Sonderdruck aus *Scherer / Fruth* (Hrsg.),
Integriertes Personal-Managementsystem mit Governance, Risk & Compliance, 2017

Business Partner Screening –

Überwachungspflichten bei Delegation von Aufgaben auf Externe: Organisationspflichten versus „Scheinselbstständigkeit“

05/2017

Prof. Dr. jur. Josef Scherer
Richter am Landgericht a.D.
Rechtsanwalt
Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht
Leiter des Internationalen Instituts für Governance, Management, Risk & Compliance der Technischen Hochschule Deggendorf

Wolfgang Jacobs
Rechtsanwalt
Kanzlei Prof. Dr. Scherer, Dr. Rieger und Partner m.b.B

Giacomo Pasini
Assistenz der Leitung des Internationalen Instituts für Governance, Management, Risk und Compliance der Technischen Hochschule Deggendorf

Fabian Ludacka
Lehrbeauftragter der Technischen Hochschule Deggendorf

Inhaltsverzeichnis

1. Einleitung *(Scherer / Jacobs)*

Eine „make or buy"-Analyse führt häufig zu einer Entscheidung für Auslagerung / Delegation von Aufgaben auf Externe.

In der arbeitsteiligen, globalen und vernetzten Welt werden sehr viele Leistungen, wie Lieferung von Material, Erstellung von Komponenten, aber auch Erbringung von sonstigen Leistungen, ausgelagert.

Bei der Betrachtung des Verhältnisses von Auftraggebern zu (externen) Auftragnehmern unter Compliance-Gesichtspunkten besteht insbesondere bezüglich des Themas „Scheinselbstständigkeit" das Problem, dass diverse Rechtsgebiete (Arbeitsrecht/Organisationsrecht, Deliktsrecht und dergleichen mehr), aber auch Wissenschaftsdisziplinen (Recht, Betriebswirtschaftslehre, et cetera) sich scheinbar widersprechen oder beim Rechtsanwender inkorrekte Ansichten auslösen.

So wird im Arbeits-, Steuer-, und Sozialversicherungsrecht sehr schnell von einer Arbeitnehmereigenschaft respektive von „Scheinselbstständigkeit" ausgegangen, wenn von „Aufsicht", „Weisungen" sowie von „Kontrolle" die Rede ist.

Negativ-Beispiele aus Ermittlungsverfahren:

(der Verfasser ist mit entsprechenden Themen **als Strafverteidiger oder auch als Compliance-Funktion** im Rahmen von **„internal investigations"** betraut):

*„[…] Aufgrund der **strengen Kontrolle** der Auftragnehmer liegt bei den Mitbeschuldigten […] Weisungsgebundenheit und Eingliederung in die betriebliche Organisation und damit Scheinselbstständigkeit vor […]."*

*„[…] Durch die **genauen Vorgaben des Auftraggebers bzgl. der zu verrichtenden** Tätigkeiten und deren Überwachung beim Auftragnehmer durch den Beschuldigten […] liegt Weisung und damit keine echte Selbstständigkeit des Beschuldigten […] bei Organisation und Durchführung der Tätigkeit durch den scheinselbstständigen Auftragnehmer vor […]."*

*„[…] dass sich insbesondere dann eine andere Beurteilung der Frage der Selbstständigkeit ergeben kann, wenn […] beispielsweise der Auftraggeber **die konkrete Ausgestaltung der Arbeitsleistung** bestimmt. […]"*

*„[…] Der […] umfangreiche Schriftverkehr zeigt ausdrücklich, dass die Beschuldigte […] keine arbeitgebertypischen Entscheidungen selbst trifft. Sie handelt ausschließlich **auf Anweisung** durch den Beschuldigten […]"*

Vgl. hierzu den seit 01.04.2017 in Kraft getretenen neuen § 611a BGB (BGBl. I 2017, S. 258): Diese Vorschrift soll die bisherigen Abgrenzungskriterien der Rechtsprechung des Bundesarbeitsgerichtes widerspiegeln:

§ 611a Arbeitsvertrag

(1) 1Durch den Arbeitsvertrag wird der Arbeitnehmer im Dienste eines anderen zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet. 2Das Weisungsrecht kann Inhalt, Durchführung, Zeit und Ort der Tätigkeit betreffen. 3Weisungsgebunden ist, wer nicht im Wesentlichen frei seine Tätigkeit gestalten und seine Arbeitszeit bestimmen kann. 4Der Grad der persönlichen Abhängigkeit hängt dabei auch von der Eigenart der jeweiligen Tätigkeit ab. 5Für die Feststellung, ob ein Arbeitsvertrag vorliegt, ist eine Gesamtbetrachtung aller Umstände vorzunehmen. 6Zeigt die tatsächliche Durchführung

des Vertragsverhältnisses, dass es sich um ein Arbeitsverhältnis handelt, kommt es auf die Bezeichnung im Vertrag nicht an.

(2) Der Arbeitgeber ist zur Zahlung der vereinbarten Vergütung verpflichtet.

