die ISO-Standards!

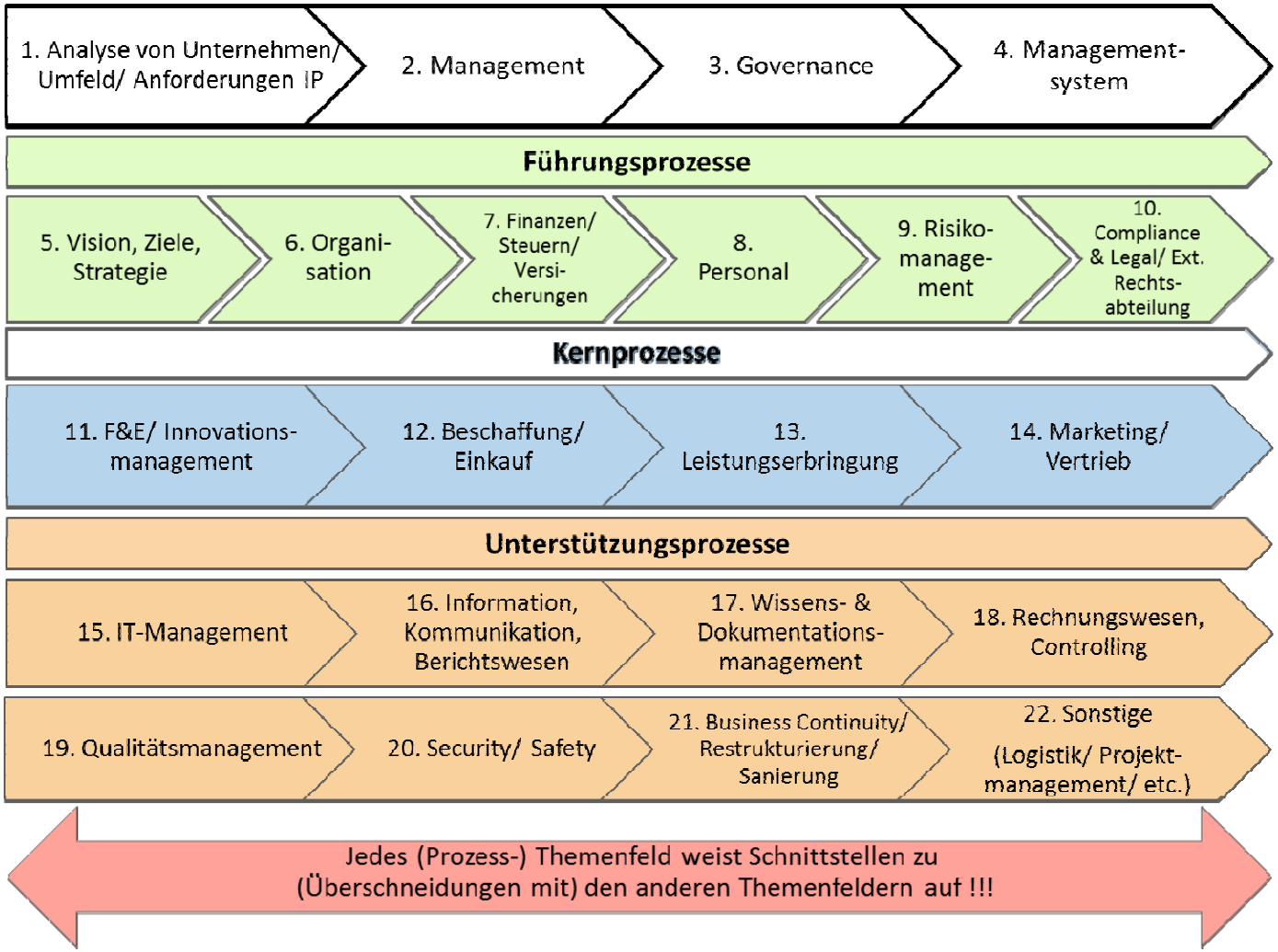
Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Prozessabläufe nach „Anerkanntem Stand von Wissenschaft und Praxis“

*Es **muss** eine nach Unternehmensbereichen / (Prozess-) Themenfeldern sortierte Prozesslandkarte bzw. „Prozess-Matrix“ erstellt werden, die dokumentiert, dass die für das jeweilige Unternehmen erforderlichen Prozesse vorhanden sind.*

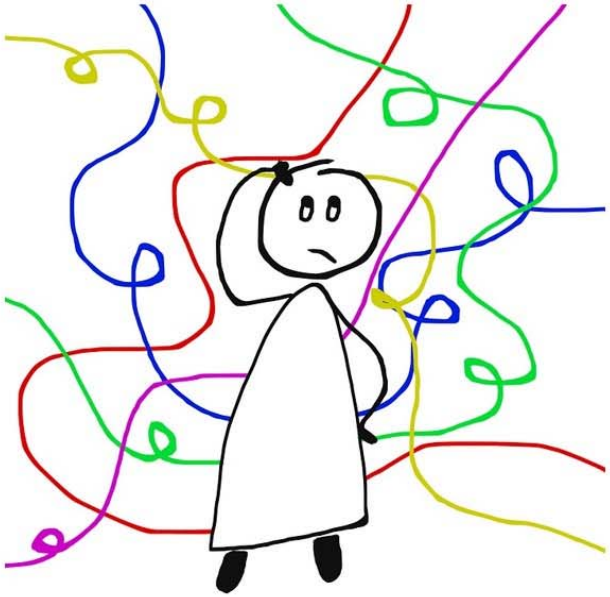
*Diese Prozesse wiederum **müssen** so angereichert werden,*
dass sie die Erfüllung diverser Compliance-Management-Anforderungen und die Erreichung der Compliance-Management-Prozessziele gewährleisten.

Prozesslandkarte



Die „Evolution“ des Prozessmanagements

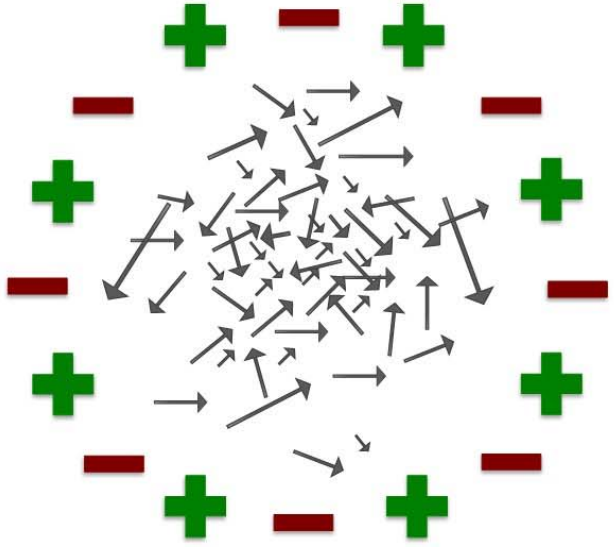
Evolutionsstufe 1 **Der Prozess existiert noch nicht, bzw. nur im Kopf!**



: Richtung der Teil-Ziele (Output)

und

: Richtung der Aktivitäten



„GRC“ als Basis für Digitalisierung, Industrie 4.0 und workflow-Management

Unternehmen, Manager und Mitarbeiter stoßen vor neue

Herausforderungen bei ihrer täglichen Arbeit

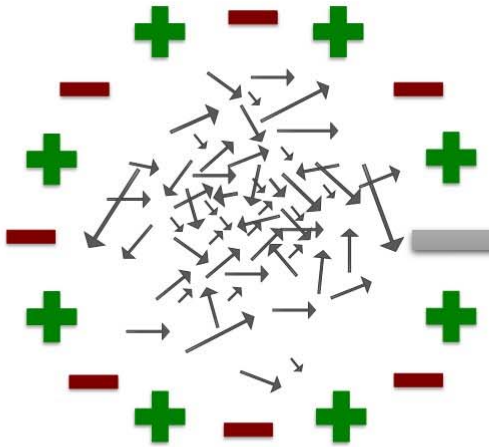
Häufig wird der **Unternehmensalltag** noch durch E-Mails, Excel-Tabellen und mit MS-Office bestritten.

Die Prozesse sind oft nicht dokumentiert oder nicht aktuell, beziehungsweise nicht nachverfolgbar.

Bei **Prozess-Anpassungen** müssen teure IT Spezialisten erst mal die Zeit finden, um die Unternehmen zu unterstützen.

E-Mails werden nach Gießkannenprinzip an alle verteilt.

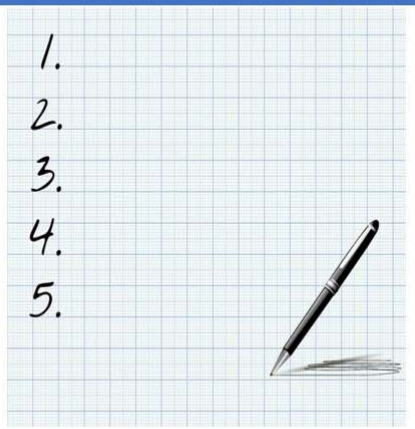
Evolutionsstufe 2 Vom Kopf zu Papier!



IST?

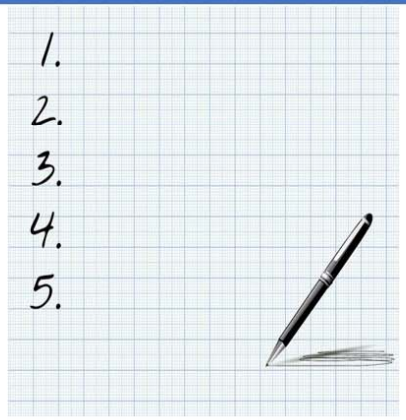
(alles dreht sich im Kreis: Stillstand)

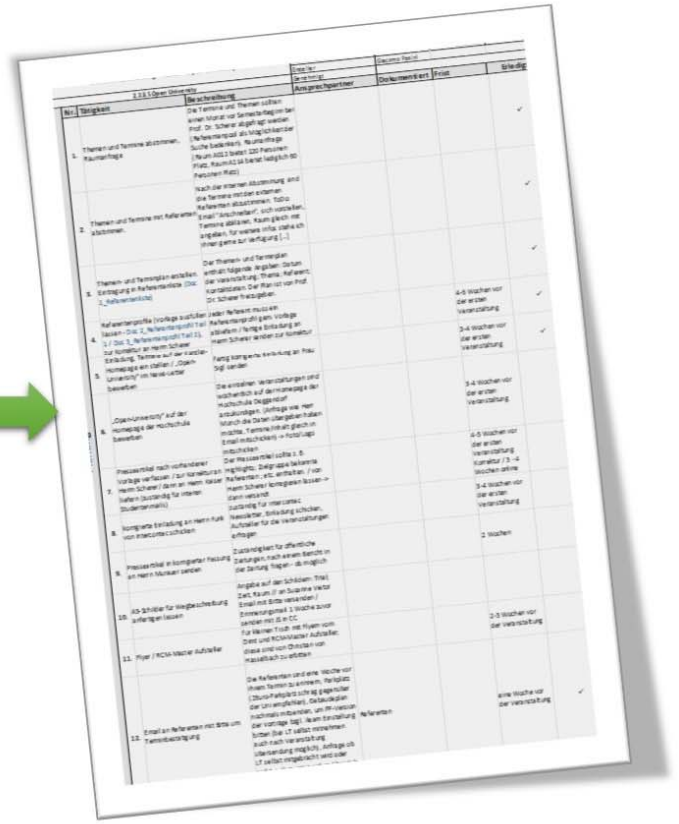
Schritt für Schritt – es entsteht ein Prozess (zumindest auf dem Papier)



Evolutionsstufe 3 Vom analogen Papier zum digitalen Dokument/Tool!

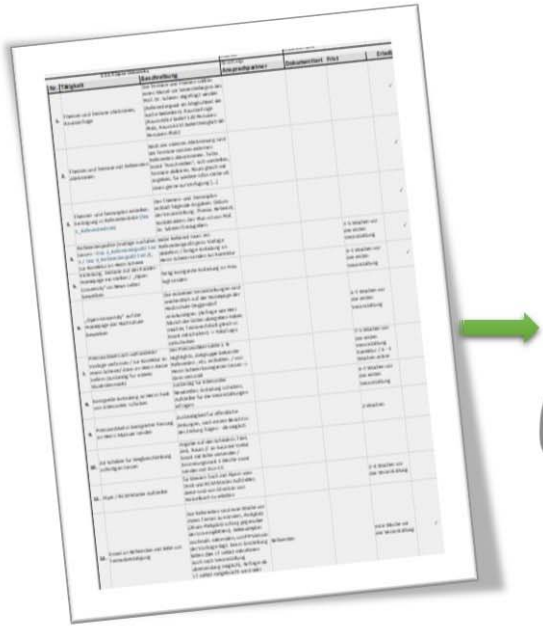
Handschriftlich dokumentierte Prozessschritte

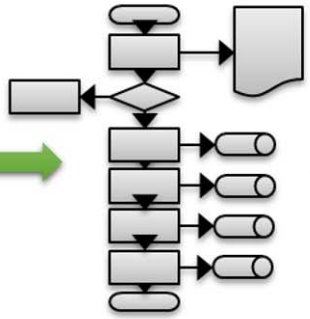


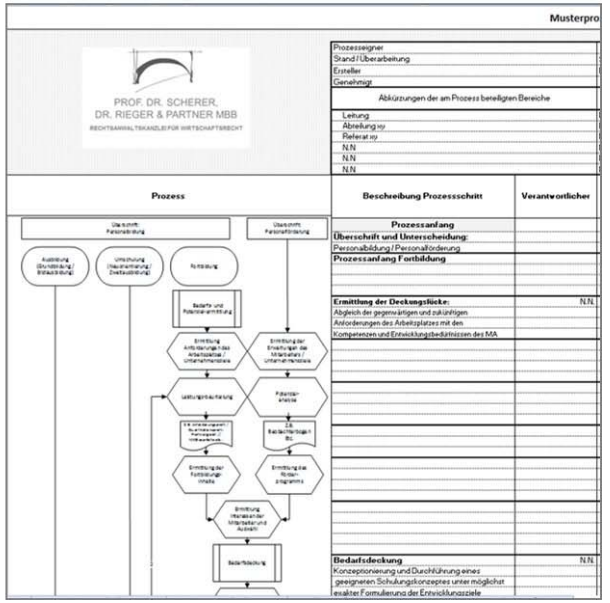


Evolutionsstufe 4

„Super Idee“ – wieso nicht die Prozessschritte visualisieren!? Und dann auch noch alle relevanten Informationen den einzelnen Prozessschritten anhängen!?

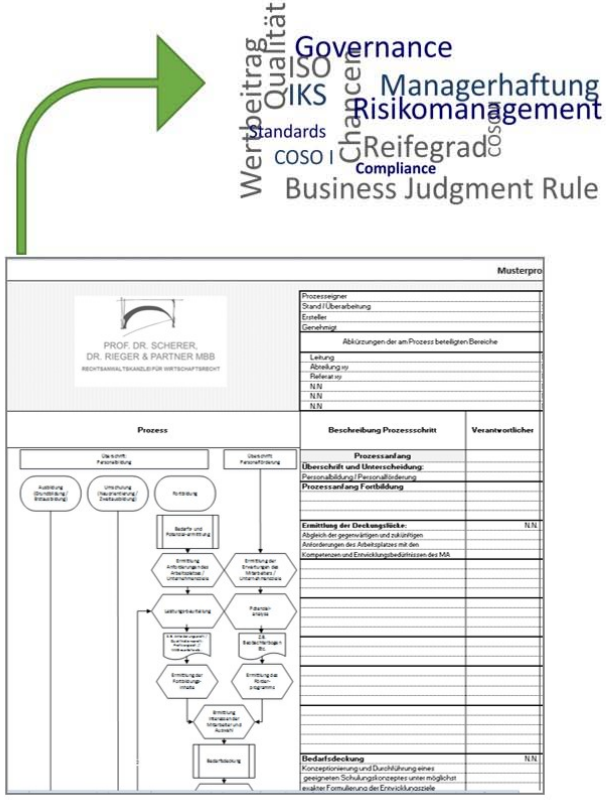


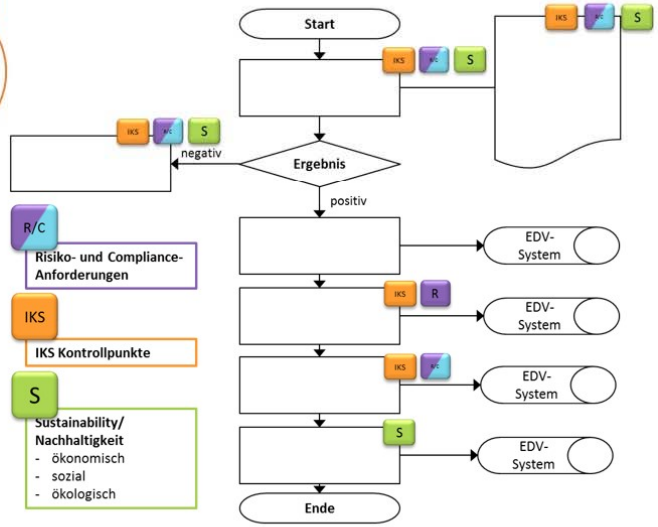




Sofern Prozesse existieren, sind diese häufig nicht ausreichend mit **Governance-, Risk-, oder Compliance-Komponenten** angereichert oder **konform** mit gängigen ISO- / IDW- / etc.- **Standards.**

Evolutionsstufe 5 **Angereicherte Prozesse? Wieso denn nicht?**



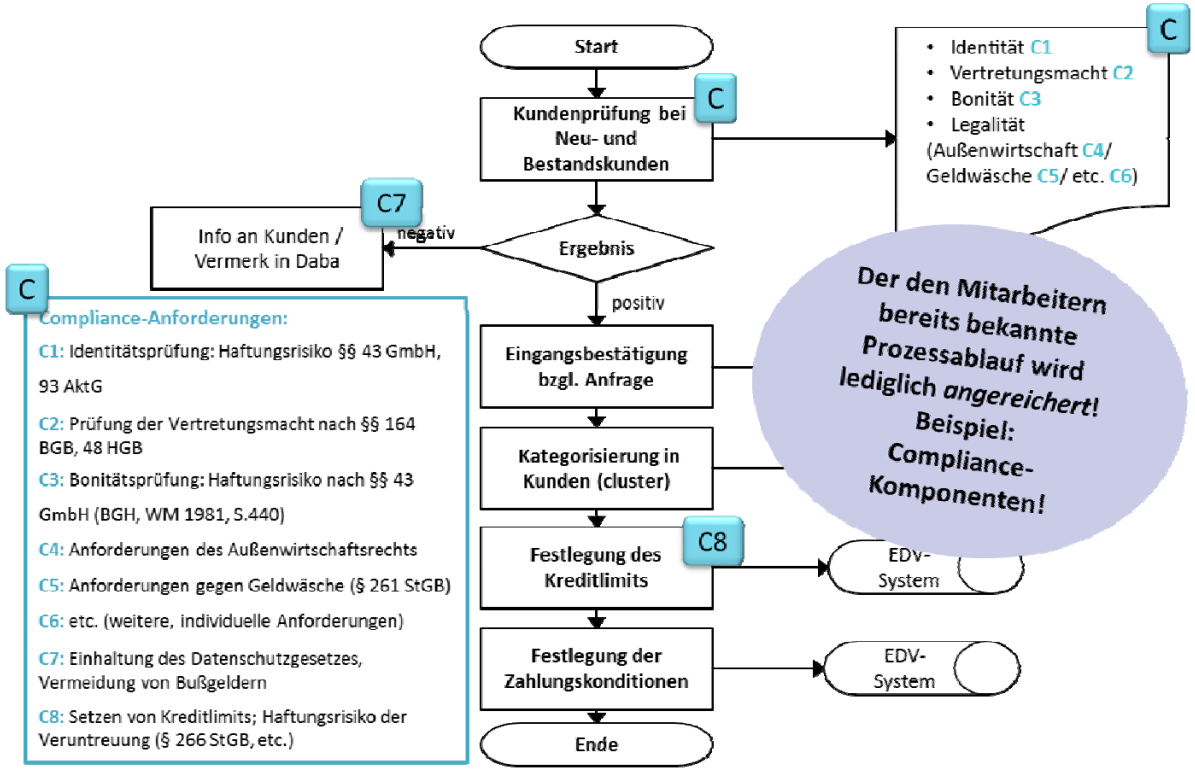


Anreicherung von Prozessen mit GRC-Komponenten unter Beachtung der Standards!