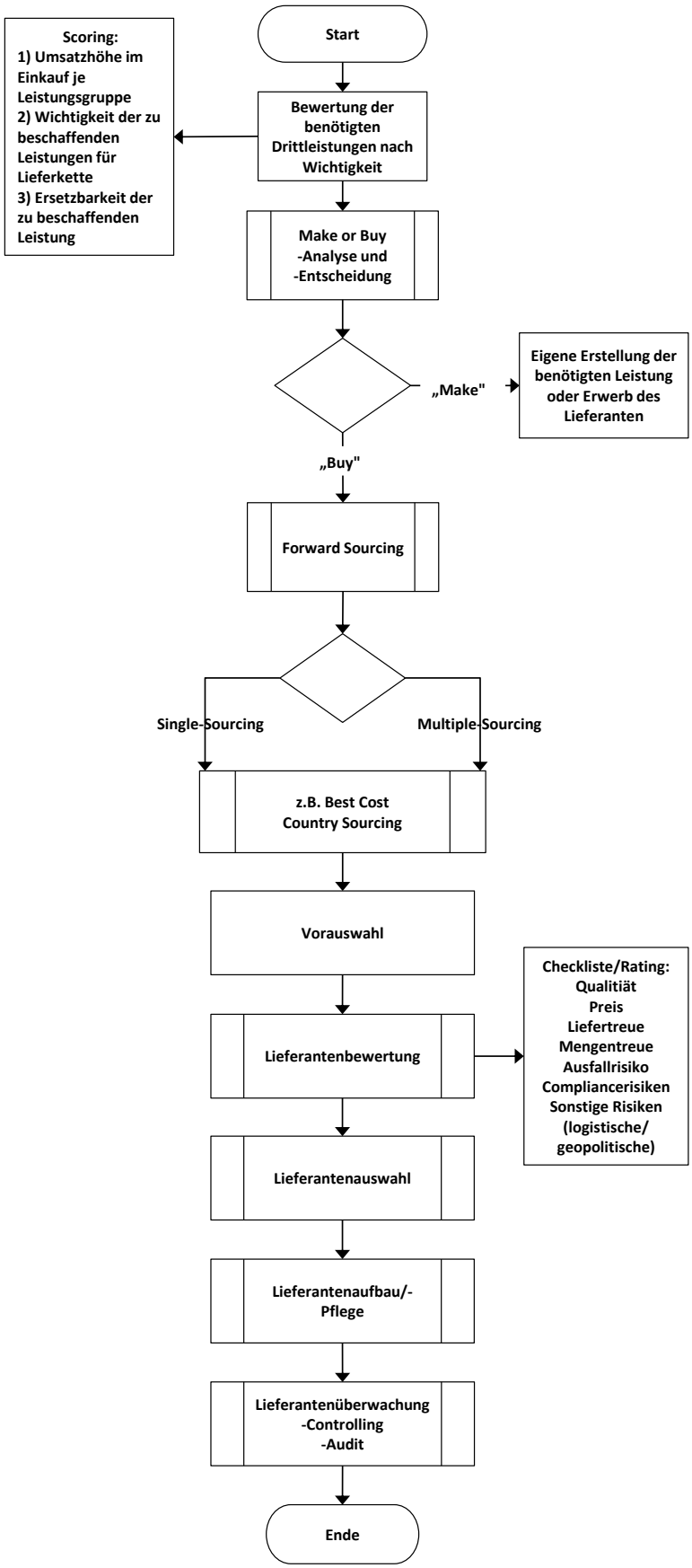
Folgende Kriterien können als Abgrenzungshilfe dienen: [1]

- persönliche, nicht nur wirtschaftliche Abhängigkeit;
- Weisungsgebundenheit hinsichtlich Ort, Zeit, Dauer und Inhalt der Tätigkeit, Bindung an feste Arbeitszeiten/Kernzeiten und an einen festen Arbeitsplatz;
- Eingliederung in die betriebliche Organisation, z. B. Aufnahme in Organigramm, Telefonverzeichnis, Email-Verteiler, gestellte Email-Adresse;
- identische Tätigkeit wie andere Arbeitnehmer;
- Tätigkeit nur für einen Auftraggeber;
- keine eigene Betriebsstätte, keine eigenen Mitarbeiter, kein Recht, eigene Mitarbeiter zur Vertragserfüllung einzusetzen;
- keine nennenswerte Selbstständigkeit in Organisation und Durchführung der Tätigkeit;
- Schulden der eigenen Arbeitskraft, nicht eines Arbeitserfolges;
- kein eigenes Unternehmerrisiko, kein Kapitaleinsatz, keine Pflicht zur Beschaffung von wesentlichen Arbeitsmitteln;
- Ausführung von einfachen bzw. untergeordneten Tätigkeiten, die üblicherweise von Arbeitnehmern ausgeführt werden und bei denen eine Weisungsgebundenheit die Regel ist;
- Erhalt typischer Arbeitgeberleistungen wie festes oder konstant gleiches Gehalt/Honorar, Überstundenvergütung, Urlaubsanspruch, Entgeltfortzahlung im Krankheitsfall etc.

Die anderen Disziplinen (Organisationsrecht/Betriebswirtschaftslehre/etc.) verlangen dagegen gerade gegenüber externen Delegationsempfängern erhöhte Anstrengungen des Delegierenden hinsichtlich der Überwachung und der Erteilung von Weisungen.[2]

Der „Idealprozess" für Beschaffung nach Anforderungen von Gesetz und Rechtsprechung, nach „Anerkanntem Stand von Wissenschaft und Praxis“, sowie den einschlägigen Standards wird hier vorab dargestellt und könnte etwa wie folgt aussehen:[3]

[1] Nach *Unnuß/Dworschak/Scheele*, Corporate Compliance Checklisten, 2. Auflage 2012, Rn. 147.
[2] Vergleiche auch ergänzend die Ausführungen in Scherer/Fruth (Hrsg.), Geschäftsführer-Compliance 2009, „Organisationspflicht der Geschäftsleitung“ (Rn. 23) sowie „Ordnungsgemäße Delegation und Überwachung durch Geschäftsleitung“ (Rn 26)
[3] Aus: *Scherer/Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk und Compliance (GRC), 1. Auflage 2016, Seite 192



Die folgenden Ausführungen stellen die genannten Disziplinen gegenüber, um letztlich in der Synthese scheinbare Widersprüche transparent zu machen oder – wo möglich – aufzulösen.

2. Gesetzliche Regelungen

2.1 § 831 BGB

§ 831 Haftung für den Verrichtungsgehilfen

(1) 1Wer einen anderen zu einer Verrichtung bestellt, ist zum Ersatz des Schadens verpflichtet, den der andere in Ausführung der Verrichtung einem Dritten widerrechtlich zufügt. 2Die Ersatzpflicht tritt nicht ein, wenn der Geschäftsherr bei der Auswahl der bestellten Person und, sofern er Vorrichtungen oder Gerätschaften zu beschaffen oder die Ausführung der Verrichtung zu leiten hat, bei der Beschaf-fung oder der Leitung die im Verkehr erforderliche Sorgfalt beobachtet oder wenn der Schaden auch bei Anwendung dieser Sorgfalt entstanden sein würde.

(2) Die gleiche Verantwortlichkeit trifft denjenigen, welcher für den Geschäftsherrn die Besorgung eines der im Absatz 1 Satz 2 bezeichneten Geschäfte durch Vertrag übernimmt.

*„Obwohl das Gesetz vom Wortlaut her nur auf die Auswahl des Gehilfen abstellt (…) und die Leitung der Ausführung nur bei der Beschaffung von Gerätschaften und Vorrichtungen durch den Geschäftsherrn erwähnt, besteht Einigkeit darüber, dass den Geschäftsherrn generell auch **Pflichten zur sorgfältigen Überwachung und Leitung** treffen."*[4]

*„Allerdings ist in § 831 Abs. 1 S. 2 nirgends von einer **Verpflichtung des Geschäftsherrn zur Überwachung des Gehilfen** die Rede, wie sie heute **neben den Pflichten zur Auswahl und zur Anleitung als dritte Dimension der Sorgfaltspflichten** des Prinzipals anerkannt ist."*[5]

*„Gerade wegen der beschränkten Möglichkeiten der Auswahlprüfung ist die Verpflichtung des Arbeitgebers zur **Überwachung des Gehilfen von großer praktischer Bedeutung**. Überwachungsmaßnahmen sind bei Beschäftigten, die ihre Arbeit in der Betriebsstätte des Prinzipals verrichten, häufig auch kostengünstig durchzuführen. Insbesondere lässt sich schon durch **Maßnahmen der Qualitätskontrolle** verhindern, dass ein Gehilfenversagen zu Schäden an den Rechtsgütern externer Dritter führt. Soweit dies geschieht, werden die im Rahmen des § 831 Abs. 1 S. 2 vorausgesetzten Sorgfaltspflichten gleichsam en passant mit erfüllt. Die Gerichte haben sich mit der Frage möglicher und ausreichender Überwachungsmaßnahmen deshalb vor allem mit Blick auf solche Gehilfen zu befassen, die außerhalb des Betriebsgeländes arbeiten, wobei wiederum die Kraftfahrer die mit Abstand bedeutsamste Fallgruppe ausmachen."*[6]

Kommt der Prinzipal diesen Überwachungspflichten nicht nach, so ist ihm im Schadensfall eine denkbare Exkulpation verwehrt: § 831 Abs. 1 Satz 1 BGB statuiert eine Verschuldensvermutung, die vom Unternehmen zu widerlegen ist.