Hier: Die Anreicherung der Basis-Prozesse mit Komponenten aus Compliance:

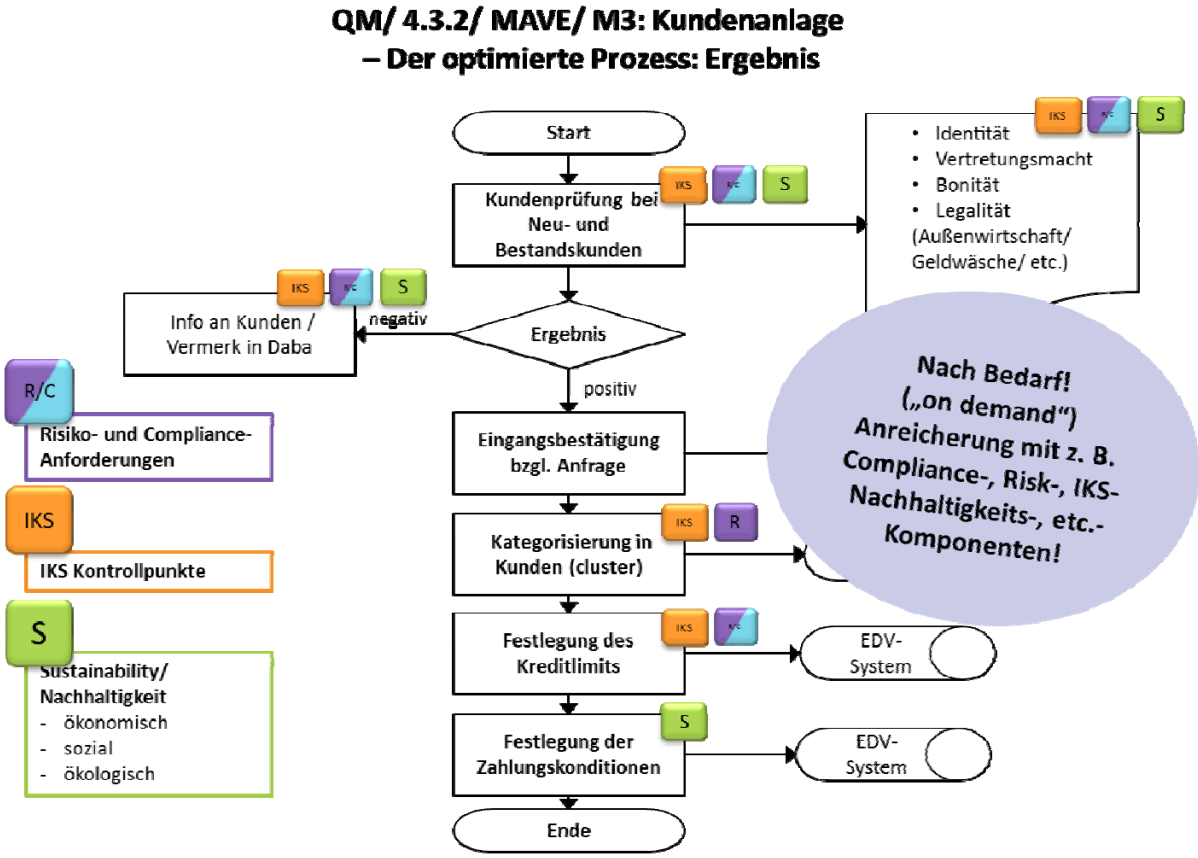
Ein Prozess *muss rechtssicher* sein!

QM/ 4.3.2/ MAVE/ M3: Kundenanlage
– Die Anreicherung mit Anforderungen aus Compliance



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 115 ff.

Die „Anreicherung“ desselben (!) Prozesses mit weiteren Komponenten aus Risk, IKS, etc.:



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 115 ff.

- Sind Ihre Prozesse dokumentiert? ❑ Ja ❑ Nein
- Optimiert? ❑ Ja ❑ Nein
- Mit Prozess-Zielen (KPI‘s) versehen? ❑ Ja ❑ Nein
- **Angereichert mit Risk, IKS, Compliance?** ❑ Ja ❑ Nein
- **Workflow-fähig?** ❑ Ja ❑ Nein

Der Sprung in die Digitalisierung: Eine große Chance!

Lösungen:

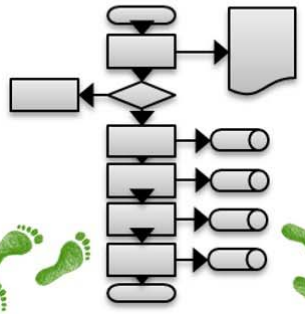
❑ Prozessabläufe / Prozessoptimierung

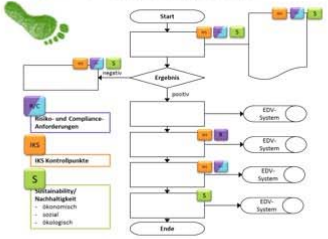
- Visualisiert (Visio / IGrafx / Viflow / …)
- Prozess-Sheet (Beschreibung der Prozessschritte / Mitgeltende Dokumente / etc.)
- Angereichert mit Komponenten aus Risk, Compliance, IKS, etc.
- Workflow-Management („Industrie 4.0“ /Digitalisierung)

Evolutionsstufe ?

Das war ein weiter Weg! Und was kommt jetzt?

Handschriftlich dokumentierte Prozessschritte





Anforderungen an zeitgemäße Workflow-Lösungen:

Ideal wäre es, wenn die Abteilungen im Unternehmen auch ohne teure IT-Spezialisten ihre Prozesse jederzeit selbst aktualisieren könnten.

Die Prozesse sollten nicht nur dokumentiert, sondern so ausgestaltet sein, dass - ähnlich wie bei einer Bestellung bei Amazon - die Mitarbeiter - geführt **durch einen Human-Workflow – *„das Richtige richtig“* machen müssten**.

E-Mails würden **nur an** die **tatsächlich zuständigen Adressaten** verteilt und alle **Informationen**, auch Compliance-Regelungen in Richtlinien, würden **bei den jeweiligen Prozessschritten bereitgestellt**.

Automatisch würde auch die Dokumentation und Auswertung der **Erfüllung von Compliance-Anforderungen** oder auch von **Prozessdurchlaufzeiten** erfolgen.

Mit Workflow-Management würde der **Mensch und Mitarbeiter durch den Prozess geführt** und damit zur **Rechts-, Zeit- und Systemtreue** angehalten.

Mit anderen Worten:

Der Mensch und Mitarbeiter, der gerade eben wegen menschlicher Schwächen auch fehleranfällig ist, würde bei standardisierten Abläufen Fehler i.d.R. nur noch machen können, wenn er *bewusst* die Prozessvorgaben technisch überwindet und auch Kontrollen in arglistiger Weise ausschaltet.

Die als Workflows abgebildeten **Prozessabläufe müssten mit allen** sonstigen Systemen und Programmen **der bereits vorhandenen IT-Landschaft** verbunden werden können, wie zum Beispiel SAP, Warenwirtschaftssystemen oder Dokumentenmanagement-Systemen.

Jeder Prozessbeteiligte wüsste, was er wann und wie und wo zu tun hat.

Auch die sogenannten **„Überwachungsfunktionen“[1] (lines of defense)** wüssten neben den Prozessbeteiligten stets, wo der Prozess gerade läuft oder eben auch sich verzögert.

So wäre eine **Information in Echtzeit** möglich und **erspart** zahlreiche Nachforschungen, Telefonate oder Meetings.

[1] Vgl. *Scherer*, „Die Welt(en) der Überwacher“, FIRM Jahrbuch 2017, S. 79 – 81.

Gerade die „**Compliance**“ **würde** durch eine stets aktuelle Einbindung von Komponenten zur Erfüllung der Anforderungen aus Gesetzen, Rechtsprechung, internen verbindlichen Regeln oder Richtlinien (wie zum Beispiel Zuwendungs- oder Datenschutzrichtlinien), sowie dem anerkannten Stand von Wissenschaft und Praxis und unter Umständen auch Industriestandards (wie ISO oder COSO etc.) **sichergestellt.**

Prozessoptimierungen und Anpassungen würden **nicht mehr nach Bauchgefühl**, sondern auf der Basis von echten und aktuellen Prozesskennzahlen höchst effizient und effektiv durchgeführt.

Über eine der Realität entsprechende **Prozesskostenrechnung** könnte sowohl der Input des jeweiligen Prozessschrittes aber auch der Output in Zahlungsströmen dargestellt werden. Das wäre die Basis für eine **Wertbeitragsberechnung** nach gelebten Prozessen.[2]

Das alles ist machbare Realität und wird in Kürze „Anerkannter Stand von Wissenschaft und Praxis“ bei Good-practice-Unternehmen!

[2] Vgl. *Ludacka*, Workflow-Management in *Scherer/Fruth*, Integriertes Compliance-Managementsystem mit GRC, 2. Auflage, 2017, Punkt 1.2.5.

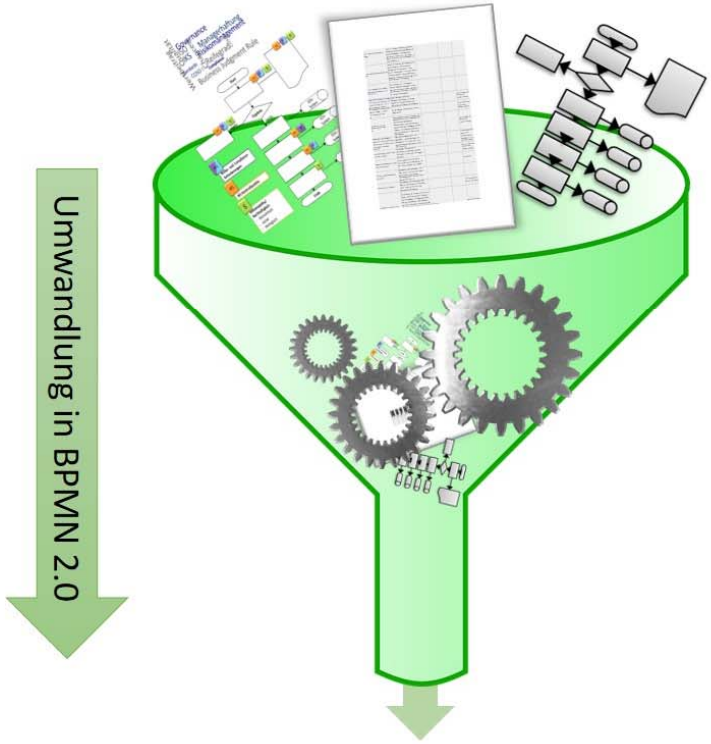
Unternehmen bzw. ihre Organe (Aufsichtsrat, Vorstand / Geschäftsführer, Gesellschafter) **sind**, falls sie selbst nicht pflichtwidrig und haftungsauslösend agieren möchten (§§ 93, 107 AktG, 43 GmbHG, 347 HGB), **gehalten, sich an diesen „Anerkannten Stand von Wissenschaft und Praxis“ zu halten.**[3]

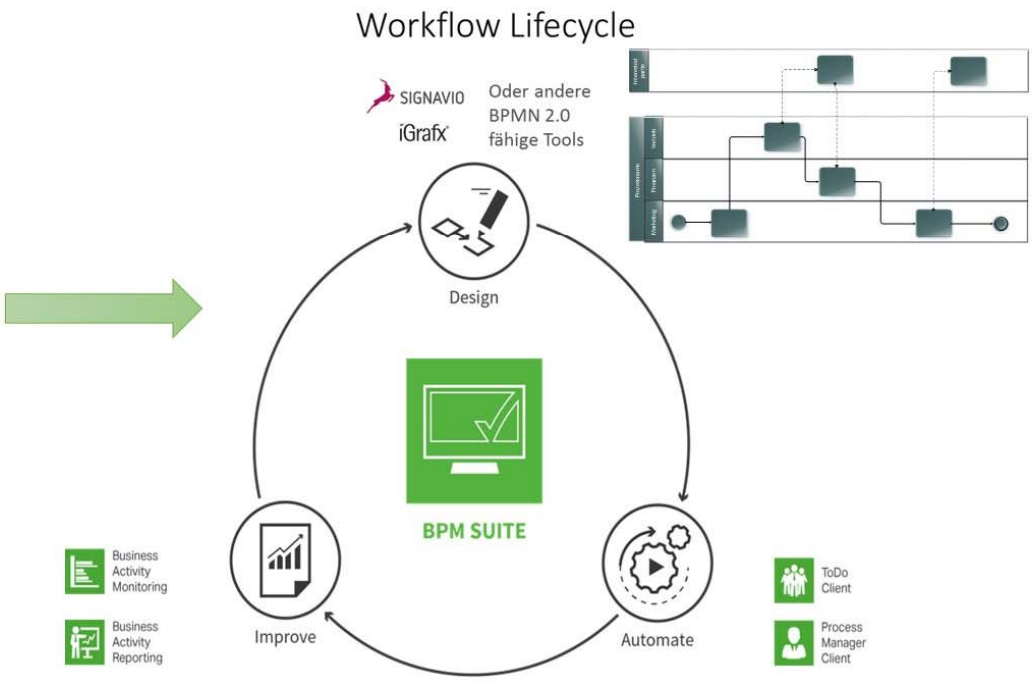
Deshalb sollten sie ihre Prozesse dokumentieren, mit Komponenten aus Governance, Risk und Compliance angemessen anreichern und digitalisieren.

[3] Vgl. *Scherer*, *Fruth,* Geschäftsführer-Compliance, 2009; *Scherer/Fruth,* Governance-Management, Band 1, 2014 und Band 2, 2015; *Scherer/Fruth,* Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis“ auf Organhaftung und Corporate Governance, Corporate Compliance Zeitschrift, 2015, S. 9 – 17.
Vgl. *Raum* (Vorsitzender Richter des 1. Strafsenates des Bundesgerichtshofs) in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017, S. 48 ff.:
„(…) In diesem Zusammenhang ist zu erörtern, **welche Bedeutung den** in jüngerer Zeit **erarbeiteten IDW (PS 980) und ISO (19600) Richtlinien / Normen bzw. den (…) angebotenen Zertifizierungen zukommen kann.** (…) Derartige Leitlinien **können** deshalb faktisch strafbarkeitskonstituierend sein. (…)“

Evolutionsstufe 6

Den Prozess zum „Leben“ erwecken!

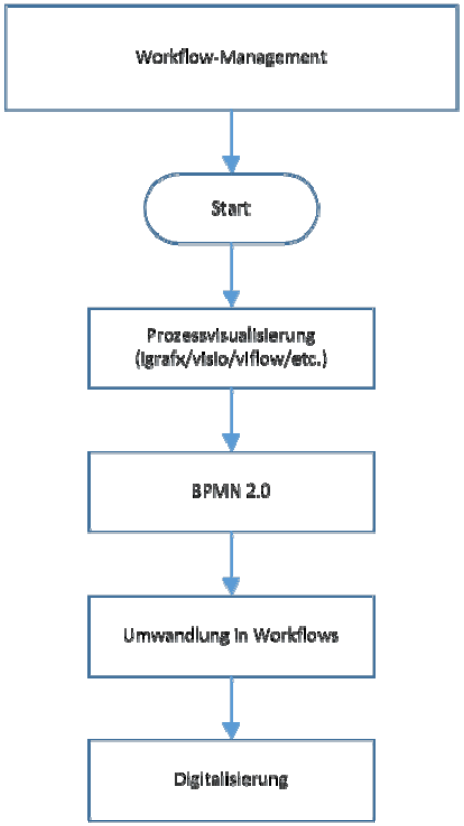




Workflowmanagement

Workflow-Management: Die Prozesse leben!

Digitalisierung und „Industrie 4.0“ in allen Geschäftsprozessen durch Workflow-Management!

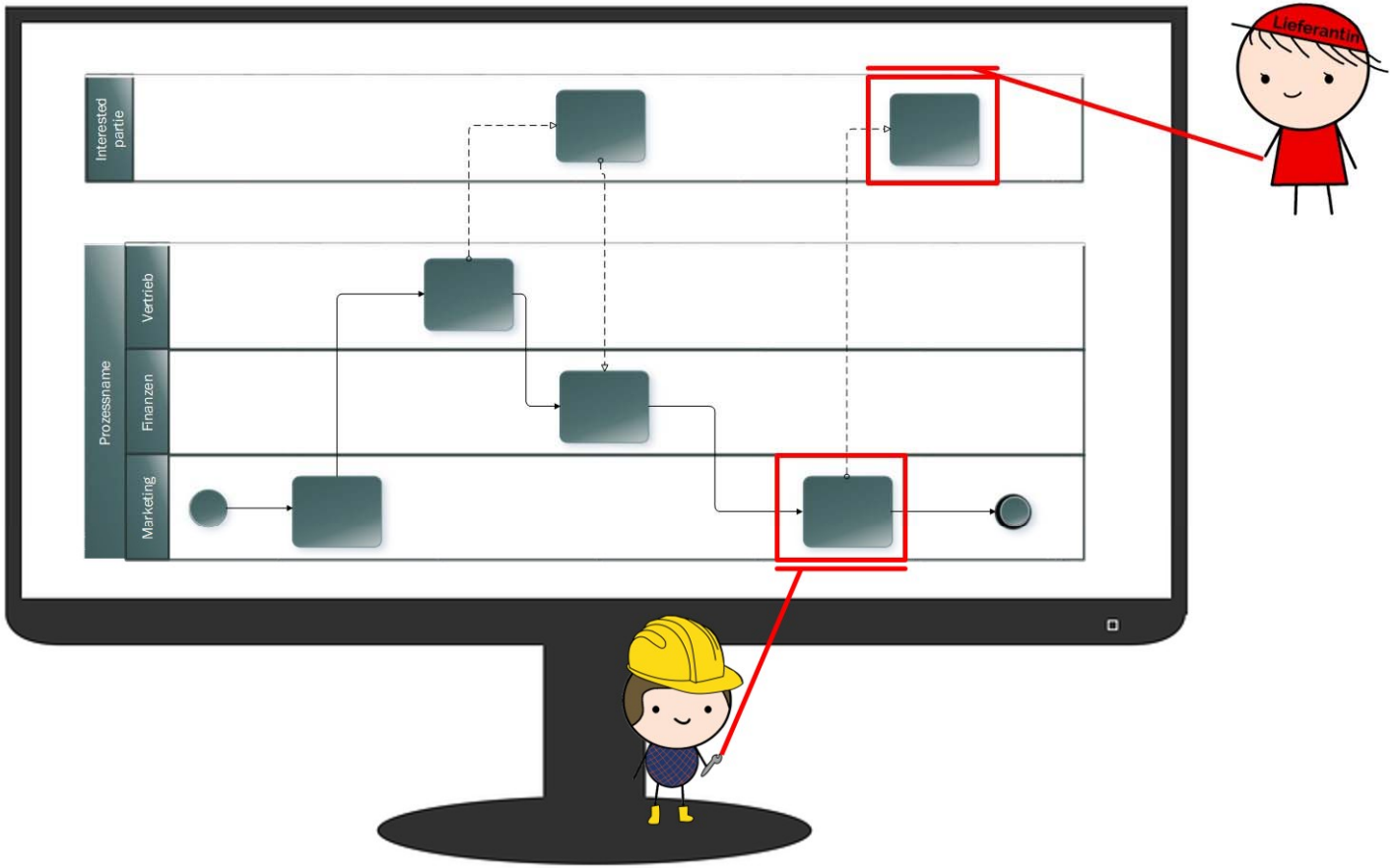


Evolutionsstufe 6

Jeder arbeitet innerhalb des Systems an seinem Prozess!

Jeder Prozesseigner bekommt einen Zugang mit den für ihn relevanten Berechtigungen und kann in Echtzeit an seinem Prozess arbeiten!

Dabei kann die Geschäftsführung / der Prozessmanager stets abrufen und sehen, Wer? Was? Wie? Wie lange? der jeweilige Mitarbeiter an seinem Prozess arbeitet und zugleich den gesamten Prozess überwachen!



Lösungen:

❑ Human-Workflow-Management

Über „Human-Workflow-Management“ werden bisher statische und „leblose“ Prozessvisualisierungen **„mit Leben erweckt“.**

Die Prozessablauf-Beteiligten werden innerhalb der individuell und vom Unternehmen selbst anpassbaren Leitplanken geführt, das Richtige richtig und fristgerecht zu erledigen.

Gleichzeitig erhalten Sie **Transparenz** über den jeweils aktuellen Stand der Aktivitäten.

Dadurch wird **sichergestellt, dass die Prozesse „gelebt“ (!) werden, bzw. – in der Fachsprache – „wirksam“ sind!**
Eine wesentliche Voraussetzung für effektive, effiziente und rechtssichere Organisation in einem einzigen, „Integrierten GRC-Kombi-Managementsystem on demand“!

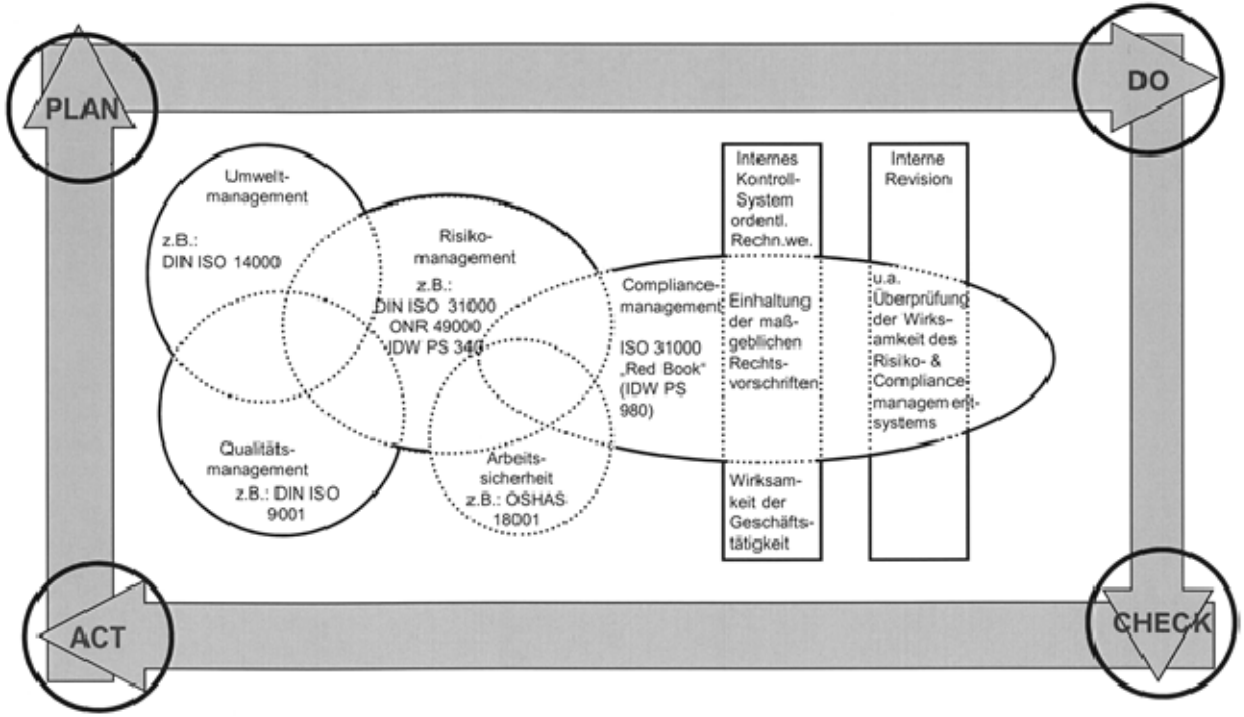
Evolutionsstufe 7

Ein digitalisiertes (Human Workflow) „Integriertes GRC-Kombi-Managementsystem on demand“

Was ist ein „Managementsystem“?

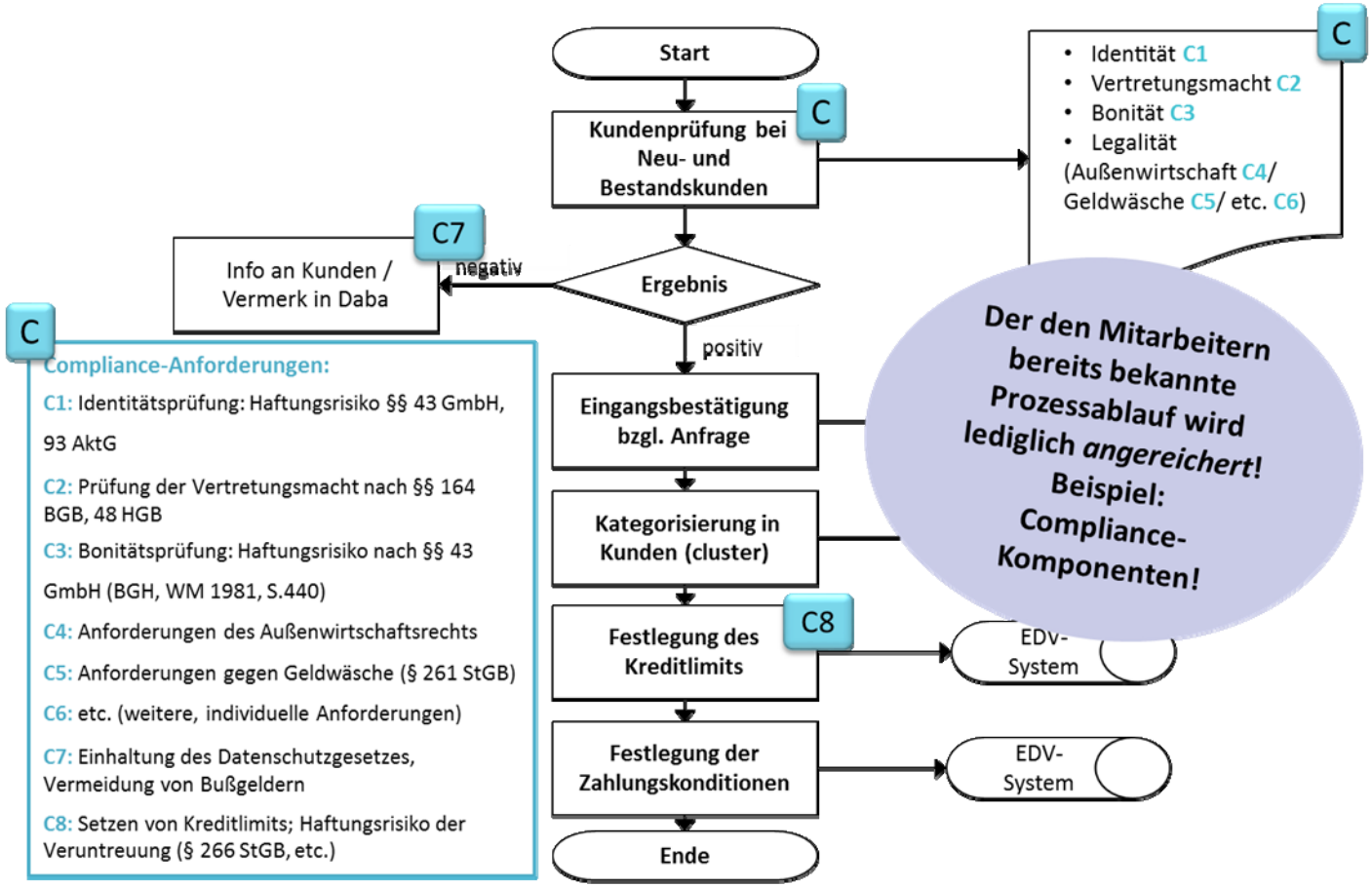
Jedes Unternehmen hat bereits ein Managementsystem:

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“.



Ein Managementsystem besteht aus Aufbau- und Ablauforganisation (Prozesse) und deren Komponenten

QM/ 4.3.2/ MAVE/ M3: Kundenanlage – Die Anreicherung mit Anforderungen aus Compliance



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 115 ff.

Kennen Sie die Referenzgrößen, an denen Ihre unternehmerischen Aktivitäten bzw. ihres Managementsystems gemessen werden?

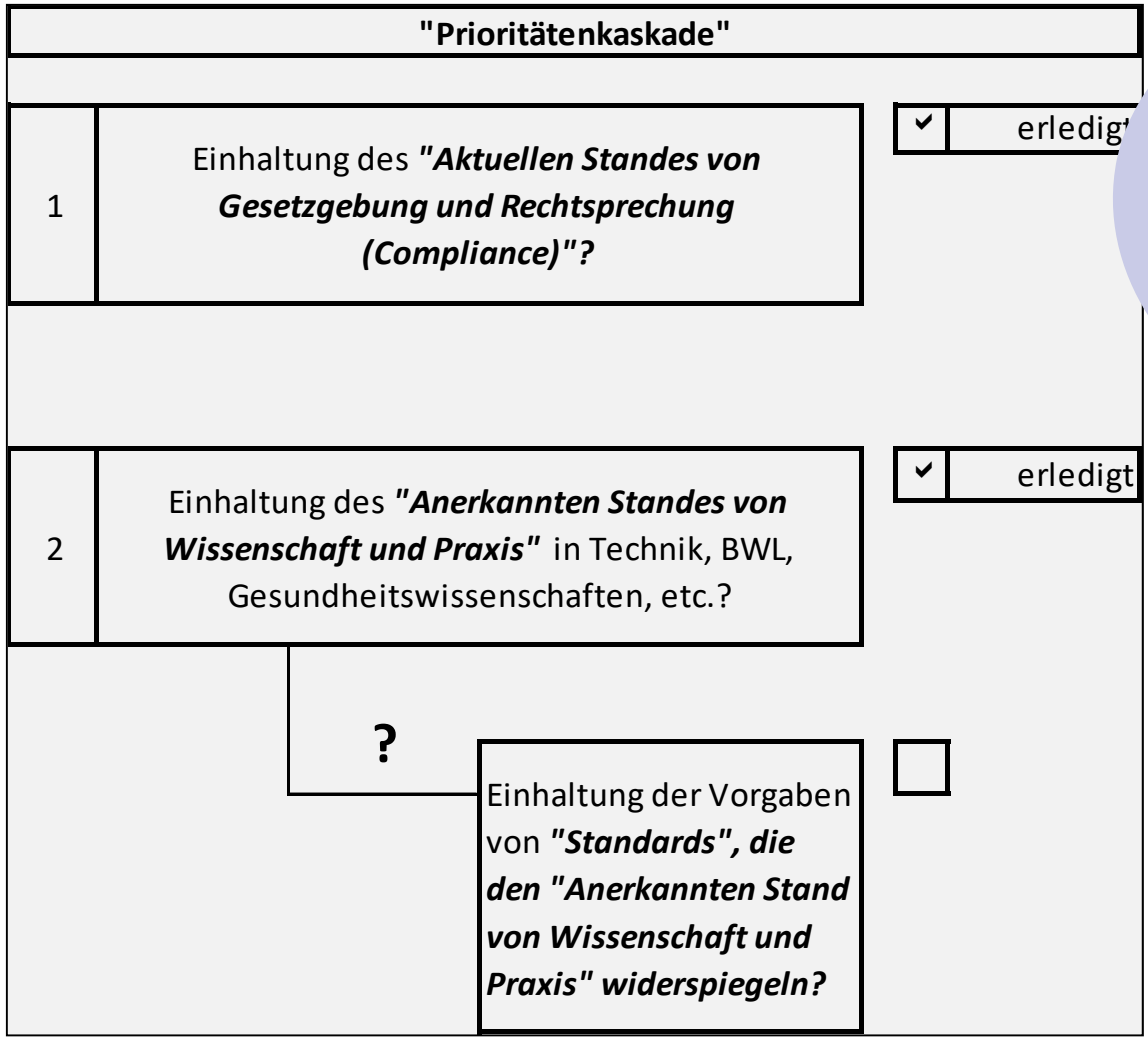


Abbildung : Prioritätenkaskade.

Quelle: *Scherer / Fruth* (Hrsg.), Governance-Management Band I, 2016, S. 104

Diese „Messgrößen“ sind für Ihre Leistungen / Prozesse / Systeme / etc. relevant!

Anforderungen an Produkte, Leistungen, Prozesse, Systeme…

Ein Produkt, eine (Dienst-)Leistung, ein Prozessablauf, eine Unternehmensabteilung, ein Managementsystem, das Entscheiden und Handeln von Management und Mitarbeitern, etc. ***muss*** *die in folgendem Schaubild dargestellten Anforderungen erfüllen, um einen hohen Reifegrad und zugleich einen hohen Pflichterfüllungsgrad aufzuweisen:*

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“ (Standards) entsprechend*	*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 (§§)*

Abbildung 67: Anforderungen an Produkte, Leistungen, Prozesse, Systeme, etc.

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 Festlegung und Sicherstellung der erforderlichen **Ressourcen** geht es an die **Implementierung und Umsetzung** im beruflichen Alltag **(Wirksamkeit, „gelebt werden“).**

Die Anforderungen der vielen **Standards** (QM, Umwelt, Arbeitssicherheit, Risiko- und Compliance, etc.) müssen lediglich als Komponenten **in** die Bestandteile der rechtssicheren Organisation (**Aufbau- und Ablauforganisation) eingefügt** werden.

Die **IT** spielt hier zunächst 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.

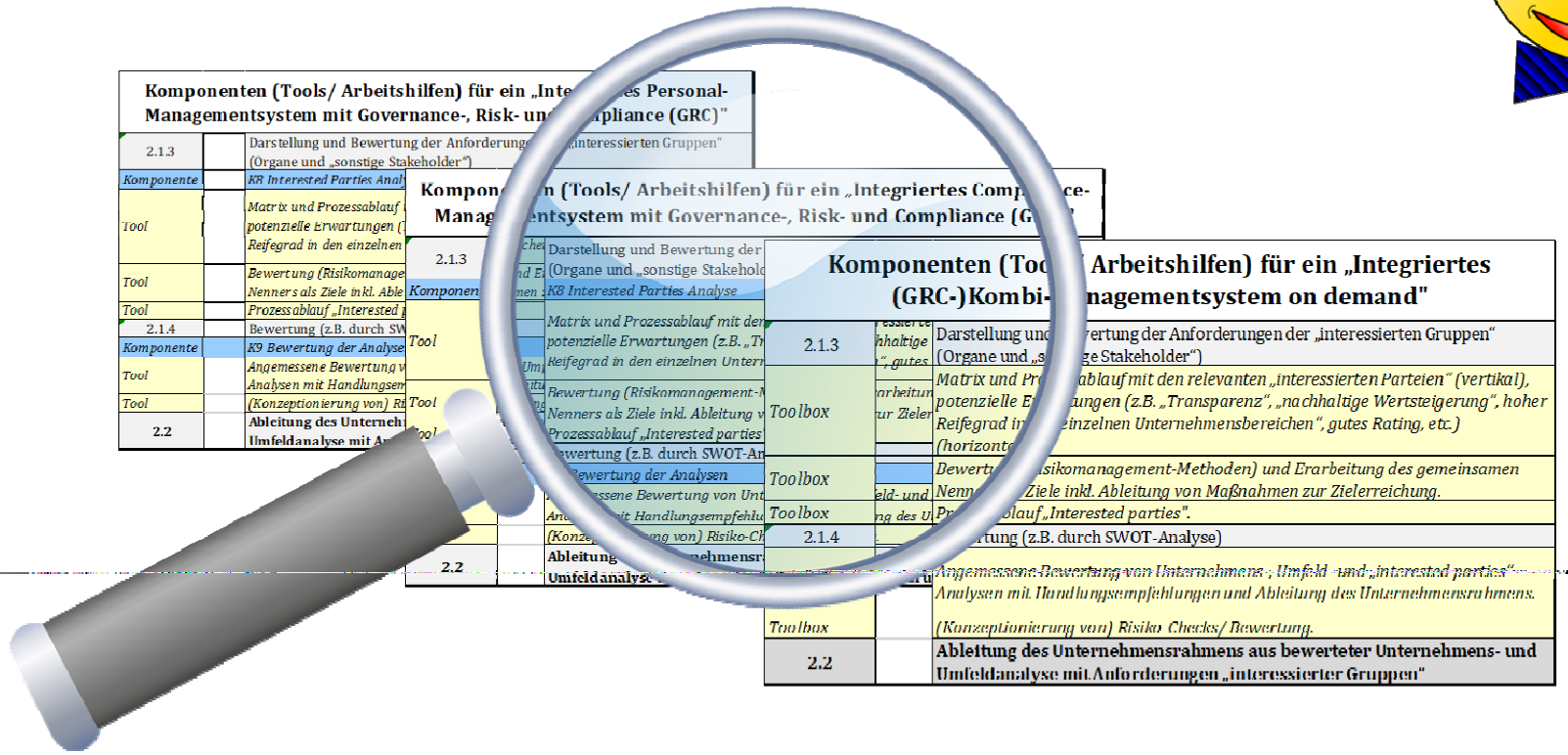
Für große Unternehmen eignet sich beispielsweise SAP, für kleine nicht unbedingt:

Wichtige Voraussetzung für Mehrwert ist die konsequente „Fütterung“ und **Pflege des Systems und die einfache Handhabbarkeit für alle Mitarbeiter.**

Und: **Gelebte, angemessene Prozesse,** idealerweise digitalisiert / als „workflows“ verfügbar.

Evolutionsstufe 7

Es scheint, als wäre es - zumindest zu 70%
- das „Gleiche“!? …



Komponenten (Tools/ Arbeitshilfen) für ein „Integriertes (GRC-)Kombi-…nagementsystem on demand"		
2.1.3		Darstellung und …rtung der Anforderungen der „interessierten Gruppen“ (Organe und „s… ge Stakeholder“)
Toolbox		*Matrix und Pr… ablauf mit den relevanten „interessierten Parteien“ (vertikal), potenzielle E… ungen (z.B. „Transparenz“, „nachhaltige Wertsteigerung“, hoher Reifegrad in… einzelnen Unternehmensbereichen“, gutes Rating, etc.) (horizont…*
Toolbox		*Bewertu… sikomanagement-Methoden) und Erarbeitung des gemeinsamen Nenn… Ziele inkl. Ableitung von Maßnahmen zur Zielerreichung.*
Toolbox		*Pr… blauf „Interested parties“.*
2.1.4		…tung (z.B. durch SWOT-Analyse)
Toolbox		*Angemessene Bewertung von Unternehmens-, Umfeld- und „interested parties“-Analysen mit Handlungsempfehlungen und Ableitung des Unternehmensrahmens.* *(Konzeptionierung von) Risiko-Checks/ Bewertung.*
2.2		**Ableitung des Unternehmensrahmens aus bewerteter Unternehmens- und Umfeldanalyse mit Anforderungen „interessierter Gruppen“**

Das „Geheimnis“ dieser Vorgehensweise?

These: Die meisten Standards / Systeme verlangen das Gleiche (redundante oder analoge Komponenten)

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Interessant scheint die Erkenntnis, dass die diversen **Managementsysteme** exemplarisch **jeweils in ca. 30 Komponenten** (z. B. Umfeldanalyse, Dokumentation, Ressourcen, Prozesse, etc.) aufgegliedert werden können.

Komponenten (Tools/ Arbeitshilfen) für ein „Integriertes (GRC-)Kombi-Managementsystem on demand"		
Block 2		**Analyse von Unternehmen, Umfeld, etc. und Ableitung des Unternehmensrahmens**
2.1		**Darstellung und Bewertung (SWOT) des Unternehmens, des relevanten Umfeldes und Anforderungen der "interessierten Gruppen"**
2.1.1	Analysen	Unternehmensanalyse
Komponente		*K6 Unternehmensanalyse*
Tool		*Checkliste Unternehmensanalyse mit (Basis-) Risiko-Checks mit Bewertung.*
Tool		*Muster Unternehmensanalyse.*
Tool		*Auszug aus Lagebericht, betreffend Unternehmensbeschreibung (Geschäftsmodell ...).*
Tool		*Business Plan (light).*
2.1.2		Umfeldanalyse
Komponente		*K7 Umfeldanalyse*
Tool		*Checkliste Umfeldanalyse.*
Tool		*Muster Umfeldanalyse.*
Tool		*Auszug aus Lagebericht, betreffend Umfeld.*
2.1.3		Darstellung und Bewertung der Anforderungen der „interessierten Gruppen" (Organe und „sonstige Stakeholder")
Komponente		*K8 Interested Parties Analyse*
Tool		*Matrix und Prozessablauf mit den relevanten „interessierten Parteien" (vertikal), potenzielle Erwartungen (z.B. „Transparenz", „nachhaltige Wertsteigerung", hoher Reifegrad in den einzelnen Unternehmensbereichen", gutes Rating, etc.) (horizontal).*
Tool		*Bewertung (Risikomanagement-Methoden) und Erarbeitung des gemeinsamen Nenners als Ziele inkl. Ableitung von Maßnahmen zur Zielerreichung.*
Tool		*Prozessablauf „Interested parties".*

Das „Geheimnis“ und der Beweis!

Einzelne Komponenten / Bestandteile sind vielfach verwendbar!

z. B. | Interested parties-Analyse |

Wird nur ein einziges Mal ausgeführt.

Aufgrund der **Redundanzen in anderen Standards** verwendbar für Qualitäts-Management / Risiko-Management / Compliance-Management / Business Continuity-Management / etc. / etc.

LESEPROBE AUS - PUNKT 2.1.3 DES CMS UNIVERSAL STANDARDS

2.1.3 Darstellung und Bewertung der Anforderungen der „interessierten Gruppen“ (Organe und sonstige „Stakeholder“)

[1] „Das Unternehmen (die Organisation) muss die - auch für das Compliance-Managementsystem – relevanten interessierten Gruppen und deren Anforderungen bestimmen.

[2] Interessierte Gruppen sind z. B.
Organe, wie Geschäftsführung, Gesellschafterversammlung, Aufsichtsorgan oder Sonstige, wie z. B. Arbeitnehmer, Betriebsrat, Kunden, Lieferanten, Behörden (z. B. Gewerbeaufsichtsamt, Zoll, Finanzamt,...), Medien.

[3] Mögliche Anforderungen mehrerer unterschiedlicher Gruppen sind z. B. funktionierendes Compliance-Management (Pflichtenbefolgung) oder Transparenz.

[4] Die Anforderungen sind zu bewerten und sich daraus ergebende erforderliche Maßnahmen (für das Compliance-Managementsystem) sind umzusetzen.