[4] Zitat nach BeckOK BGB/*Spindler* BGB § 831 Rn. 28 (Fettdruck durch die Verfasser):
[5] Zitat nach MüKoBGB/*Wagner* BGB § 831 Rn. 34
[6] Zitat nach MüKoBGB/*Wagner* BGB § 831 Rn. 39

Die Folge ist eine – aus Compliance-Gesichtspunkten zu vermeidende – Haftung.

Es ist noch klarzustellen, dass selbstständige Delegationsempfänger aufgrund ihrer Selbstständigkeit zwar nicht als Verrichtungsgehilfen im Sinne des § 831 BGB angesehen werden.[7]

Gleichwohl finden die Grundsätze der Haftung des Unternehmers bei Delegationen auch oder erst Recht bei Einschaltung Selbstständiger Anwendung.
Mittlerweile ist es im Rahmen der Anforderungen an die ordnungsgemäße Organisation und an die Compliance eines Unternehmens jedenfalls unabdingbar, **bei einer Einschaltung externer, selbstständiger Leistungserbringer** (sei es im Wege des Outsourcing klassischer Unternehmensaufgaben, sei es für den Bereich der Zulieferer als „gewöhnliche" Vertragspartner) diese **sorgfältig auszuwählen, zu instruieren und zu überwachen.**

2.2 § 823 BGB

§ 823 Schadensersatzpflicht
(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) 1Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckenden Gesetzes verstößt. 2Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

Besonders relevant im Zusammenhang mit dem hier behandelten Untersuchungsgegenstand dürfte die Übertragung von Verkehrssicherungspflichten, die im Rahmen des § 823 BGB bestehen, auf Dritte sein. Auch dabei sind Überwachungspflichten immanent.

Hierzu schreibt *Förster*:[8]
*„Die dem Übertragenden verbleibende Verkehrssicherungspflicht „verengt" sich auf die Auswahl eines geeigneten Kandidaten für die Übernahme und **dessen anschließende Überwachung** (BGH NJW 2006, 3628 Rn. 11); (…). Der Auswahl der „richtigen" Person kommt insofern besondere Bedeutung zu, dass damit die entscheidende Weiche für die sorgfältige Ausführung der übertragenen Verkehrssicherungspflichten und damit zugleich für den Umfang der anschließend notwendigen Überwachung gestellt wird: Je besser die Auswahl, desto geringer wird regelmäßig die nachfolgende Überwachung sein müssen. Eine schlechte Wahl **hingegen bedarf einer entsprechend intensiveren Überwachung**, um ggf. Fehler noch korrigieren zu können – falls der Übertragende die dazu notwendigen Einwirkungsmöglichkeiten besitzt. (…) **Die Aufsicht über den einmal Ausgewählten besteht allgemein in einer fortlaufenden Überwachungstätigkeit** (BGH NJW 1972, 1321 [1322 f.]), **die dem Übertragenden ermöglicht, die sorgfältige Erfüllung der von ihm verlagerten Verkehrssicherungspflicht durch den Übernehmer sicherzustellen und notfalls selbst rechtzeitig eingreifen zu können."***

Sofern also (auch) Verkehrssicherungspflichten übertragen werden – wie beispielsweise die Einhaltung von Sicherheitsanforderungen zur Vermeidung der Gefahr für Leib und Leben im Rahmen der extern erbrachten Leistungen - ist dabei auch eine intensive Überwachung selbstständig Tätigen zwingend nötig, um eigene Haftungsrisiken zu vermindern.

[7] Vgl. *Schulze-Ansgar* in Staudinger, Bürgerliches Gesetzbuch, 9. Auflage 2017, § 831 Rn. 7.
[8] Bamberger/Roth-*Förster,* Beck'scher Online-Kommentar BGB, 41. Edition, Stand: 01.11.2016 zu § 823 Rn 357 – 361 (Fettdruck durch Verfasser)

Eine solche *Überwachung* würde in der Praxis sozialversicherungs- /straf- /arbeitsrechtlichen Praxis gelegentlich jedoch wiederum – fälschlicherweise (!) bei verkürzter Betrachtung – als Indiz für ein angebliches „Weisungsverhältnis“ und „Eingliederung in die betriebliche Organisation“ gesehen werden können, was eine inkorrekte rechtliche Beurteilung darstellen würde.

Ähnliches gilt auch für den Bereich der aus § 823 Abs. 1 BGB abgeleiteten Produkthaftung: Besonders relevant erscheint in diesem Zusammenhang die Haftung für Fabrikationsfehler („Ausreißer“). Grundsätzlich haftet ein Hersteller für solche Fabrikationsfehler seines Zulieferers dann nicht, wenn der Fehler (für den Hersteller) trotz aller zumutbaren Vorkehrungen unvermeidbar war.