BEWERTUNG: BEI PUNKT 2.1.3 HANDELT ES SICH UM EINE **PFLICHTANFORDERUNG**

DIE GEGENÜBERSTELLUNG (SYNOPSE)

ISO 19600: 2014 (Compliance-Management)

„4.2 Understanding the needs and expectations of interested parties

ISO 37001: 2016 (Antikorruption)

„4.2 Understanding the needs and expectations of interested parties

IDW PS 980: 2011 (Compliance-Managementsystem)

„5.4.1. Prüfungshandlungen zur Risikobeurteilung
(40) 5.4.1.1. Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens

„(A29) Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens [Tz. 40]

ONR 192050: 2013 (Compliance-Management-Systeme)

- Hier ist keine entsprechende Anforderung ersichtlich -

COSO I: 2013 (Internal Control)

Prinzip	***Fokuspunkte***
Prinzip 9 *Die Organisation identifiziert und bewertet Veränderungen, die das IKS wesentlich beeinträchtigen können.*	*35 Beurteilt Veränderungen in externer Umwelt.*

PAS 99: 2012 (Integriertes Management System)

(Public Available Standard / British Standards Institution)

„4.2 Understanding the needs and expectations of interested parties

ISO 9001: 2015 (Qualitätsmanagementsystem)

„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

3.6.7. ISO 9004: 2009 (Leiten und Lenken für den nachhaltigen Erfolg einer Organisation)
„Interessierte Parteien, Erfordernisse und Erwartungen

Deutscher Rechnungslegungs Standard Nr. 20 (DRS 20) : 2012
((Konzern-) Lageberichterstattung gem. §§ 289, 315, 342 HGB)

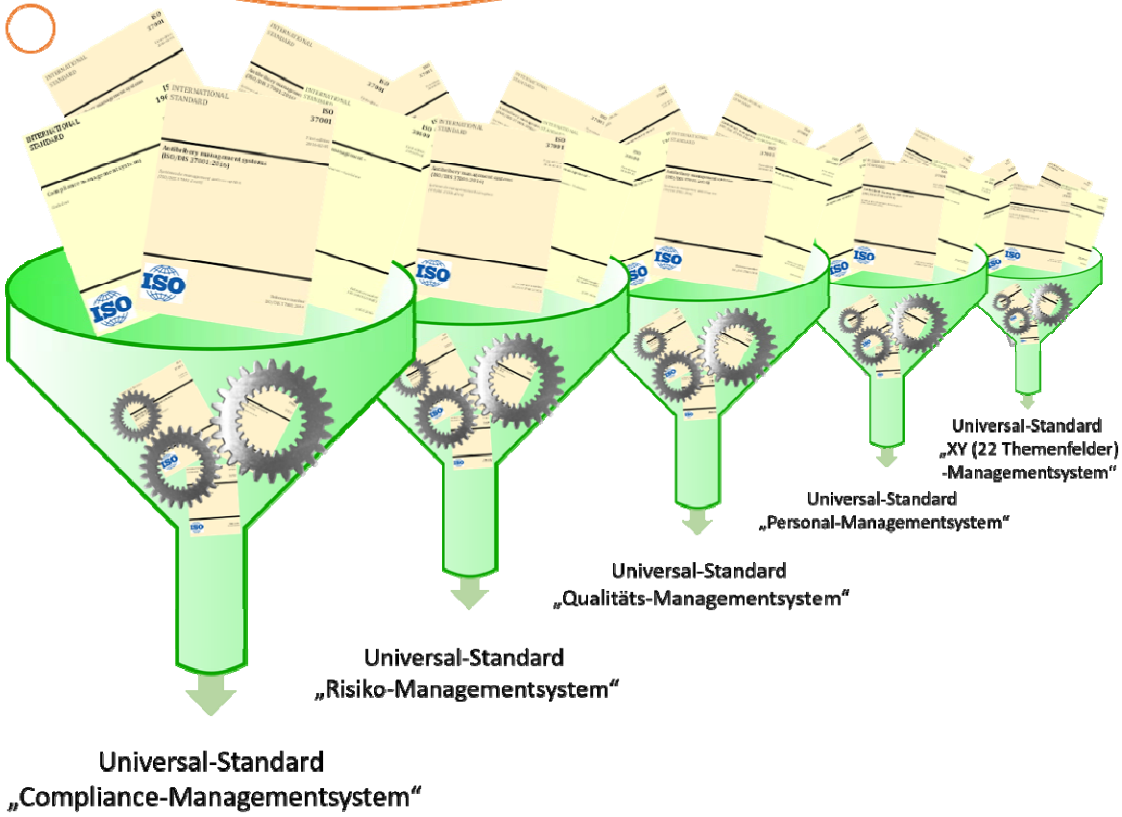
„3.“ / *„37.“* / *„59.“*

ISO 37001: 2016 (Anti-Korruptionsmanagementsystem)

„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Evolutionsstufe 7

**… also warum den Aufwand 5 mal betreiben?
Lasst uns doch alles in einen Topf werfen, ist
doch eh immer das „Gleiche“, zumindest zu 70%!**



Sofern ein Unternehmen nun schon Qualitäts- und Umwelt- oder Arbeitssicherheitsmanagement implementiert hat, sind zugleich meist auch **bereits bis zu zwei Drittel der Elemente** eines Risiko- oder Compliance-Managementsystems vorhanden.

Der zusätzliche Aufwand bei bekannter Systematik hält sich somit in Grenzen.

Wichtig ist auch der **Hinweis**, dass bei Implementierung von Risiko- und Compliancemanagement **nicht ein zusätzliches, neues Managementsystem** aufgebaut, **sondern das vorhandene nur „angereichert**“ wird.

Ein Standard statt unzähliger „Inseln“ – integriert in Human Workflowmanagement

Alle (!) (Manager, Mitarbeiter und „Überwacher“) wollen das Gleiche:

Deshalb haben wir den Universal-Standard für ein „Integriertes GRC-Managementsystem“ entwickelt!

- Statt vieler Inselsysteme und noch mehr Standards und Zertifizierungen eine *einzige* effektive und effiziente Lösung!

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

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

Welche „Logik“ steckt dahinter?

Eine ganz einfache.

Deshalb für Management und Mitarbeiter einleuchtend, überzeugend und umsetzbar!

Vergleicht man die diversen, vielzähligen Standards (ISO/IDW/COSO(etc.), so lässt sich ein **ähnlicher Aufbau mit sehr ähnlichen inhaltlichen Modulen** erkennen.

Das Verständnis der in Standards wiedergegebenen Anforderungen und **das Erkennen einer Systematik is**t für die Adressaten **erforderlich, um die Vorgaben in der täglichen Arbeit leben zu können („Wirksamkeit“) und gegebenenfalls Audit-Fragen unterschiedlichster interessierter Gruppen** (z.B. Kunden / Behörden / Versicherer/ Kreditinstitute [Rating]/Zertifizierer /etc.) **beantworten zu können.**

Die **vielen – sehr ähnlichen – Standards** diverser Anbieter (ISO / COSO / IDW / DIIR / etc.) zu einem bestimmten Themenbereich (z.B. Compliance/Risk/Revision/etc.) **werden nach dem neuen Ansatz des Instituts zunächst auf einem einzigen (Themen-) Universal-Standard „verschmolzen".**

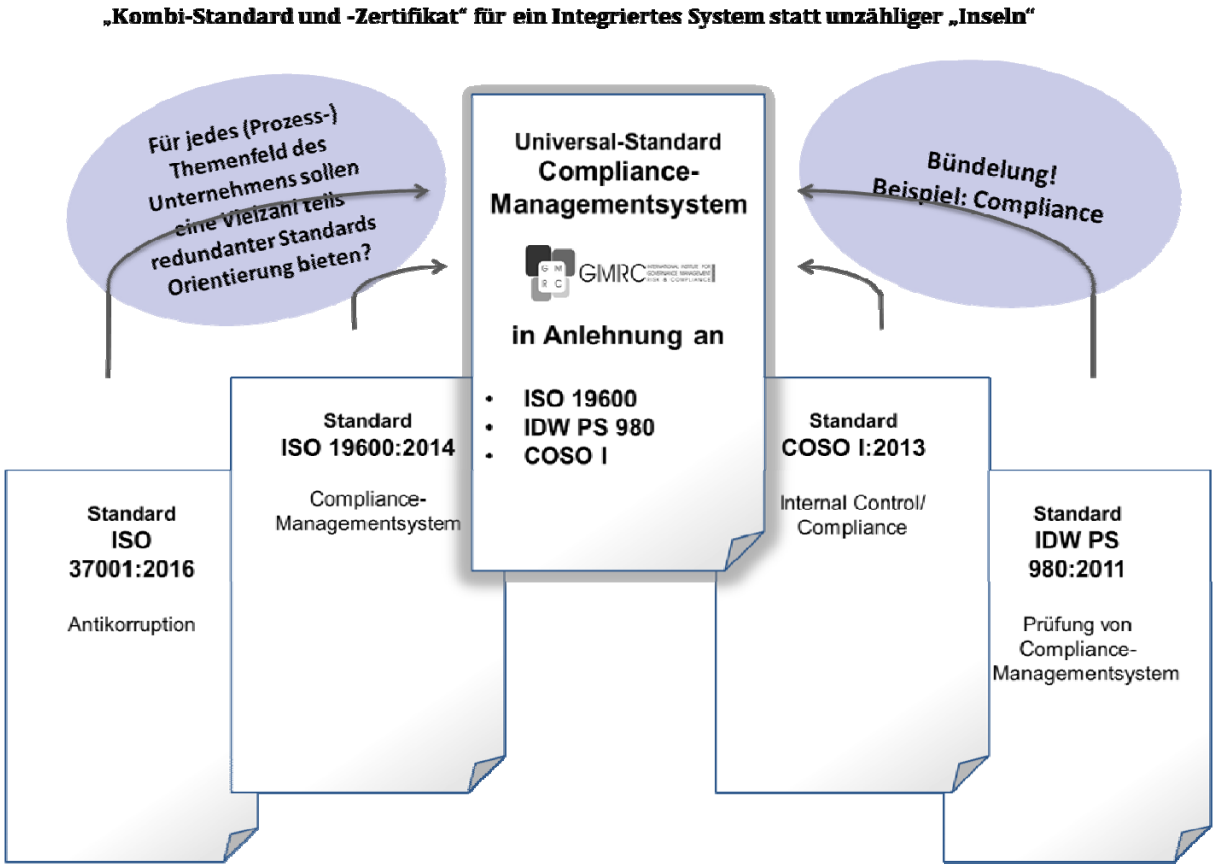
Dieser „Universal-Standard" bringt also inhaltlich eigentlich nichts Neues, sondern strukturiert und versucht, die jeweils beste Formulierung abzubilden.

Über Synopsen verweist er auf die jeweiligen Fundstellen in den **kommerziellen Standards.**

Vgl. www.gmrc.de / Universal-Standard

Beispiel: *Compliance*-Management:

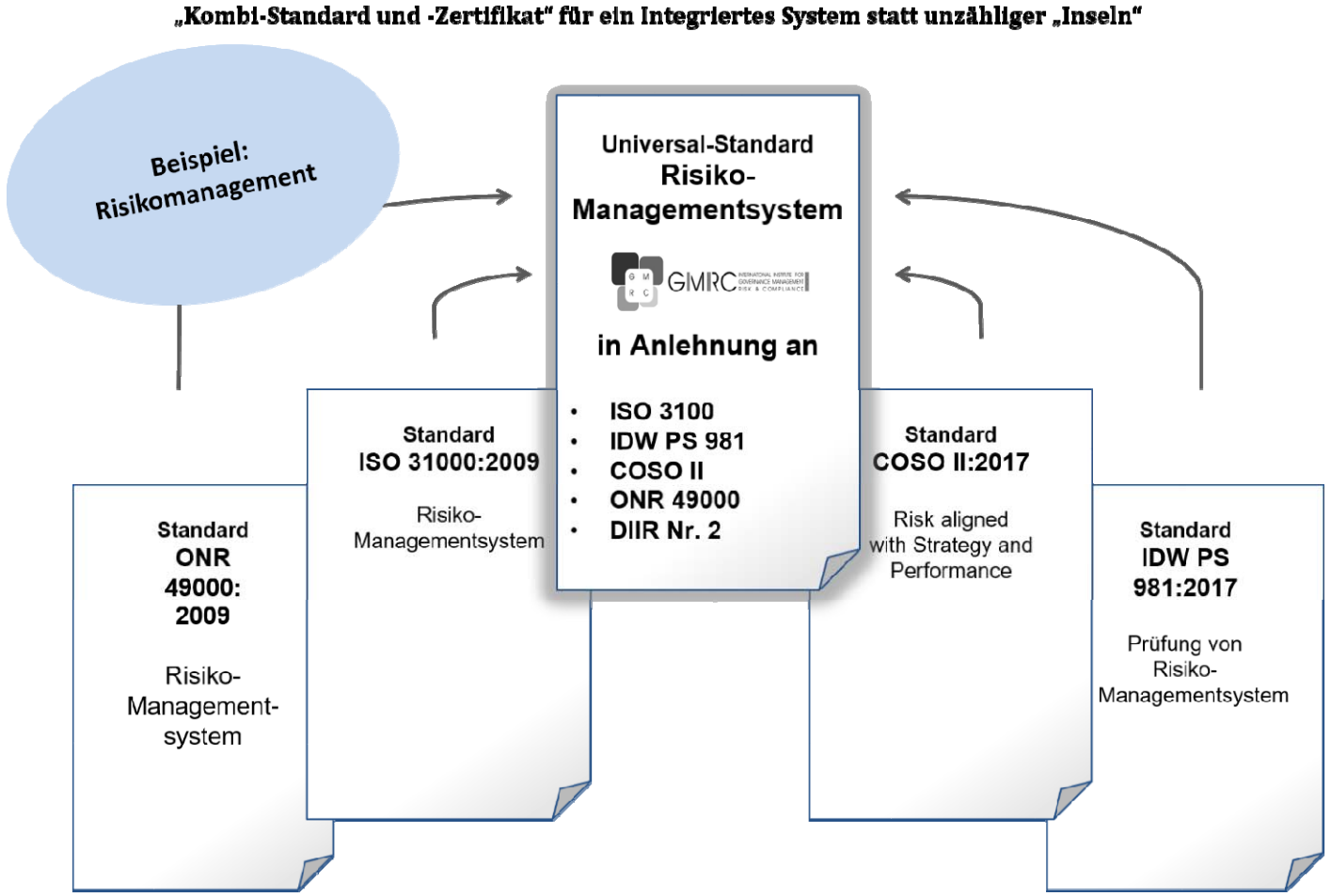
Die „Verschmelzung“ vieler Standards auf einen einzigen Universal-Standard!



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Beispiel: *Risiko*-Management:

Die „Verschmelzung“ vieler Standards auf einen einzigen!

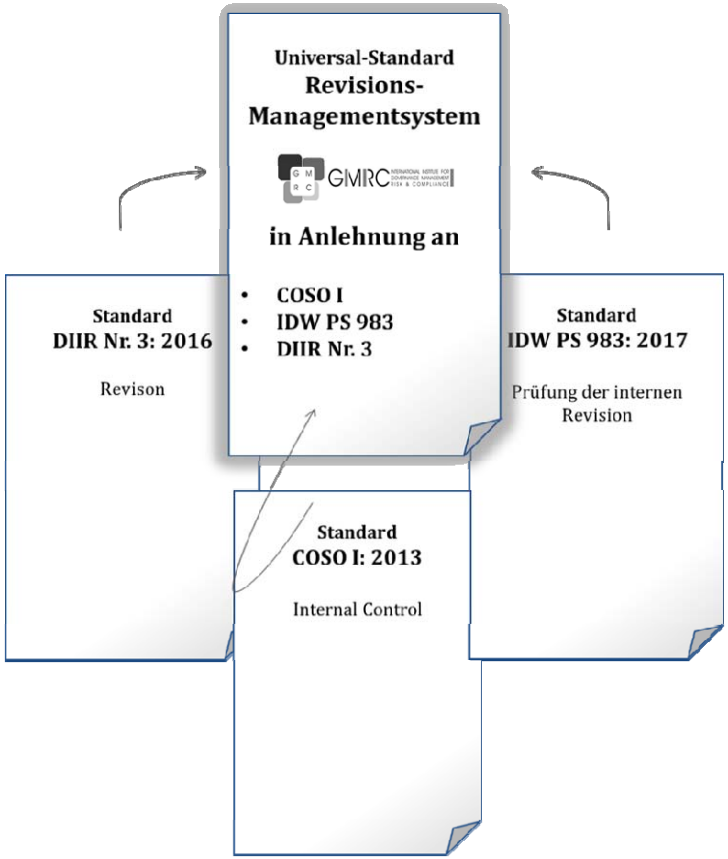


Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Beispiel: *Revisions*-Management:

Die „Verschmelzung“ vieler Standards auf einen einzigen!

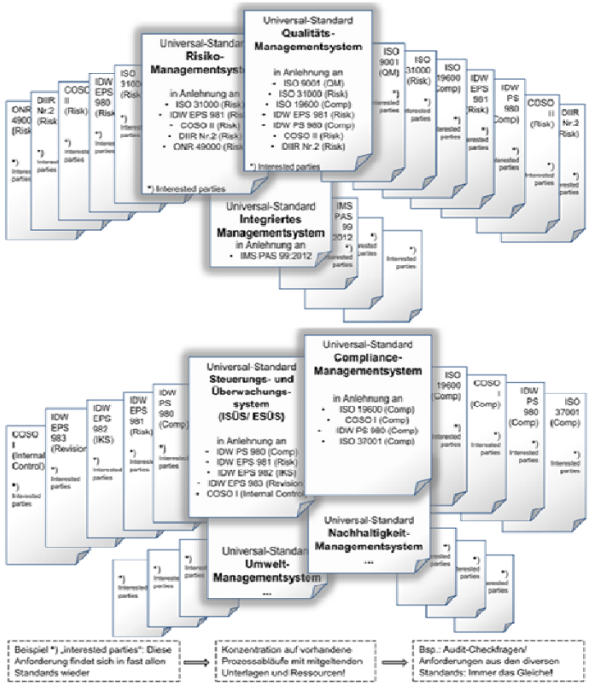
„Kombi-Standard und -Zertifikat“ für ein Integriertes System statt unzähliger „Inseln“



Und so geht es weiter:

Bei allen (Prozess-) Themenfeldern, die für Sie relevant sind: Auflösung des „Normen-Dickichts“ durch Konzentration / Verschmelzung!

„Kombi-Standard und -Zertifikat“ für ein Integriertes System statt unzähliger „Inseln“

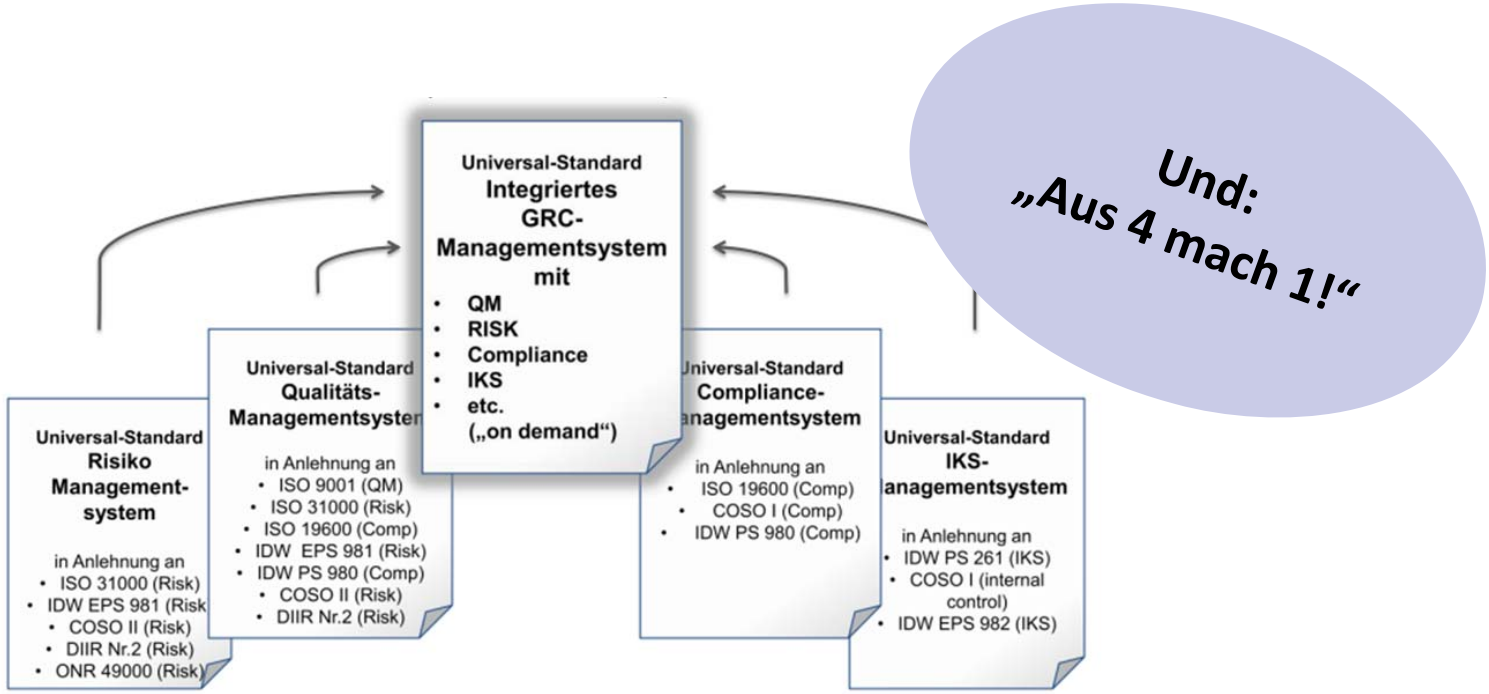


Auflösung der Redundanzen in den für Ihr Unternehmen relevanten Themenbereichen: Z. B. „Aus 20 mach 4!“

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Und zu guter Letzt:

Verschmelzung der für Sie relevanten, übrig gebliebenen Themen-Standards zu einem einzigen „GRC-Universal-Standard on demand“



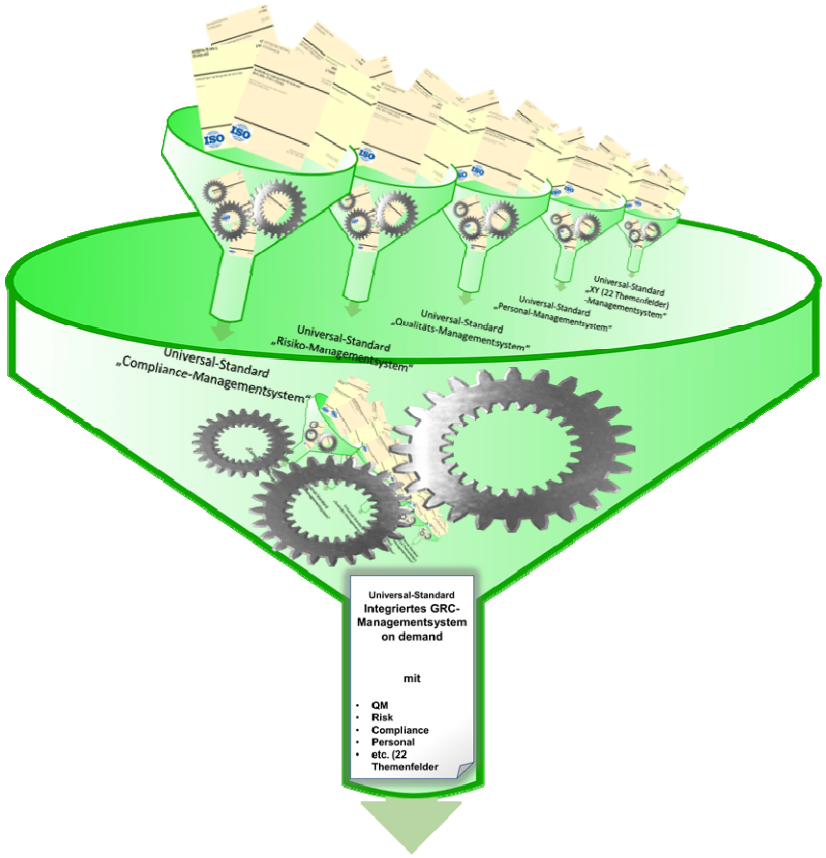
Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

Evolutionsstufe 7

Compliance, Risiko, Personal, QM, …!? Immer noch zu 70% das „Gleiche“?