„Die Darlegungs- und Beweislast hierfür trägt der Hersteller. Er kann den Entlastungsbeweis dadurch führen, dass er nachweist, dass er den Zulieferer ordnungsgemäß ausgewählt und dabei den ***Produktionsprozess überprüft, überwacht und sichergestellt hat, dass eine Zertifizierung des Bauteils vorliegt, und ein anerkanntes Qualitätssicherungssystem bei der Eingangskontrolle eingeführt hat****.“*[9]

In speziellen ***branchenspezifischen Regelungen****, z. B. im Bereich der „Herstellung“ von Lebensmitteln bestehen weitere und noch tiefgreifendere Überwachungspflichten für den Hersteller.*

Diese ergeben sich sowohl

(1) aus den europarechtlichen bzw. nationalen Vorgaben, wie beispielsweise der EG-Hygieneverordnung VO (EG) Nr. 852/2004 oder der Lebensmittel-Informationsverordnung VO (EU) Nr. 1169/2011 sowie zahlreicher weiterer Verordnungen sowie

(2) aus nationalen Regelungen (Lebensmittel-, Bedarfsgegenstände- und Futtermittelgesetzbuch“ - LFGB)

(3) als auch aus der u. U. vertraglich mit Kunden oder Zertifizierer eingegangenen Verpflichtung zur Erfüllung von Standards gemäß branchenüblicher Siegel, Zertifikate und Vorgehensweisen (z.B. IFS Food, Global G.A.P., HACCP - Hazard Analysis and Critical Control Points, etc…).

[9] Zitat aus Geigel-*Wellner*, Haftpflichtprozess, 27. Auflage 2015, 14. Kapitel. Anwendungsfälle des § 823 Abs. 1 BGB, Rn. 274 (Fettdruck durch die Verfasser).

2.3 § 130 OWiG iVm. § 30 OWiG

§ 130 [Verletzung der Aufsichtspflicht in Betrieben und Unternehmen]

(1) 1Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichts-maßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehö-rige Aufsicht verhindert oder wesentlich erschwert worden wäre. 2Zu den erforderlichen Aufsichtsmaß-nahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.

(2) Betrieb oder Unternehmen im Sinne des Absatzes 1 ist auch das öffentliche Unternehmen.

(3) 1Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. 2§ 30 Absatz 2 Satz 3 ist anzuwenden. 3Ist die Pflichtverlet-zung mit Geldbuße bedroht, so bestimmt sich das Höchstmaß der Geldbuße wegen der Aufsichtspflicht-verletzung nach dem für die Pflichtverletzung angedrohten Höchstmaß der Geldbuße. 4Satz 3 gilt auch im Falle einer Pflichtverletzung, die gleichzeitig mit Strafe und Geldbuße bedroht ist, wenn das für die Pflichtverletzung angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.

§ 30 OWiG bestimmt sodann die Voraussetzungen, unter denen eine Geldbuße verhängt werden kann.

„Schon wegen der erheblichen Bußgelddrohung gegen das Unternehmen hat dieses ein evidentes und massives Interesse daran, dass die erforderlichen Aufsichtsmaßnahmen durchgeführt werden."[10]

Die Pflichten aus § 130 OWiG umfassen damit auch die Sorge für ordnungsgemäße Leistungserbringung durch *externe* Delegationsempfänger. Dies wiederum ist nur durch entsprechende organisatorische Maßnahmen (z.B. „Know your supplier", etc.) sicherzustellen.

2.4 § 278 BGB, § 31 BGB, § 428 HGB

§ 278 S. 1 BGB:

Der Schuldner hat ein Verschulden seines gesetzlichen Vertreters und der Personen, deren er sich zur Erfüllung seiner Verbindlichkeit bedient, in gleichem Umfang zu vertreten wie eigenes Verschulden.

§ 31 BGB:

Der Verein ist für den Schaden verantwortlich, den der Vorstand, ein Mitglied des Vorstands oder ein anderer verfassungsmäßig berufener Vertreter durch eine in Ausführung der ihm zustehenden Verrichtungen begangene, zum Schadensersatz verpflichtende Handlung einem Dritten zufügt.

[10] Hauschka/Moosmayer/Lösler-*Pelz*, Corporate Compliance, 3. Auflage 2016, § 5. Strafrechtliche und zivilrechtliche Aufsichtspflicht, Rn. 3

§ 428 HGB:

Der Frachtführer hat Handlungen und Unterlassungen seiner Leute in gleichem Umfange zu vertreten wie eigene Handlungen und Unterlassungen, wenn die Leute in Ausübung ihrer Verrichtungen handeln. Gleiches gilt für Handlungen und Unterlassungen anderer Personen, deren er sich bei Ausführung der Beförderung bedient.

Diese Normen (§ 278 BGB/§ 428 HGB) differenzieren bei Delegationen nicht zwischen Selbstständigen und Nichtselbstständigen.

Die Quintessenz und der Grundgedanke der in § 278 BGB, § 31 BGB sowie § 428 HGB zu findenden Regelungen lässt sich also – vereinfacht – zusammenfassen: „Es besteht grundsätzlich die Möglichkeit einer Haftung, falls Dritte eingesetzt werden, da fremdes Verschulden zugerechnet wird."