Also schaffe Dir doch einfach Dein „Integriertes (GRC-)Kombi-Managementsystem on demand“!

Vom „Inselsystem“ zum „Integrierten System“



Universal-Standard
„Integriertes Kombi-Managementsystem on demand“

Evolutionsstufe 7

Optimal wäre, wenn die Digitalisierung hier uns unterstützen könnte!

Workflow-Management?

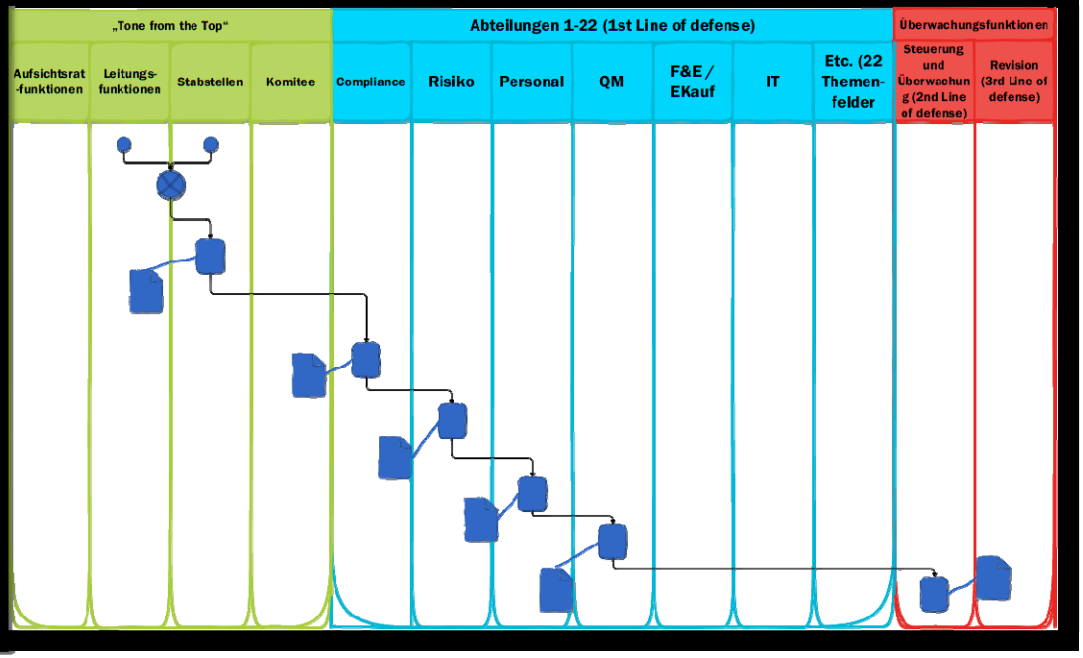
Automatisierung?

Prozessmanagement?

Digitale Transformation?

Evolutionsstufe 7

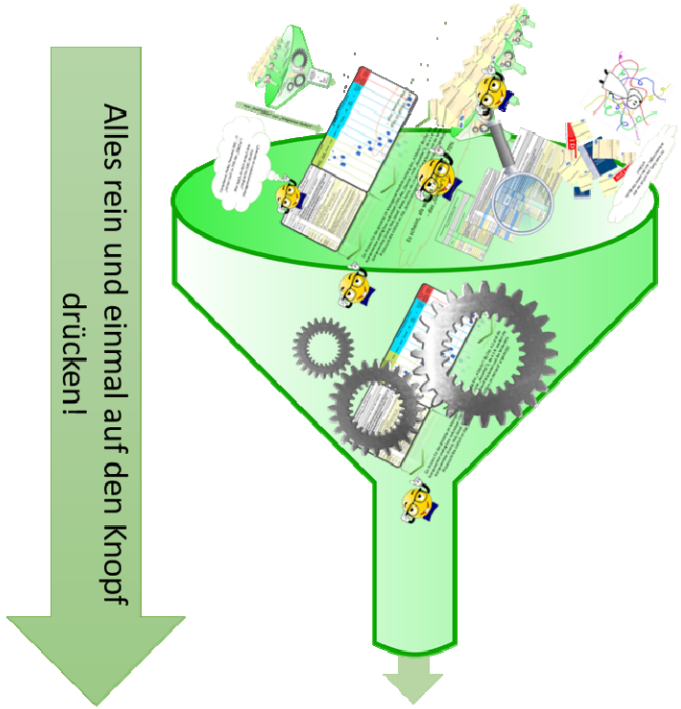
Komponenten (Tools/ Arbeitshilfen) für ein „Integriertes (GRC-)Kombi-Managementsystem on demand"		
Block 2		**Analyse von Unternehmen, Umfeld, etc. und Ableitung des Unternehmensrahmens**
2.1		**Darstellung und Bewertung (SWOT) des Unternehmens, des relevanten Umfeldes und Anforderungen der "interessierten Gruppen"**
2.1.1	Analysen	Unternehmensanalyse
Komponente		*K6 Unternehmensanalyse*
Tool		*Checkliste Unternehmensanalyse mit (Basis-) Risiko-Checks mit Bewertung.*
Tool		*Muster Unternehmensanalyse.*
Tool		*Auszug aus Lagebericht, betreffend Unternehmensbeschreibung (Geschäftsmodell ...).*
Tool		*Business Plan (light).*
2.1.2		Umfeldanalyse
Komponente		*K7 Umfeldanalyse*
Tool		*Checkliste Umfeldanalyse.*
Tool		*Muster Umfeldanalyse.*
Tool		*Auszug aus Lagebericht, betreffend Umfeld.*
2.1.3		Darstellung und Bewertung der Anforderungen der „interessierten Gruppen" (Organe und „sonstige Stakeholder")
Komponente		*K8 Interested Parties Analyse*
Tool		*Matrix und Prozessablauf mit den relevanten „interessierten Parteien" (vertikal), potenzielle Erwartungen (z.B. „Transparenz", „nachhaltige Wertsteigerung", hoher Reifegrad in den einzelnen Unternehmensbereichen", gutes Rating, etc.) (horizontal).*
Tool		*Bewertung (Risikomanagement-Methoden) und Erarbeitung des gemeinsamen Nenners als Ziele inkl. Ableitung von Maßnahmen zur Zielerreichung.*
Tool		*Prozessablauf „Interested parties".*

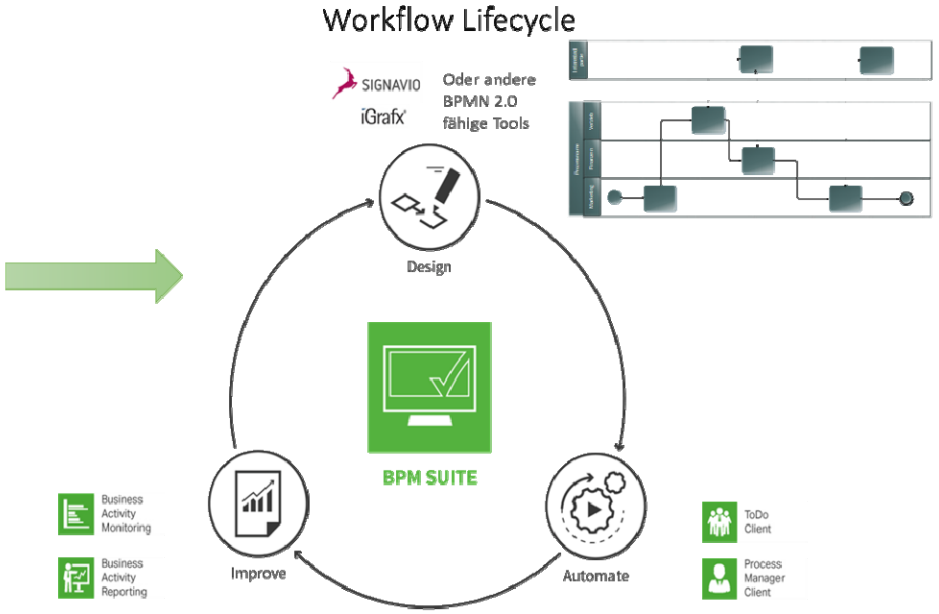


Ein einziger Prozess für das gesamte XY-Managementsystem entlang der „4 Blöcke"!:
Bis Pkt. 4.3 sind die Komponenten analog bzw. redundant (70% das „Gleiche", nicht „dasselbe"!).
Ab 4.3 ff. werden die Komponenten (Comp, Risk, Ekauf, MaVe, Perso, etc.) individuell und die jeweiligen Fachprozesse einfach an das „Kombi-Managementsystem on demand" angedockt!

Evolutionsstufe 7

Das „Kombi-Managementsystem“ zum „Leben“ erwecken!





Workflowmanagement

5. P/D/C/A: „Check und Act“: Steuerungs- und Überwachungs-Management

5.1 *Einer* arbeitet, *viele* überwachen!

Teuer und nervig!

"Welt der Überwacher"						
Line of defense	**Funktion**	**Berufsgruppe**	**Prüft was? z.B. Konzeptionierung, Implementierung, Wirksamkeit vor allem von: Prozessabläufen**	**Prüft wie? z.B. Dokumentenprüfung, Bobachtung, Interviews anhand von Kriterien aus ISO-/ IDW-Standard, Zielvereinbarung, Kennzahlen, usw.)**	**Prüft (Standard-) Konformität anhand von welchen Standards/ Vorgaben?**	**Form der Ergebnisse (Bericht/ Testat/ Zertifikat)**
1st line	Mitarbeiter selbst	Mitarbeiter	Prüft eigene Arbeit und Arbeitsergebnisse	Soll-Ist-Vergleich bei Zielen, Prozessen	Mitarbeiter halten sich an Prozessabläufe (Soll-Ist-Abgleich mit Prozessen und Zielvereinbarung)	Bericht/ Reporting an Vorgesetzten
	Vorgesetzter	Mitarbeiter	überwacht Mitarbeiter und eigene Arbeit	Soll-Ist-Vergleich bei Zielen, Prozessen	Mitarbeiter halten sich an Prozessabläufe (Soll-Ist-Abgleich mit Prozessen und Zielvereinbarung)	Bericht/ Reporting an Vorgesetzten
	Vorstand/ Geschäftsführer	Geschäftsleitung	überwacht MA und eigene Arbeit	Soll-Ist-Vergleich bei Zielen, Prozessen	Mitarbeiter halten sich an Prozessabläufe (Soll-Ist-Abgleich mit Prozessen [illegible]vereinbarung)	Bericht/ Reporting an Aufsichtsrat und Gesellschafter

Die Welt der Regulierer und Überwacher: Interne und externe Kontrolleure werden immer mehr!

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

2nd line	Controlling	Controller	Konzeptionierung/ Implementierung/ Wirksamkeit	Soll-Ist-Abgleich, Kennzahlenermittlung, usw.	Controlling-Standards	Reporting
	IKS (rechnungslegungsbezogen)	Wirtschaftsprüfer	Konzeptionierung/ Implementierung/ Wirksamkeit	Soll-Ist-A…		Testat/ Bericht
	Compliance	Compliance-Officer	Konzeptionierung/ Implementierung/ Wirksamkeit			Reporting an …und …g
		Wirtschaftsprüfer	Konzeptionierung/ Implementierung/ Wirksamkeit			
		Externer Zertifizierer	Konzeptionierung/ Implementierung/ Wirksamkeit	Doku… Beobachtu…	ISO 37001 (Anti-Korruption)	
		Auditor	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	COSO I? ISO 19600? IDW PS 980?	Bericht
		etc.	?	?	?	?
	Risikomanagement	Risikomanagement-Beauftragter	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	ISO 31000? COSO II? ONR 49000?	Bericht/ Reporting an Aufsichtsrat und Geschäftsleitung
		Wirtschaftsprüfer	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	IDW E PS 981 IDW PS 340 (Risiko-Früherkennungs-System)	Testat
		Externer Zertifizierer	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	in Anlehnung an ISO 31000 (nicht zertifizierbar)	Zertifikat
		Auditor	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	ISO 31000? COSO II? ONR 49000?	Audit-Bericht
		etc.	?	?	?	?
		etc.	?	?	?	?
	QM	QM-Beauftragter	?	Dokumentenprüfung/ Beobachtung/ Interviews	ISO 9001 ISO TS 16949	Bericht/ Reporting an Geschäftsleitung
		Externer Zertifizierer (z.B. TÜV/Dekra/Sonstige!	Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	ISO 9001 ISO TS 16949	Zertifikat
	weitere Funktionen der 2nd line	N.N.	?	Dokumentenprüfung/ Beobachtung/ Interviews	?	?

Die Welt der Regulierer und Überwacher: Interne und externe Kontrolleure werden immer mehr!

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

3rd line	Revision	Revisor	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	Standards des Deutschen Instituts für interne Revision (DIIR), z.B. Nr.2 für Risikomanagement	Bericht/ Reporting an Geschäftsleitung/ Aufsichtsrat
	Assurance/ Internal Investigation	?	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	?	Bericht/ Reporting an Geschäftsleitung/ Aufsichtsrat
4th line	Aufsichtsrat	Im Aufsichtsrat sind unterschiedliche Berufsgruppen vertreten/ der Prüfungsausschuss soll über besondere Sachkunde verfügen: (§ 107 AktG) überwacht Wirksamkeit von IKS, Revision, (Compliance-)Risikomanagement	alles und speziell: IKS, Revision, Compliance, Risk	Delegation auf Wirtschaftsprüfer: Dieser: Dokumentenprüfung/ Beobachtung/ Interviews	IDW PS 980, IDW E PS 981, IDW E PS 982, IDW E PS 983 usw.	Testat Testat Testat Testat Bericht des Prüfungsausschusses
	Medien	Investigative Journalisten und "Regenbogenpresse-Sensations-Paparazzi"	Fakten, Gerüchte, Vermutungen, Verdachtsmomente, etc. alles!	Rech unt bi bl au und (Edw Investiga Journalismu Einschleusen (W Interviews (Mario Barth), usw.		
	Third party audits	Kunden, Lieferanten	Konzeptionierung/ Implementierung/ Wirksamkeit	Zertifikatsnachweise oder: Dokumentenprüfung/ Beobachtung/ Interviews	Unterschiedlichste Standards	Bericht
	Staatsanwälte	Staatsanwalt	Dokumente, Zeugenaussagen	Beschlagnahme, Durchsuchung, Zeugenbefragung	Dokumente, Zeugen	Einstellung des Verfahrens Anklage etc.
	Behörden	Beamte	Dokumente	Beschlagnahme, Durchsuchung, Zeugenbefragung	Dokumente, Zeugen	Einstellung des Verfahrens Anklage Verwaltungsakte etc.
	Politik	Politiker	Alles	z. B. Untersuchtungsausschuss	Diverses	Berichte
	Banken	Bankmitarbeiter	Kennzahlen	Dokumente, …	Basel, MaRisk etc.	Ratingbericht
	Gerichte (Straf-, Zivil-, Verwaltungsgerichte)	Richter	Wirksamkeit	Urkunden, Sachverständigengutachten, Zeugeneinvernahme	Gesetz, Rechtsprechung, Anerkannter Stand von Wissenschaft und Praxis	Urteile (Bestrafung, Schadensersatz, Bestätigung von behördlichen Untersagungen, etc.)
	...					
	...					

„1 Funktion arbeitet - Und 20 überwachen!“

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

5.2 Was wollen alle „Überwacher“ wissen? Das Gleiche – wie schon zuvor!

Alle wollen das Gleiche: Auch die „Überwacher“! Was?

1. Angemessene Ziele und Kennzahlen (Plan)

Beispiele: Pflichtziele (Compliance) und fakultative Ziele (business-judgment-rule):
Z. B. Wertsteigerung, Wertbeiträge, Nachhaltigkeit,
Social responsibility, Innovationsführerschaft

2. Angemessene Planung (Plan)

Beispiele: Wirtschaftsplan, Finanzplan, Personalplan, Produktionsplanung, Liquiditätsplanung, Investitionsplanung, etc.

3. Sorgfältige Umsetzung: Wirksame (gelebte) angemessene Prozesse (Do)

Beispiele: Beachtung der Gesetze (Compliance) und Beachtung des anerkannten Standes von Wissenschaft und Praxis, Beachtung von Standards (?), Beachtung der Anforderungen an Produkte und Leistungen (effektiv, qualitativ, sicher, rechtssicher usw.)

4. Angemessenes und wirksames Steuerungs- und Überwachungssystem (Check)

Alle wollen das Gleiche: Auch die „Auch die Überwacher“! Was?

Beispiele: Das „lines of defense“-Modell.

5. Grad der Zielerreichung (über Kennzahlen / KPI‘s)?:

Beispiele: Finanzkennzahlen, Personalkennzahlen (Human Capital Metrics), Compliancekennzahlen, Innovations-, Nachhaltigkeits-, Social Responsibility-Kennzahlen, usw.

Sind Sie als Inhaber/Gesellschafter des Unternehmens an Governance, Risk und Compliance (GRC) interessiert, weil es hilft, den Unternehmenswert nachhaltig zu sichern bzw. zu erhöhen?

- ❑ Ja
- ❑ Nein

Schenken Sie Ihrem Kunden mehr Vertrauen in Bezug auf seine Zahlungsfähigkeit, wenn dieser ein gelebtes Risiko- und Compliance-Managementsystem unterhält und sein Unternehmen danach lenkt?

- ❑ Ja
- ❑ Nein

Bitte bewerten Sie nachfolgende Thesen:
Ein gelebtes Integriertes Managementsystem mit Risk und Compliance (GRC) bringt in der aktuellen wirtschaftlichen Situation:

Vorteile gegenüber Kunden (z. B. glaubt / weiß der Kunde, dass er einen sicheren / zuverlässigen Lieferanten hat):

- ❑ Ja, sehr wahrscheinlich
- ❑ eher unwahrscheinlich (glaube ich nicht)

Bitte bewerten Sie nachfolgende Thesen:
Ein gelebtes gelebtes Integriertes Managementsystem mit Risk und Compliance (GRC) bringt in der aktuellen wirtschaftlichen Situation:

Vorteile für den Unternehmer selbst (z.B. durch die Möglichkeit, Unternehmen und Mitarbeiter optimal führen zu können und durch Reduzierung der eigenen Haftungsrisiken):

- ❑ Ja, sehr wahrscheinlich
- ❑ eher unwahrscheinlich (glaube ich nicht)

Bitte bewerten Sie nachfolgende Thesen:
Ein gelebtes Integriertes Managementsystem mit Risk und Compliance (GRC) bringt in der aktuellen wirtschaftlichen Situation:

Vorteile für das Unternehmen (z.B. durch Nutzung brachliegender Chancen und realistischer Einschätzung sowie Beherrschung von Risiken):

- ❑ Ja, sehr wahrscheinlich
- ❑ eher unwahrscheinlich (glaube ich nicht)

Aufsichtsräte / Beiräte

Da sich **bei Aufsichtsräten** eine erhöhte Sensibilität bzgl. ihrer Verantwortung und Haftungsgefahren einstellt, wird sich auch die **Nachfrage nach effizienten Kontroll- und Berichtsmechanismen** erhöhen.

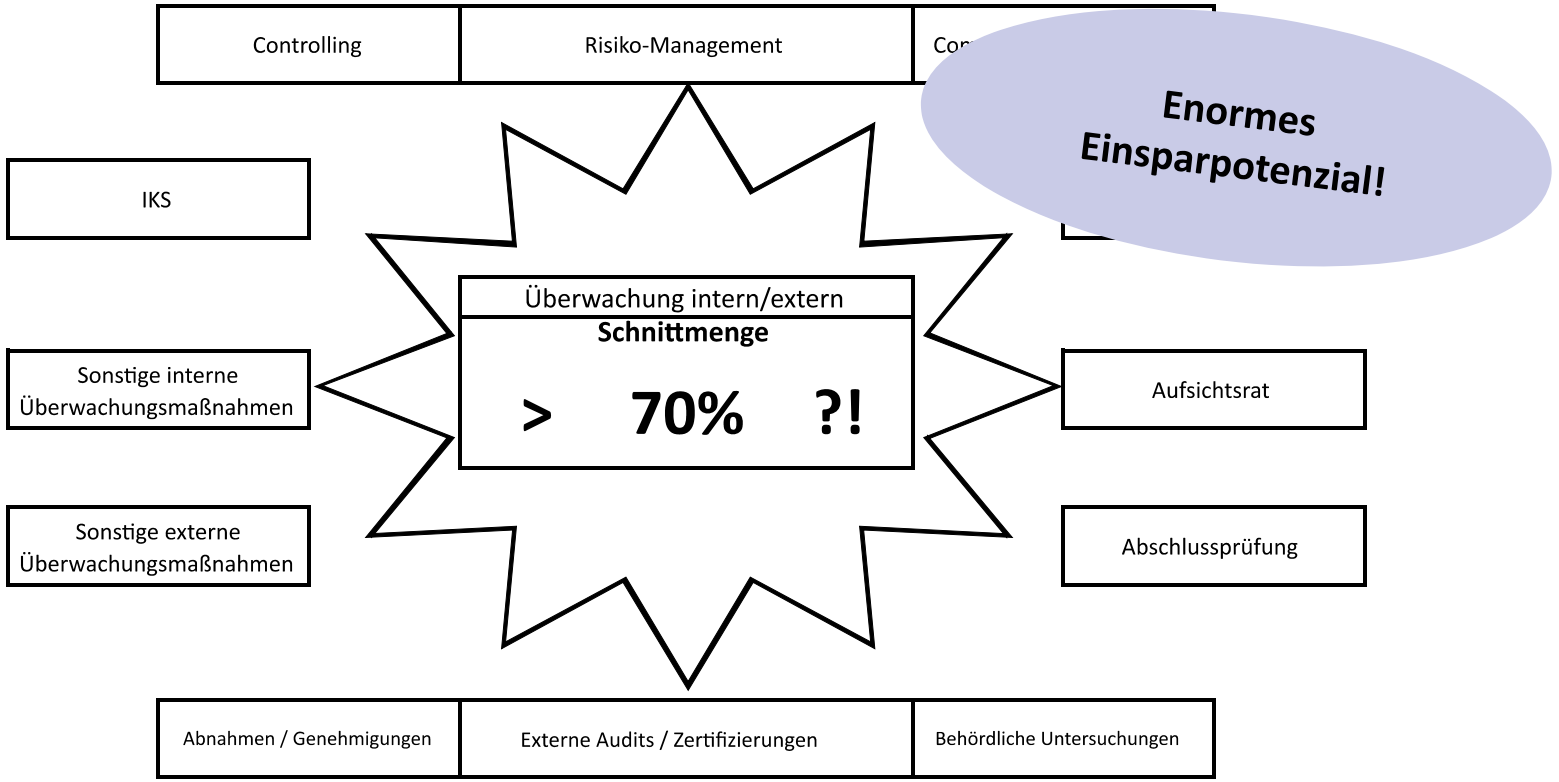
Der Aufsichtsrat ist gem. § 107 AktG für die Wirksamkeit (das „Gelebt-werden“) von Risiko-, Compliance-Managementsystem, Internem Kontrollsystem und Revision *persönlich* verantwortlich!

Bitte bewerten Sie nachfolgende Thesen:
Ein gelebtes Integriertes Managementsystem mit Risk und Compliance (GRC) bringt in der aktuellen wirtschaftlichen Situation:

Vorteile für Aufsichtsrat / Beirat (z.B. durch Reduzierung der eigenen Haftungsrisiken sowie Erleichterung der Wahrnehmung der Kontrollaufgaben):

- ❑ Ja, sehr wahrscheinlich
- ❑ eher unwahrscheinlich (glaube ich nicht)

5.3 Enormes Potenzial für Wertzuwachs und Wertbeiträge durch GRC



…Redundanzen vermeiden,

Ressourcen (Zeit, Geld, Nerven, …) schonen!

Quelle: *Scherer / Fruth* (Hrsg.), Governance-Management, Band II, 2016, S. 221

Wertbeitrag und Wert eines Integrierten Managementsystems

„Wenn in den diversen einzelnen Unternehmensfunktionen/ Prozessfeldern/ Themenbereichen / oder bei (Corporate) Governance generell („GRC als Klammer“) ein ***hoher Reifegrad*** *erreicht wird, resultiert daraus* ***automatisch*** *ein* ***hoher Nachhaltigkeitsgrad, Wertbeitrag und Pflichterfüllungsgrad.***

Damit werden die Ziele von Unternehmen, Management und Mitarbeitern mit hoher Wahrscheinlichkeit erreicht und es entsteht ***somit auch ein hoher Zielerreichungsgrad.“***

(Scherer)

*Auch **Achleitner**[9], eine Koryphäe im Bereich private equity und investment, ist der Ansicht, dass „**Corporate Governance ein wichtiger Werttreiber**“ wird/ist:*

*„Wenn man sich die Hebel der Wertschöpfung in den vergangenen 30 Jahren anschaut, dann war die Verbesserung der operativen Wertschöpfung der wichtigste. (…) „Die **operative Wertschöpfung wird die größte Herausforderung für die Unternehmen (…) in Zukunft sein. (…) In den vergangenen Jahren stand Corporate Governance oft unter dem Überwachungsaspekt. Der wertschöpfende Aspekt fehlte dagegen. Es geht um bessere unternehmerische Entscheidungen durch funktionierende und gelebte Governance** (…)*

Eine gute Corporate-Governance-Praxis wird ein entscheidender Wettbewerbsfaktor in der Zukunft** (…) aus der Beteiligungspraxis hören sie, **dass es Fälle gibt, in denen die Corporate Governance zwei Drittel der Wertsteigerung der Firmen beisteuert. (…)“

[9] Achleitner, TU München, (Entrepreneurial Finance), Handelsblatt, 30.06.2015, S. 28.

6. Umrüstung der Organisation auf ein Integriertes „GRC-Kombi-Managementsystem on demand“

Umrüstung der Organisation auf ein Integriertes „Kombi-Managementsystem on demand“

1. Ausgangslage Analyse/ Bewertung: Was wird gewünscht, gebraucht?
Anforderungen der benötigten/ gewünschten Kombi-Standards „on demand“ (z.B. Integriertes System mit QM mit Risk, Compliance, IKS und Nachhaltigkeit ...)

Ziel: Über einen (Risiko-) Workshop wird ermittelt, welches Kombi-Managementsystem konkret benötigt wird. Für eine Pilotphase kann auch ein spezielles Prozess-Themenfeld des Unternehmens ausgewählt werden.

↓

2. Konzept mit Soll-Ist-Abgleich

Ziel: Die Konzeptionierung des Integrierten Managementsystems stellt als Prüfgegenstand zum einen ein Basiselement in Hinblick auf eine mögliche *Konzeptionierungs- und Implementierungsprüfung* dar. Zum anderen dient die Konzeptionierung der Planung zukünftiger Implementierungstätigkeiten, indem ein Soll-Ist-Abgleich Lücken im vorhandenen Managementsystem aufzeigt.

↓

3. Implementierung

Ziel: Die im Soll-Ist-Abgleich ermittelten fehlenden Komponenten werden in die Geschäftsprozesse basis-implementiert. Dies bedeutet, die Komponenten werden g
revisionssicher neu erstellt oder vorhandene Komponenten geprüft, danach vom Top-Management als verbindlich erklärt und an geeigneter Stelle in die Geschäftspro
eingebunden. Die Leistung des Auftragnehmers kann sich hierbei sowohl auf die aktive Erstellung oder Prüfung von Dokumenten beziehen oder auf eine unterstützend
beratende Tätigkeit z.B. in Hinblick auf die passende Verortung der Komponenten in den Geschäftsprozessen beschränken.

↓

4. Ready for (Konzeptionierungs- und Implementierungs-) Audit

Ziel: Durch ein internes Audit soll die Zertifizierungsreife für die Konzeptionierungs- und Implementierungsprüfung auf Basis des Universal-Standards festgestellt werden. Gleichzeitig wird der Auftraggeber bei der Zertifizierungsgesellschaft zur Zertifizierung angemeldet und Organisatorisches durch den Auftragnehmer übernommen.

↓

5. Zertifizierung nur bzgl. Konzeptionierung und Implementierung

Ziel: Die *Konzeptionierungs- und Implementierungs-Zertifizierung* erfolgt über Kooperationspartner (z.B. für Compliance *ComZert* oder für QM *TÜV/ Dekra*/ etc.) oder das Internationale Institut für Governance, Management, Risk und Compliance (www.gomaricom.de)

Nach dem Audit erhält der Auftraggeber einen Auditbericht, der mögliche Nachbesserungen aufzeigen kann. Der Auftragnehmer unterstützt den Auftraggeber, diese Nachbesserungen vorzunehmen. Etwaige Maßnahmen werden im Vorfeld gemeinsam mit dem Auftraggeber besprochen und projektiert.

↓

Vorgehensweise bei der „Umrüstung“

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand, -Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017, <IMS>

Umrüstung der Organisation auf ein Integriertes „Kombi-Managementsystem on demand“

6. Kommunikation an interested parties

Ziel: Die diversen "interested parties" werden klassisch oder über einen Datenraum mit speziellen Zugriffsberechtigungen über den „Erfolg“ benachrichtigt.

7. Herbeiführung der Wirksamkeit in diversen Bereichen

Ziel: Das integrierte Managementsystem bzw. die in die Organisation basis-implementierten Komponenten müssen von den Mitarbeitern verstanden und in der Folge „gelebt-werden“. Das Trainingskonzept plant dabei die wesentlichen methodischen, didaktischen und inhaltlichen Komponenten und ermöglicht dadurch die zielgerichtete Durchführung von Schulungen.

Der Auftragnehmer übernimmt die Schulungen der Führungskräfte und/oder Mitarbeiter auf Basis des abgestimmten Schulungskonzeptes.

Der Auftragnehmer unterstützt das Unternehmen bei der Herbeiführung der Wirksamkeit („Gelebt-werden“) des integrierten Managementsystems für ausgewählte Komponenten (z.B. Kernprozesse) beratend bzw. schulend.

8. Ready for (Wirksamkeits-) Audit

Ziel: Der Auftragnehmer übernimmt die Vorbereitungen auf das Zertifizierungsaudit, indem das Angebot beim Zertifizierer eingeholt und ggf. verhandelt wird sowie Themen im Zusammenhang mit dem sog. Auditmanagement (z.B. Termine, etc.) geregelt werden.

Durch ein internes Audit soll die Zertifizierungsreife **für die Wirksamkeitsprüfung** (bezogen auf bestimmte Komponenten) auf Basis des Universal-Standards festgestellt werden. Gleichzeitig wird der Auftraggeber bei der Zertifizierungsgesellschaft zur Zertifizierung angemeldet und Organisatorisches durch den Auftragnehmer übernommen.

9. (Wirksamkeits-) Zertifizierung

Ziel: Die *Wirksamkeits*-Zertifizierung erfolgt über Kooperationspartner (z.B. für Compliance ComZert oder für QM: TÜV/ Dekra/ etc.) oder das Internationale Institut für Governance, Management, Risk und Compliance (www.gomaricom.de).

Nach dem Audit erhält der Auftraggeber einen Auditbericht, der mögliche Nachbesserungen aufzeigen kann. Der Auftragnehmer unterstützt den Auftraggeber, diese Nachbesserungen vorzunehmen. Etwaige Maßnahmen werden im Vorfeld gemeinsam mit dem Auftraggeber besprochen und projektiert.

10. Kommunikation an interested parties

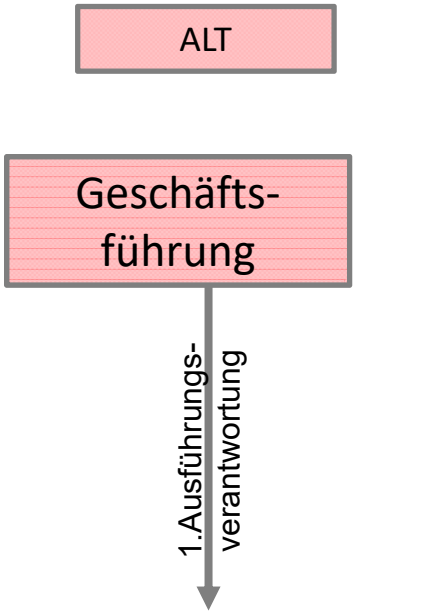
DIe diversen "interested parties" werden klassisch oder über einen Datenraum mit speziellen Zugriffsberechtigungen über den "Erfolg" benachrichtigt.

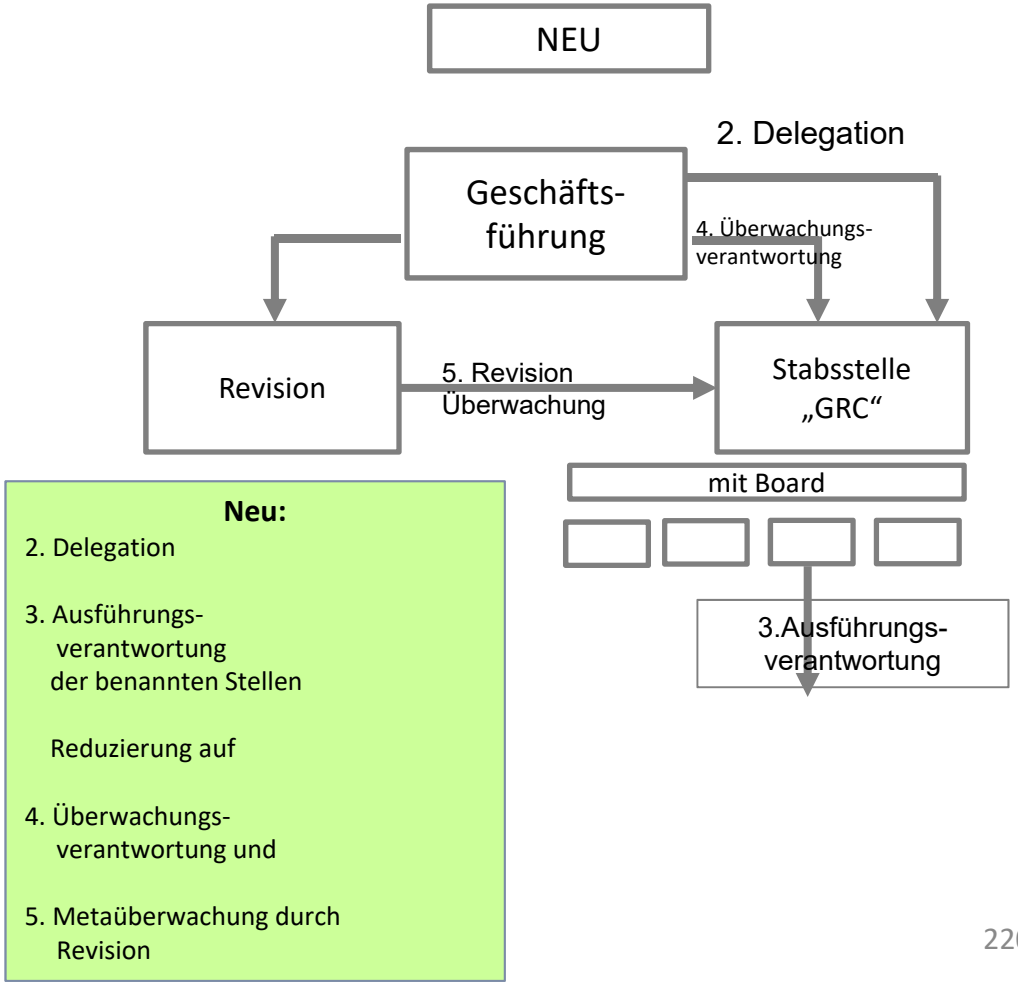
Vorgehensweise bei der „Umrüstung“

Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand / - Ziele, Organisations- sowie Steuerungs- und Überwachungsmanagement, 2017

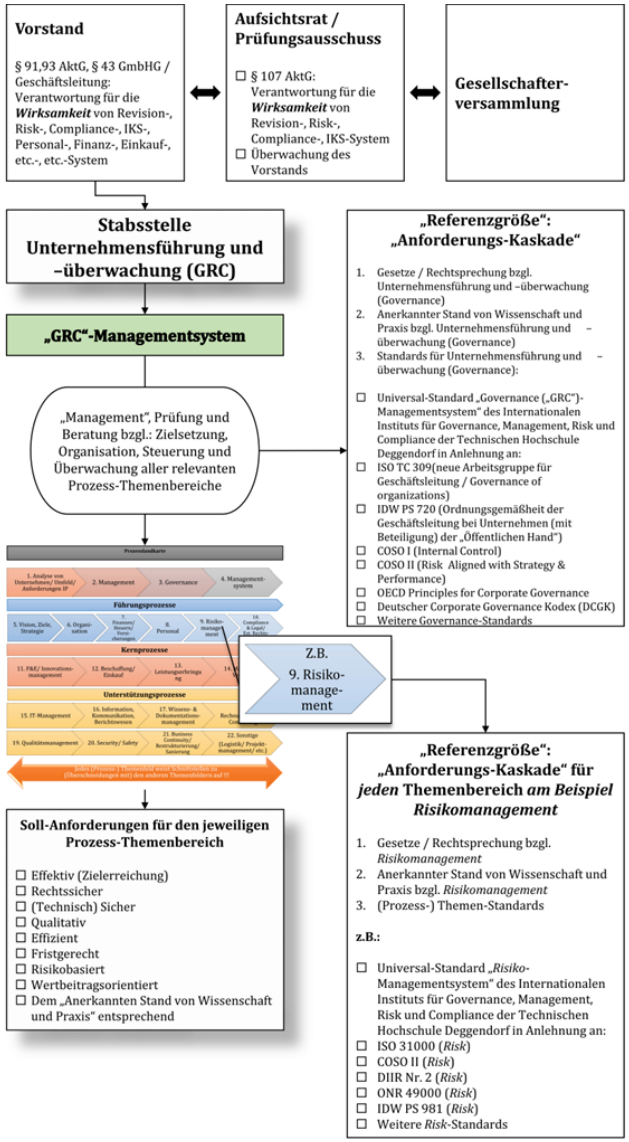
Aufgaben und Ziele der Geschäftsführung

Delegation von (Routine-)Aufgaben und Verantwortung auf die Stabsstelle „GRC“
„Rücken frei“ für höchstpersönliche Aufgaben