*„Auch **selbständige Unternehmer können Erfüllungsgehilfen** sein, (...). Dies ist anders als bei § 831, hieran zeigt sich auch ein wichtiger Unterschied zwischen beiden Regelungen: **Soll der Vertragspartner optimal gewählt werden können, muss ihm grundsätzlich die Verlagerung der Erfüllung auf andere zugerechnet werden, auch auf Selbständige, die der Gläubiger nicht gewählt hat.**"*[11]

Denklogisch ergibt sich wiederum aus diesem Haftungsrisiko heraus die Notwendigkeit, entsprechend eingesetzte Dritte – egal ob selbstständige Unternehmer oder angestellte Arbeitnehmer – intensiv zu überwachen. Nur so kann der Unternehmer wirksam Regressansprüche vermeiden.

2.5 § 32 VAG (Versicherungsbranche)

Die Pflicht zur Überwachung externer, selbstständiger Leistungserbringer („Ausgliederung") ist mittlerweile nicht mehr nur in der Rechtsprechung, sondern auch in der Gesetzgebung als zwingende Organisationspflicht verankert, beispielsweise in § 32 VAG:[12]

(1) Ein (…)unternehmen, das Funktionen oder (…)tätigkeiten ausgliedert, bleibt für die Erfüllung aller aufsichtsrechtlichen Vorschriften und Anforderungen verantwortlich.

(2) 1Durch die Ausgliederung dürfen die ordnungsgemäße Ausführung der ausgegliederten Funktionen und (…)tätigkeiten, die Steuerungs- und Kontrollmöglichkeiten des Vorstands sowie die Prüfungs- und Kontrollrechte der Aufsichtsbehörde nicht beeinträchtigt werden. 2Insbesondere hat das ausgliedernde Unternehmen hinsichtlich der von der Ausgliederung betroffenen Funktionen und (…)tätigkeiten sicherzustellen, dass

1. ***das Unternehmen selbst, seine Abschlussprüfer** und die Aufsichtsbehörde **auf alle Daten zugreifen können,***
2. *der Dienstleister mit der Aufsichtsbehörde zusammenarbeitet und*
3. *die Aufsichtsbehörde **Zugangsrechte zu den Räumen des Dienstleisters** erhält, die sie selbst oder durch Dritte ausüben kann.*

[11] Münchener Kommentar zum BGB-*Grundmann*, 7. Auflage 2016, § 278 Rn. 45 (Fettdruck durch Verfasser)
[12] Vgl. hierzu *Scherer / Fruth (Hrsg.),* Anlagenteil zu Governancemanagement Band II 2016, S. 242 ff.

*(3) **Bei der Ausgliederung** wichtiger Funktionen und (…)tätigkeiten haben (…)unternehmen außerdem sicherzustellen, dass **wesentliche Beeinträchtigungen der Qualität der Geschäftsorganisation, eine übermäßige Steigerung des operationellen Risikos sowie eine Gefährdung der kontinuierlichen und zufriedenstellenden Dienstleistung (…)vermieden werden**.*

*(4) 1Das ausgliedernde (…)unternehmen hat **sich die erforderlichen Auskunfts- und Weisungsrechte vertraglich zu sichern** und die ausgegliederten Funktionen und (…)tätigkeiten in sein Risikomanagement einzubeziehen (…)*

2.6 § 25a KWG

§ 25a [1] Besondere organisatorische Pflichten; Verordnungsermächtigung

*(1) [1]Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. [2]Die Geschäftsleiter sind für die ordnungsgemäße Geschäftsorganisation des Instituts verantwortlich; sie haben die erforderlichen Maßnahmen für die Ausarbeitung der entsprechenden institutsinternen Vorgaben zu ergreifen, sofern nicht das Verwaltungs- oder Aufsichtsorgan entscheidet. **[3]Eine ordnungsgemäße Geschäftsorganisation** muss insbesondere ein **angemessenes und wirksames Risikomanagement** umfassen, auf dessen Basis ein Institut die Risikotragfähigkeit laufend sicherzustellen hat; das Risikomanagement umfasst insbesondere (…)*
. die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer Internen Revision, wobei das interne Kontrollsystem insbesondere
a) aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche, (…)

2.7 Primärzuständigkeit, Delegationsbefugnis, Anforderungen an Delegation und Letztverantwortlichkeit des Geschäftsführers

Grundsätzlich und primär zuständig für die Einhaltung aller Pflichten, die ein Unternehmen treffen, ist die Geschäftsleitung, die dabei entsprechend hohe Sorgfalt aufwenden muss, vgl. etwa § 43 GmbHG, § 93 AktG u.v.m.