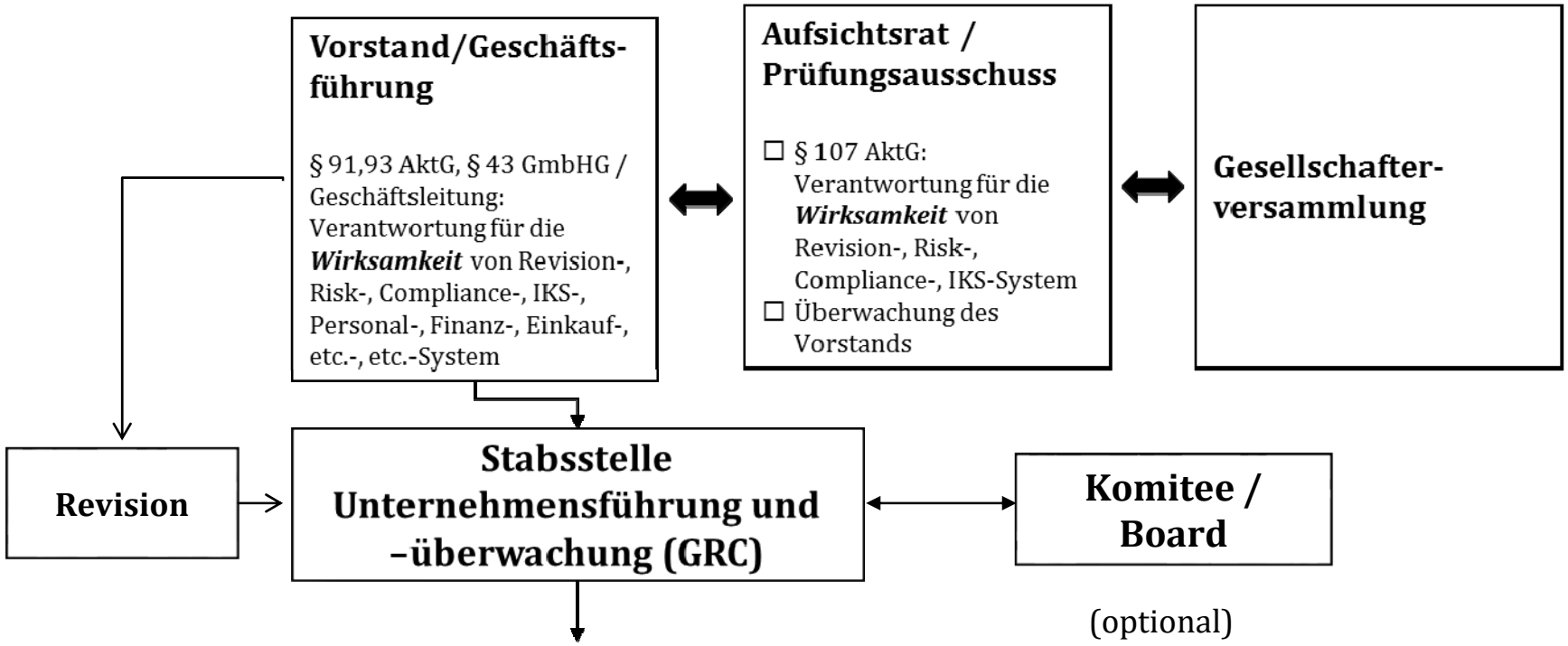




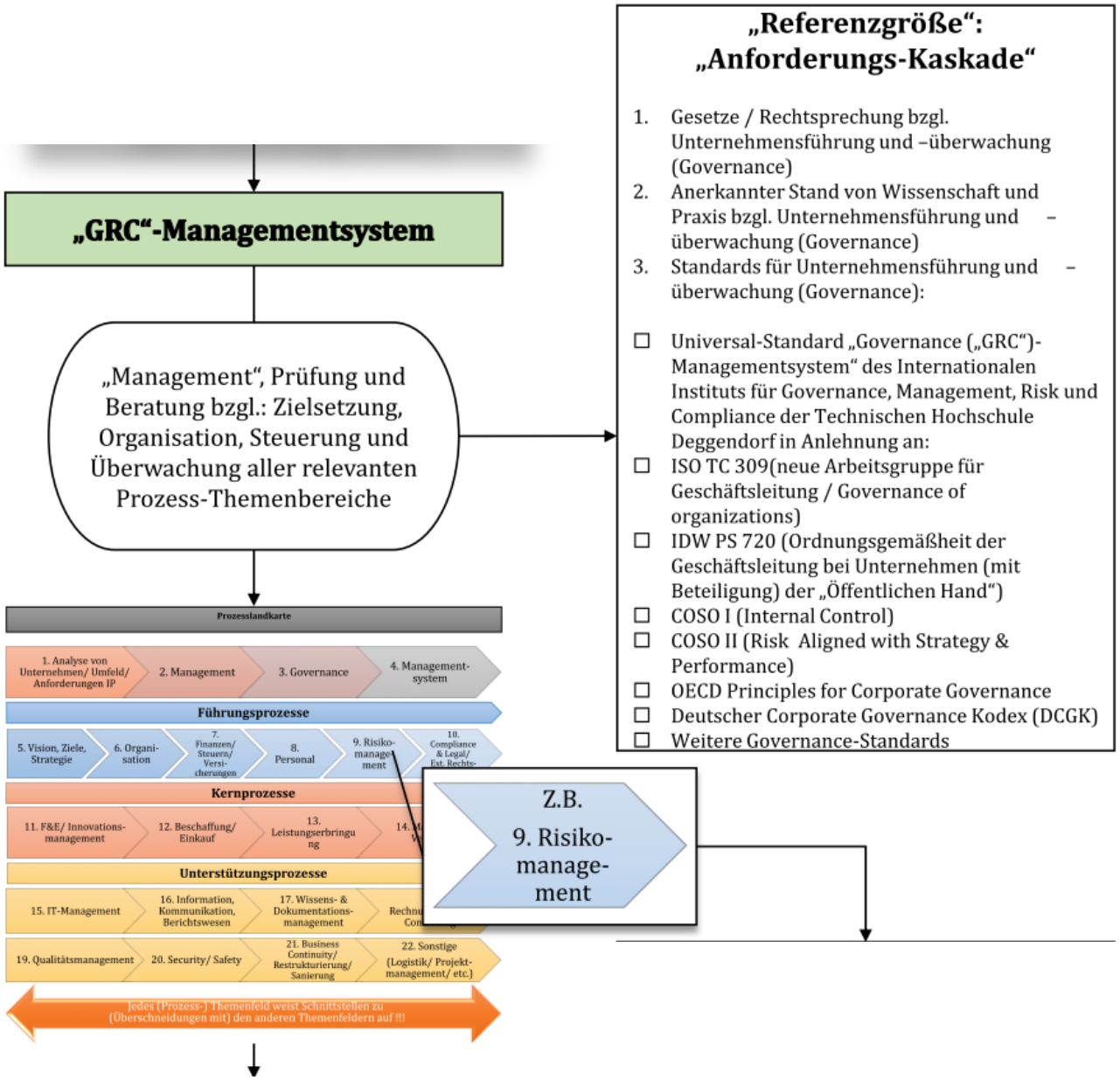
Das Zusammenspiel von Geschäftsleitung und „GRC-Stelle“



Delegation vieler Organisations-, Steuerungs- und Überwachungs-aufgaben auf die „GRC-Stelle“



Wie sehen die Anforderungen an eine solche „GRC-Stelle“ aus?



Was sind die Anforderungen/Referenzgrößen bzgl. der Themen, um die sich die „GRC-Stelle“ zu kümmern hat?

Z.B.
9. Risiko-manage-ment

Soll-Anforderungen für den jeweiligen Prozess-Themenbereich

- ☐ Effektiv (Zielerreichung)
- ☐ Rechtssicher
- ☐ (Technisch) Sicher
- ☐ Qualitativ
- ☐ Effizient
- ☐ Fristgerecht
- ☐ Risikobasiert
- ☐ Wertbeitragsorientiert
- ☐ Dem „Anerkannten Stand von Wissenschaft und Praxis“ entsprechend

„Referenzgröße“: „Anforderungs-Kaskade“ für *jeden* Themenbereich *am Beispiel Risikomanagement*

1. Gesetze / Rechtsprechung bzgl. *Risikomanagement*
2. Anerkannter Stand von Wissenschaft und Praxis bzgl. *Risikomanagement*
3. (Prozess-) Themen-Standards

z.B.:

- ☐ Universal-Standard „*Risiko*-Managementsystem“ des Internationalen Instituts für Governance, Management, Risk und Compliance der Technischen Hochschule Deggendorf in Anlehnung an:
- ☐ ISO 31000 (*Risk*)
- ☐ COSO II (*Risk*)
- ☐ DIIR Nr. 2 (*Risk*)
- ☐ ONR 49000 (*Risk*)
- ☐ IDW PS 981 (*Risk*)
- ☐ Weitere *Risk*-Standards

Positive Folgen der Delegation von Aufgaben und Verantwortung auf die Stabsstelle „GRC“ (mit Board)

Delegation

Die Geschäftsführung trägt grundsätzlich persönlich die straf- und zivilrechtliche Verantwortung für *alle* Tätigkeiten im Unternehmen.

Durch eine rechtssichere Delegation, beispielsweise auf eine Stabsstelle, kann sich die Geschäftsführung gewissermaßen „enthaften“. Des Weiteren reduziert sich die Gesamtverantwortung auf folgende Komponenten:

1. Überwachungsverantwortung (diese kann – teilweise – delegiert werden als Meta-Überwachung.)

2. Übernahme der vollen Verantwortung in Krisensituationen

Folgendes ist zu beachten:

- Auswahl und Instruktion von Delegationsempfängern und Aufgabenverteilung (Organigramme, Stellenbeschreibungen) (mit *Dokumentation)* (persönlich durch die Geschäftsführung oder über Stabsstelle „GRC“ etc.)
- Beachtung des Delegationsprozesses (mit *Dokumentation*)
- *Überwachung* der Art und Weise der Umsetzung der Aufgaben sowie der zu beachtenden gesetzlichen Bestimmungen (Verfahrens- und Prozessbeschreibungen, Muster, Arbeitsanweisungen etc.) (mit Dokumentation) (persönlich durch die Geschäftsführung oder über Stabsstelle „GRC“ etc.)
- Kontrolle und laufende Verbesserung

Lösungen:

Wie sieht für eine geplante Umrüstung auf ein Integriertes Managementsystem eine Beauftragung aus und was kostet es?

Mögliche Alternativen:

1: Inselsystem

2: Integriertes-System

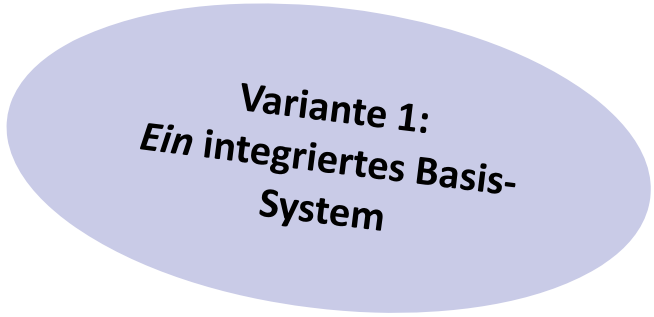
3: Prototyp-Komponenten

6.1 Variante 1:

„Inselsystem“ als Basis für spätere Erweiterung auf ein Integriertes Managementsystem

Es wird lediglich ein „Insel-Managementsystem“ benötigt / gewünscht:

Beispiel: Ein *Risiko*-Managementsystem



Würden Sie lieber zunächst eine Insel als ausbaufähige Basis für eine Erweiterung auf ein Integriertes Managementsystem einführen?

Welche erachten Sie für am dringendsten?

- ☐ Qualitätsmanagementsystem
  (z.B. ISO 9001:2015 neu:))
  mit Risiko- & Compliancemanagement!
- ☐ Risiko-Managementsystem
- ☐ Compliance-Managementsystem
- ☐ Internes Kontroll-System
- ☐ Revision
- ☐ Nachhaltigkeits-Managementsystem

Würden Sie lieber zunächst eine Insel als ausbaufähige Basis für eine Erweiterung auf ein Integriertes Managementsystem einführen?

Welche erachten Sie für am dringendsten?

- ☐ IT-Sicherheits-Managementsystem
- ☐ Arbeits- und Gesundheitsschutz-Managementsystem
- ☐ Personal-Managementsystem
- ☐ Datenschutz-Managementsystem
- ☐ etc.
- ☐ Sonstiges: _____

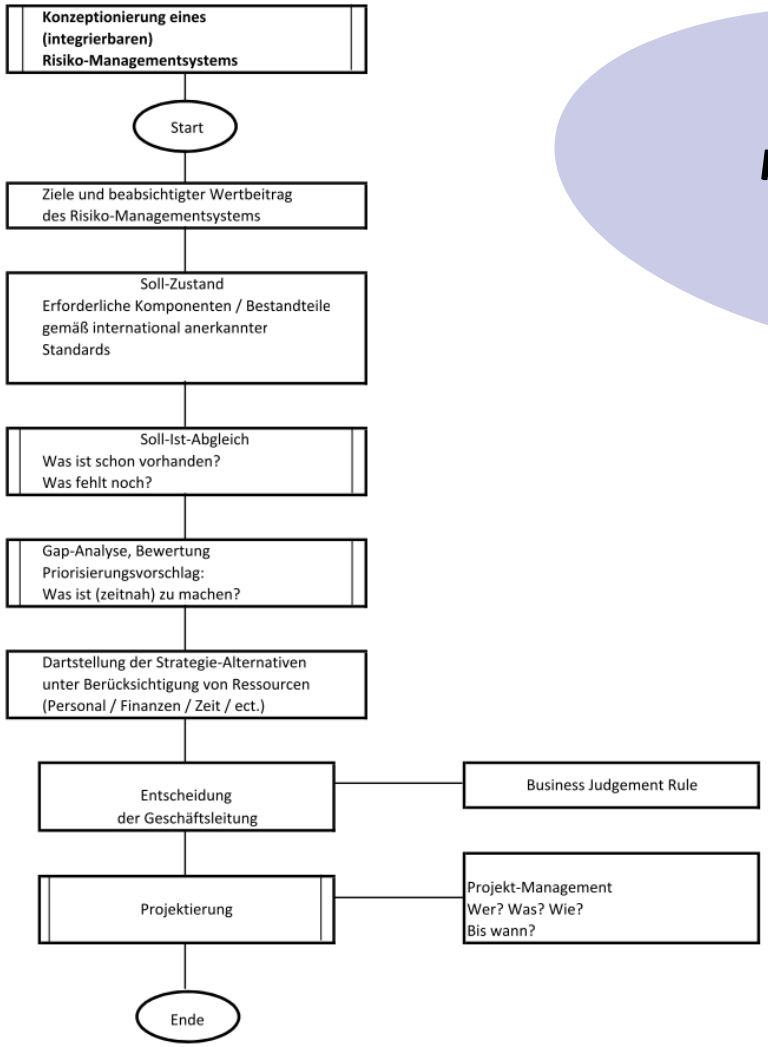
_____

Lösungen:

- **Insel-Managementsystem**

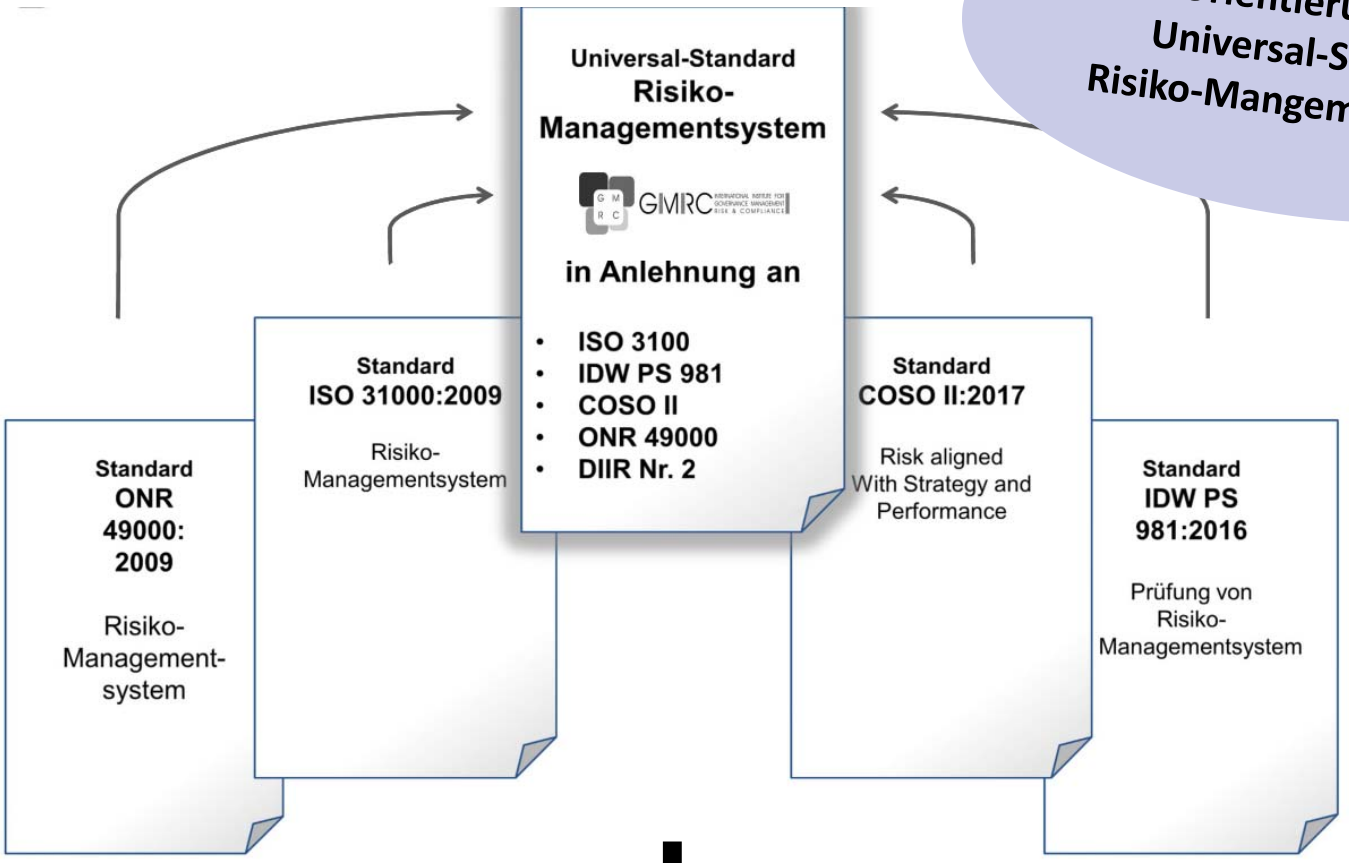
(z. B. „nur“ Compliance-Managementsystem oder „nur“ Risiko-Management)

Ablauf: Konzeptionierung eines (integrierbaren) Risiko-Managementsystems



Soll-Zustand:
Erforderliche Komponenten / Bestandteile
gemäß international anerkannter Standards

Orientierung am Universal-Standard Risiko-Mangementsystem



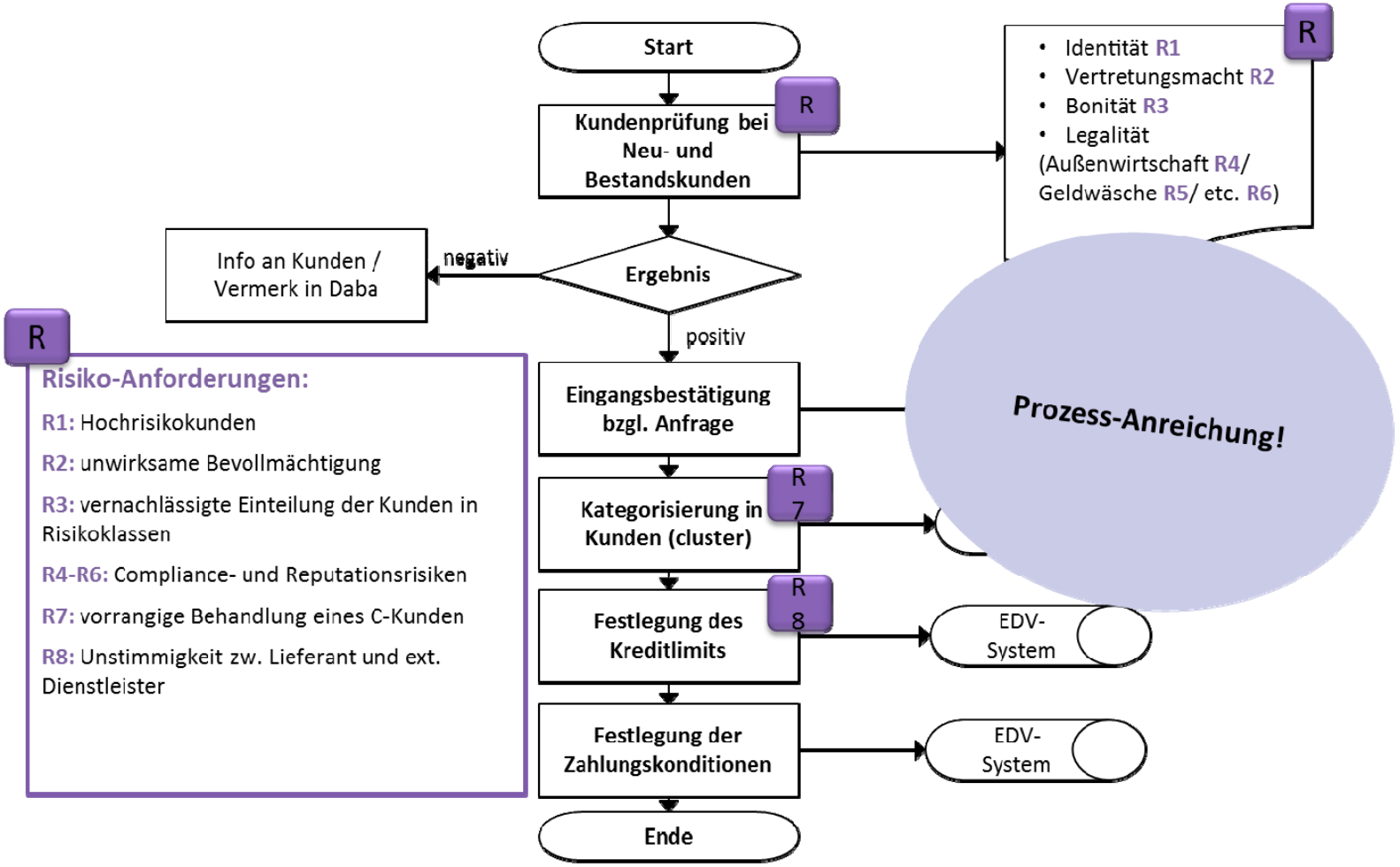
Auszug aus Katalog der Komponenten / Bestandteile des Universal-Standards Risiko-Managementsystem