„I. Allzuständigkeit, Gesamtzuständigkeit, Gesamtverantwortung
Nach den Vorstellungen des Gesetzgebers ist der Vorstand einer Aktiengesellschaft bzw. der Geschäftsführer einer GmbH für alle Angelegenheiten der Gesellschaft, insbesondere für die Erledigung sämtlicher Geschäfte zuständig, die der Betrieb des Unternehmens der Gesellschaft mit sich bringt (Grundsatz der Allzuständigkeit). Besteht der Vorstand bzw. die Geschäftsführung aus mehreren Personen, so sind sie gemeinschaftlich, als Kollegium, zuständig; ihre Pflichten als Organwalter bestehen nebeneinander und sind parallel zu erfüllen (Grundsatz der Gesamtzuständigkeit). Für die Erfüllung dieser Pflichten sind sie gemeinsam verantwortlich und haften der Gesellschaft solidarisch als Gesamtschuldner (Grundsatz der Gesamtverantwortung).“[13]

[13] Hauschka/Moosmayer/Lösler-*Schmidt-Husson*, Corporate Compliance, 3. Auflage

Damit diese umfassende Verantwortung nicht allein „auf den Schultern" der Geschäftsleitung verbleibt, hat diese die Befugnis zur Delegation:

„Ordnungsgemäße Delegation und Überwachung durch Geschäftsleitung
Aufgaben der Unternehmensleitung können delegiert werden, wobei im Falle ordnungsgemäßen Vorgehens hier eine Haftungsreduzierung zu Gunsten des Delegierenden erreicht werden kann. Voraussetzung ist, dass die Delegation den Anforderungen der Rechtsprechung genügt. Darüber hinaus hat der Delegierende weiterhin seiner Aufsichtspflicht nachzukommen, was zumindest zu stichprobenartiger Kontrolle der Erfüllung der delegierten Aufgaben verpflichtet."[14]

Die Anforderungen an eine rechtssichere Delegation können dabei wie folgt zusammengefasst werden:
„Sie bestehen in der Auswahl von geeigneten Delegationsempfängern, in einer entsprechenden Instruk-tion und einer Überwachung, dass die Leistungen der Delegationsempfänger die Anforderungen:
Effektivität, Sicherheit, Rechtssicherheit, Qualität, Termintreue, etc. erfüllen."[15]
Zuletzt verbleibt es jedoch stets bei der Gesamtverantwortung bzw. Letztverantwortung der Geschäftsleitung:[16]

„1. Gesamtverantwortung undelegierbar
Anders als die Grundsätze der All- und Gesamtzuständigkeit steht der Grundsatz der Gesamtverantwortung nicht zur Disposition der Beteiligten. (…) In diesem Sinne ist die Gesamtverantwortung von Vorständen und Geschäftsführern unentrinnbar. Beeinflussen können die Mitglieder von Leitungsorganen allenfalls, ob und wie sie Aufgaben delegieren. Wenn sie sich dabei an die ihnen ebenfalls vorgegebenen Sollenssätze ordnungsgemäßen Delegierens halten, entrinnen sie den Haftungsfolgen, die das Recht an fehlerhafte Delegation knüpft und in denen sich der Grundsatz der Gesamtverantwortung manifestiert."

[14] Vgl. dazu *Scherer/Fruth* (Hrsg.)-*Scherer*, Geschäftsführer-Compliance, 1. Auflage 2009, Rn. 26
[15] *Scherer/Fruth (Hrsg.) „Integriertes Compliance-Management mit GRC", 2. Auflage, 2017, 1.2.5. Tools und Methoden* sowie noch detaillierter: Hauschka/Moosmayer/Lösler-*Schmidt-Husson*, Corporate Compliance, 3. Auflage 2016, § 6. Delegation von Organpflichten, Rn 6-9
[16] So auch Hauschka/Moosmayer/Lösler-*Schmidt-Husson*, Corporate Compliance, 3. Auflage 2016, § 6. Delegation von Organpflichten, Rn 10

2.8 Europarechtliche Tendenzen

2.8.1 Datenschutz-Grundverordnung ab 05/2018: Art. 28 DSGVO: Auftragsdatenverarbeitung (ADV)

Art. 28 DSGVO Auftragsverarbeiter

1. *Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen,* ***so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt*** *und den Schutz der Rechte der betroffenen Person gewährleistet.*

2. *[…]*

3. *Die Verarbeitung durch einen Auftragsverarbeiter erfolgt* ***auf der Grundlage eines Vertrags*** *[…] der […]* ***den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag*** *bzw. dieses andere Rechtsinstrument* ***sieht insbesondere vor, dass der Auftragsverarbeiter***

    1. ***die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen […] verarbeitet […]***

    8. ***dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. […]***

2.8.2 Neuregelung in Frankreich: Art. 17 des Gesetzes zur Transparenzsteigerung und Korruptionsbekämpfung

In dem am 10. Dezember 2016 veröffentlichten Gesetz, welches ab 01.06.2017 in Kraft tritt *(„LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique")*, ist in Art. 17 eine ausführliche Liste der Anti-Korruptions-Maßnahmen und –Verfahren vorgesehen, die die unter den Anwendungsbereich des Gesetzes fallenden Unternehmen umsetzen müssen.

Danach ist unter anderem – sinngemäß – ein Prozess vorzusehen, durch den die Risikolage hinsichtlich Compliance bei den Kunden, wichtigen Zulieferern und Zwischenhändlern dargestellt wird.