2.2		Ableitung des Unternehmensrahmens aus bewerteter Unternehmens- und Umfeldanalyse mit Anforderungen „interessierter Gruppen"
2.2.1	Ableitung des Unternehmensrahmens	Unternehmensvision, Mission, Leitbild, Ziele, Strategie, Planung
Komponente		K10 Unternehmensvision, Mission, Leitbild, Ziele, Strategie, Planung mit Unternehmenspolitik
Tool		*Prozess(sheet) „Strategieentwicklung" unter Beachtung der kurz-, mittel- und langfristigen Planung.*
Tool		*(Konzeptionierung eines) Strategieworkshop.*
Tool		*(Konzeptionierung eines) Handbuch „Vision, Mission, Leitbild, Ziele, Strategie, Planung und Steuerung".*
Tool		*Kompetenzziele für Management und Mitarbeiter im Bereich CMS.*
Tool		*Matrix mit Zielen (Kennzahlen) der Unternehmensbereiche / Prozesse.*
Tool		*Kennzahlensystem.*
Tool		*Muster-Zielvereinbarung mit Management und Mitarbeitern.*
Tool		*Formular BJR bei Setzung von Zielen/ Entscheidungen mit Ermessensspielräumen.*
2.2.2		Unternehmenspolitik (Grundsätze der Unternehmensführung)
Tool		*Dokument „Unternehmenspolitik" mit Ableitung auf die Unternehmensbereiche.*
2.2.3		Organisatorischer Rahmen (unternehmensweit)
Tool		*Gesellschafts-(Gruppen-)struktur-Optimierung.*
Tool		*Rechtssichere Organigramme.*
Tool		*Schnittstellenmanagement über Prozesse / Stellenbeschreibungen / Koop-Vereinbarungen mit Geschäftspartnern.*
Tool		*Rechtssichere Stellenbeschreibungen.*
Tool		*Rechtssicheres Interaktionsmanagement.*
Tool		*Delegationsprozess-Sheet (rechtssichere Delegation) inkl. Überwachung Externer Business Partner.*
Tool		*Prozesslandschaft und dokumentierte und geschulte Prozessbeschreibungen (inkl. Verfahrensanweisungen).*
Tool		*(Wirksame) Aufsichts- und Kontrollmechanismen (z. B. Internes Steuerungs- und Überwachungssystem oder IKS).*
Tool		*(Wirksames) Info- und Kommunikationsmanagement.*
Tool		*(Wirksames) Dokumentations- und Wissensmanagement.*
Tool		*Compliance-Managementsystem.*
Tool		*Angemessenes CMS (angemesse CMSressourcen in Quantität und Qualität).*
2.2.4		Kommunikationsrahmen (unternehmensweit)
Komponente		*K12 Kommunikationsmanagement*
Tool		*Kommunikationskonzept (5xW) / interne und externe Kommunikation.*
Tool		*Informationsmanagement mit Kommunikation (inkl. Reporting).*
Tool		*Übersicht über periodische / regelmäßige protokollierte Besprechungen / Reportings.*
2.2.5		Dokumentationsrahmen (unternehmensweit)
Komponente		*K13 Dokumentationsmanagement*
Tool		*Lenkungsprozess für Dokumente und Aufzeichnungen.*

Ausschnitt: Katalog der Komponenten eines Risiko-Managementsystems

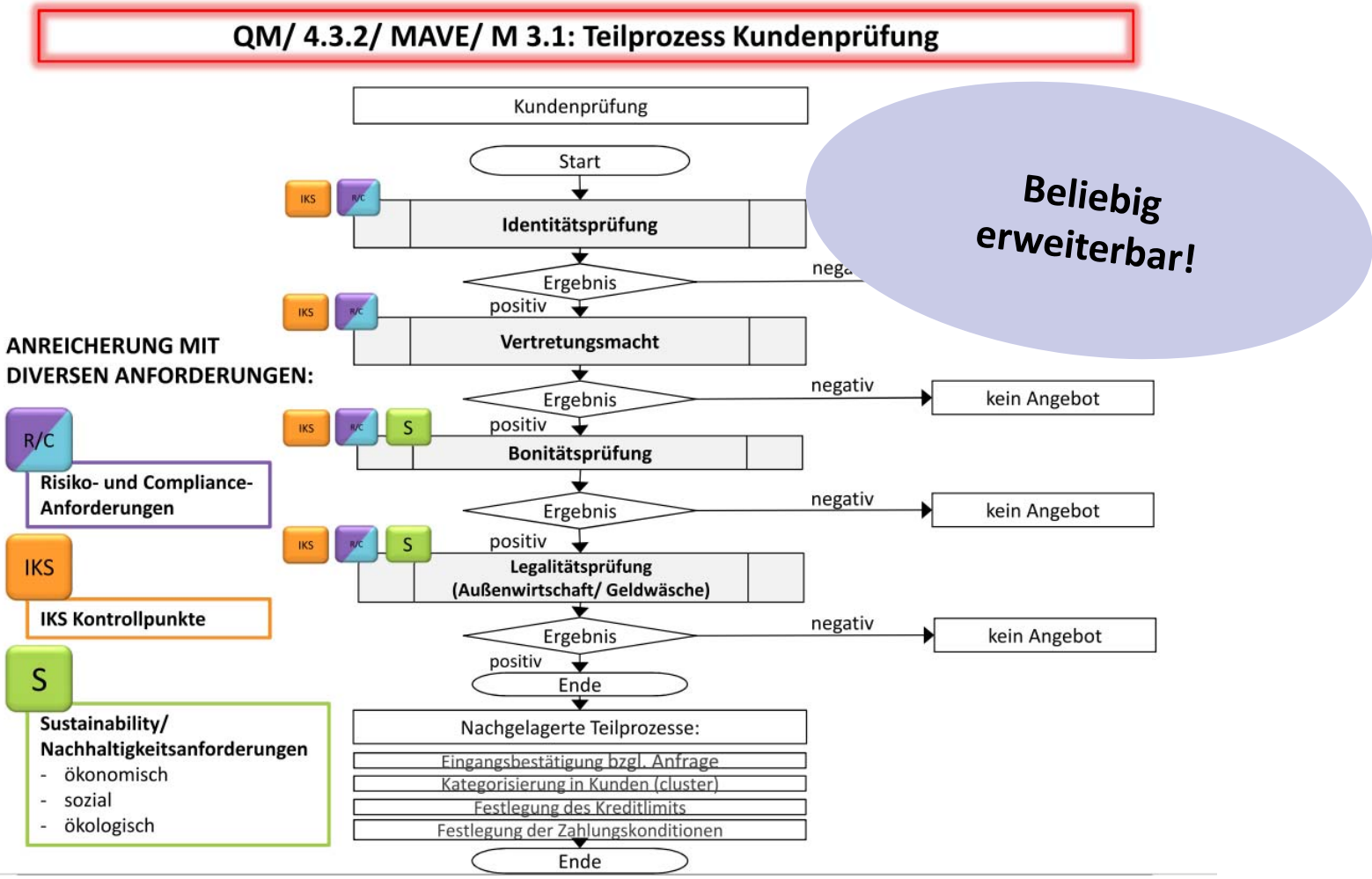
Anreicherung der Prozesse mit Risikomanagement-Komponenten

QM/ 4.3.2/ MAVE/ M3: Kundenanlage – Die Anreicherung mit Anforderungen aus Risk



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 119

Aufgrund analoger Vorgehensweise als Grundlage für Anreichung mit Compliance-Management- C , Internes Kontroll-System- IKS , Nachhaltigkeits-Management- , etc. S -Komponenten verwendbar!



Quelle: *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit GRC, 2016, S. 122

6.2 Variante 2: Integriertes GRC-Kombi-Managementsystem „on demand“ (die umfassendste Lösung)

Lösungen:

- **Integriertes Managementsystem**

  (z. B. Qualitäts-Managementsystem (ISO 9001:2015) mit Risk, Compliance und IKS: alles in einem!)

Lösungen:

❑ Beratung und Vertretung im Wirtschaftsrecht

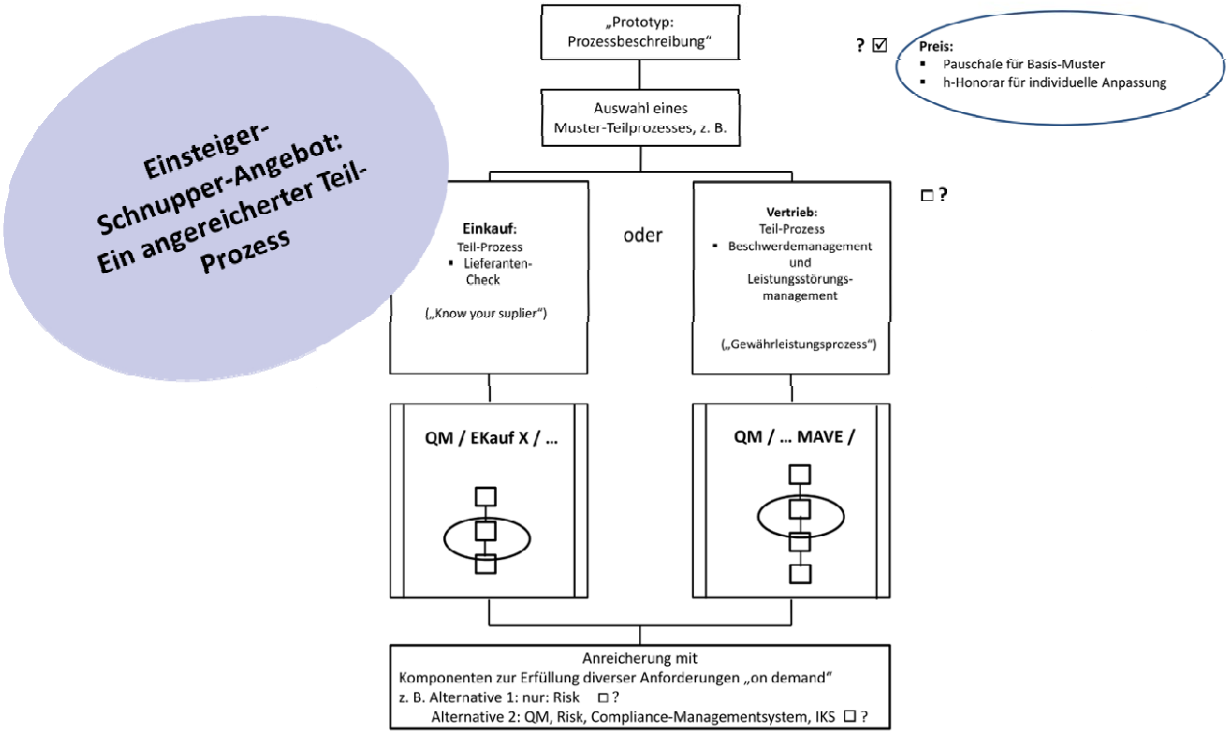
Durch Compliance, Globalisierung und Digitalisierung **veränderten sich auch die Anforderungen an flankierende Beratung im Wirtschaftsrecht.**

Die wachsenden rechtlichen und regulatorischen Anforderungen erfordern **besondere persönliche und fachliche Kompetenzen in der Rechtsberatung**.

6.3 Variante 3: Erstellung einer Prototyp-Komponente

Diese Variante ist empfehlenswert:

Testen Sie mit wenig Zeit und Geld eine Prototyp-Komponente (einen Prozess oder ein Tool) und entscheiden Sie, ob Wertbeiträge für Sie und Ihr Unternehmen entstehen.



7. Tue Gutes und rede darüber:

Intern oder extern:

Reifegradmessung / Audit / Zertifizierung

Lösungen:

- **Reifegradmessung / Audit / Zertifizierung**

Ihre Leistungen, Prozessabläufe, Managementsystem(e) oder einzelne Komponenten daraus, müssen – **objektiv nachgewiesen und dokumentiert** – den Anforderungen von Geschäftspartnern, Behörden und sonstigen „interessierten Parteien“ („stakeholder“) genügen.

Gleichzeitig jedoch sollte **der dafür erforderliche Aufwand möglichst gering** sein:
Durch integrierte Systeme werden Redundanzen aufgelöst und **Audits / Zertifikate wesentlich günstiger**.

7. Wir stellen uns vor:

Das Internationale Institut für Governance, Management, Risk und Compliance der Technischen Hochschule Deggendorf

als

„Deggendorfer Schule GRC“ für Unternehmensführung und -überwachung (Governance), Risiko- und Compliance-Management

Link zur Homepage und zum Flyer:

www.gmrc.de

Besonderheiten der „Deggendorfer Schule GRC“ des Internationalen Instituts für Governance, Management Risk & Compliance der Technischen Hochschule Deggendorf (www. gmrc.de):

1. **Organisations- und Prozessorientierung/Workflow-Management:**
   Darstellung jedes Themenbereichs eines Unternehmens anhand der typischen (bekannten) Aufbau- und Ablauforganisation als workflow (Digitalisierung).

2. **Interdisziplinarität:**
   Wirtschaftswissenschaften, Recht, Technik, Psychologie, Soziologie: Welche Anforderungen der diversen Disziplinen sollten beachtet werden?

3. **Compliance-Orientierung:**
   Welche (rechtlich) verbindliche (internationalen) Rahmenbedingungen (aus Gesetzen, Rechtsprechung, etc.) sind zu beachten?

4. **Orientierung am (international) „Anerkannten Stand von Wissenschaft und Praxis“**
   Was ist „good practice“?

5. **Orientierung an (inter)nationalen anerkannten Standards:**
   ISO, COSO, IDW, DIN, DIIR, etc..

6. **Risikobasierung:**
   Identifikation, Bewertung und Steuerung von Gefahren und Chancen bei Zielfestlegung, Entscheidungen und Umsetzungsmaßnahmen zur Zielerreichung.

7. **Wertbeitragsorientierung**:
   Reflexion, Beschreibung und Messung der Aufwand / Nutzen - Relation (in den einzelnen Unternehmensbereichen bzw. Prozessen).

8. **Integrierter Managementsystem-Ansatz**:
   Ein integriertes „Kombi-GRC-System“ statt „Insellösungen“

9. **„Industrie 4.0“ und Mensch:**
   Darstellung von vertikalen (zwischen einzelnen Unternehmensfunktionen) und horizontalen (entlang der „Wertschöpfungskette“ zu Lieferanten und Kunden) sowie diametralen (zu den „interested parties“) Schnittstellen und Clustern (vgl. „Industrie 4.0“) sowie der künftig erforderlichen Kompetenzen von Geschäftsleitung und Mitarbeitern.

Die „Deggendorfer Schule GRC“ – www.gmrc.de

Ein Kompetenzzentrum:

- **Netzwerk von Koryphäen in Wissenschaft und Praxis**
- **Netzwerk** von **Governance-**, Risikomanagement- und Compliance-**Profis**
- **Netzwerk** von spezialisierten **Auditoren** (QM/Risk/Compliance/IKS/Revision/etc.).
- **Netzwerk** von **Workflow**-Management-**Spezialisten**

❑ Aktuelle Veröffentlichungen

(überwiegend kostenlos zum Volltext-download)

Zur Vertiefung finden Sie auf www.gmrc.de viele Veröffentlichungen zu den Themen:

- ❑ Managerhaftung
- ❑ Digitalisierung und Prozessmanagement
- ❑ Ordnungsgemäße Unternehmensführung (Governance)
- ❑ Risiko- und Compliance-Management
- ❑ Rechtssichere Organisation
- ❑ Managementsysteme
- ❑ u.vm.

Leistungen:

- ❑ Auditierung/Zertifizierung von **Integrierten Managementsystemen** (z. B. QM / Risk / Compliance/ IKS)
  und **einzelner Komponenten** (z. B. einzelne Prozesse)
- ❑ Auditierung/Zertifizierung von **Qualitäts-Managementsystem** mit Risk und Compliance
- ❑ Auditierung/Zertifizierung von **Risiko-Managementsystem**
- ❑ Auditierung/Zertifizierung **Internes Kontrollsystem**
- ❑ Auditierung/Zertifizierung von **Compliance-Managementsystem**[1]
- ❑ Auditierung/Zertifizierung **Internes Revisionssystem**
- ❑ Auditierung/Zertifizierung **von weiteren Managementsystemen (IT-Sicherheit / Datenschutz / Nachhaltigkeit / Arbeitsschutz- und Gesundheit / Personalmanagement / etc.)**
- ❑ **Personen-Zertifizierung** im Bereich Governance, Risk, Compliance, IKS, Revision, etc. (Beauftragte / Auditoren / Revisoren)

1 Über Kooperationspartner ComZert

Lösungen: Win / win für Manager und Versicherer bei *zertifizierten* Managementsystemen

- **Versicherungs-Check für Manager**

- D&O (Managerhaftung)
- Strafrechtsschutz
- Vermögensschadenshaftpflicht
- etc.

Ein Beispiel von mehreren Bausteinen/Komponenten:

8. Wer arbeitet noch im Zeitalter der Digitalisierung und was sind die Anforderungen?

- **Roboter**
- **IT / Algorythmen**
- **Menschen!**

Wichtig:

Beachtung der Anforderungen von Recht (Compliance), Technik, BWL, Psychologie, etc.!

Worin sehen Sie die größten Herausforderungen der Zukunft

- für Ihr Unternehmen und für sich persönlich als Führungskraft?

_____

_____

_____

Lösungen:

❑ IT-Tools

- **Digitalisierte Prozesse**
- **Managementsystem-Tools**
- **Einzelne IT-basierte Komponenten**, wie

  - Richtlinienmanagement
  - e-learning-Programme
  - und vieles mehr

  helfen, die Datenflut zu bewältigen und effizient die Ziele zu erreichen.

  Analoge Bewältigung der Organisations- und Dokumentationsanforderungen ist allmählich nicht mehr „anerkannter Stand“.

Lösungen:

❑ Schulungen / Coaching / Consulting

Das neue, digitale Zeitalter und komplexere Anforderungen an Unternehmer und Mitarbeiter setzen entsprechende **Kompetenzen** voraus.

Die **Inhalte** von Schulungen und Beratung **müssen sich dem Fachkräftemangel und den neuen Gegebenheiten anpassen**.

Die erfordert neue Ansätze.

Lassen Sie regelmäßig die Versicherungssituation für Ihr Unternehmen und für sich selbst als Unternehmer kompetent überprüfen?

- ❑ Ja
- ❑ Nein

Sind die Bedingungen Ihres Manager-Versicherungspakets so ausgestellt, dass Sie bestmöglich vor persönlicher Regressierung geschützt sind?

- ❑ Ja
- ❑ Nein

Konnten Sie bei Verhandlungen mit

- **Kreditgebern**
- **Versicherern**

bessere Ergebnisse erzielen, weil Sie die Chancen des Unternehmens dargestellt und kommuniziert haben, dass Sie die Risiken im Unternehmen kennen und beherrschen?

❑ Ja

❑ Nein

Hinweis:
Sogar die besten Versicherungen sind nur ein *zusätzlicher Schutz* zu einer sicheren Organisation. **Flankierend** zur Versicherung sollten schon mal vorab Satzung, Geschäftsordnung, Verträge, Stellenbeschreibung und Entscheidungs- und Organisationsstruktur **für die Geschäftsleitung haftungsreduzierend** ausgestellt sein.

Wir helfen Ihnen, fit für Gegenwart und Zukunft zu sein!

Prof. Dr. Josef Scherer

Rechtsanwalt,
Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement,
Richter am Landgericht a. D.,
Gründer und Leiter des Internationalen Instituts für Governance, Management, Risk & Compliance (GMRC)
der Technischen Hochschule Deggendorf

Kontakt und weitere Informationen:

E-Mail: josef.scherer@th-deg.de
www.gmrc.de

Hinweis: Soweit die Quellen nicht gesondert angegeben sind, sind die Inhalte dieser Broschüre dem wesentlich ausführlicherem Werk
***Scherer/Fruth* (Hrsg.), Integriertes Kombi-Managementsystem on demand – Ziele-, Organisations-, Umsetzungs- sowie Steuerungs- und Überwachungsmanagement, 1. Auflage 2017, entnommen.**

Kontakt und weitere Informationen:

Internationales Institut für Governance, Management, Risk & Compliance (GMRC)

Institutsleitung
Prof. Dr. Josef Scherer

E-Mail: josef.scherer@th-deg.de

Impressum:
„Das Richtige richtig tun!“

... ist gar nicht schwer.

**Empirische Erhebung,
Gebrauchsanweisung und
Quick-Check-GRC
(Unternehmensführung)
in wenigen Minuten !**

Prof. Dr. Josef Scherer
c/o Internationales Institut für Governance, Management,
Risk- und Compliancemanagement der
Technischen Hochschule Deggendorf
Dieter-Görlitz-Platz 1
94469 Deggendorf

Deggendorf 2017

Vielen Dank
für Ihre Aufmerksamkeit!

Weitere Fragen – später mal?

Josef.scherer@th-deg.de