Das Gesetz fordert also die Überprüfung des Compliance-Standes der Geschäftspartner.

Unverkennbar ist hierbei wiederum denklogische Voraussetzung, dass weitreichende Informationen über die Geschäftspartner bzw. die „Leistungserbringer" eingeholt und abgeprüft werden und auch deren interne Organisationsstrukturen und Prozesse sowie deren Zahlungsströme „durchleuchtet" werden – europaweit.

Dies stellt also – vermutlich erstmals – eine allgemein / branchenübergreifend geltende, gesetzlich vorgeschriebene, weitreichende „Überwachungspflicht" von Vertragspartnern dar. Damit wird deutlich die Richtung aufgezeigt, in der die bereits begonnene Entwicklung dieser Überwachungspflichten als Teil einer rechtssicheren Organisation voranschreitet.

Gleichzeitig fehlt jedoch – bislang - noch die Anpassung, Klarstellung in Normen und der Rechtsprechung im Bereich des Themas Scheinselbstständigkeit, die den Aspekt der „Überwachung" als einen wesentlichen Anknüpfungspunkt für die Beurteilung des Vorliegens von „Scheinselbstständigkeit" heranziehen, dass alles, was zu einer ordnungsgemäßen Delegation / Überwachung gehört, nicht als Indiz für eine „Scheinselbstständigkeit" herangezogen werden darf.

2.8.3 Neuregelungen in Spanien

Auch in Spanien werden jüngst sehr strenge Compliance-Standards und Gesetze umgesetzt, die insbesondere auch die Kontroll- und Überwachungspflichten gegenüber externen Delegationsempfängern besonders hervorheben.

3. Anerkannter Stand von Wissenschaft und Praxis

"Business Partner Screening / Know your Supplier": Definition

Der Begriff des „Business Partner Screening" ist u.a. auch dem Bereich der „Einkaufs-Compliance" zuzuordnen, ebenso die „Know your supplier"-Themen. Bei der Beschaffung bzw. Bereitstellung von Prozessen, Leistungen oder Produkten von dritter Seite sind besondere Maßnahmen zu ergreifen:

*„Je nach Relevanz und **Risikobewertungsergebnis** bzgl. **ausgegliederter Leistungen** sind unterschiedliche Anforderungen zu erfüllen und Maßnahmen zu ergreifen. Eine der ersten Maßnahmen, die sich erst seit Kurzem*

*in den moderneren Unternehmen etabliert, ist das **„Business-Partner-Screening“**, bei dem der externe Leistungserbringer einem Rating/Audit unterzogen wird: Er wird also bezüglich Qualität, Service, Liefertreue, Preis, Ausfallsicherheit, Compliance, Risikomanagement, Nachhaltigkeit, u.v.m. genauestens untersucht, zum Teil mittels „**Lieferantenaudits**“ oder der **Einforderung diverser Zertifikate**.“* [17]

Grützner/Jako schreiben zu „Business Partner Screening (BPS)“: [18]

***„Das „Business Partner Screening“ (BPS) umfasst i. d. R. die systematische und risikoorientierte Analyse von Geschäftspartnern insbesondere hinsichtlich ihrer Integrität und Zuverlässigkeit.** Dabei kommt dem BPS insbesondere im Bereich der Lieferantenauswahl, der Zusammenarbeit mit Vertriebspartnern sowie im Rahmen von → Mergers & Aquisitions für eine wirksame → Korruptionsprävention und die damit verbundene Vermeidung von → Reputationsrisiken eine zunehmende Bedeutung zu. Das BPS wird oftmals in einem mehrstufigen, risikoorientierten Verfahren unter Mitwirkung von externen Experten durchgeführt.“*

und zu „Vendor Integrity Screening (VIS)“:

*„Als eine Form der → Korruptionsprävention werden im Rahmen eines „Vendor Integrity Screenings“ (VIS) **potentielle oder auch schon vorhandene Lieferanten im Hinblick auf ihre Integrität überprüft (→ Business Partner Screening). Dies erfolgt u. a. auf der Basis von Selbstauskünften, die je nach Risikoeinschätzung durch interne wie auch externe Hintergrundrecherchen sukzessive ergänzt werden sollten**.“*

Lösler-Herb [19] stellen fest:

*„Ein weiterer Aspekt ist im Rahmen der Sicherstellung von Compliance in der Einkaufsorganisation und dort insbesondere beim Thema „Dokumentation der Lieferantenauswahl“ zu beachten. Schließlich ist auch in diesem Rahmen ein Kriterium, **ob der auszuwählende Lieferant bereit ist, an (Lieferanten-)Audits oder Self Assessments teilzunehmen.“** [20]*

4. Hinweise in relevanten Standards

Standards orientieren sich in der Regel am sogenannten „Anerkannten Stand von Wissenschaft und Praxis“, der das Mindestmaß für ordnungs- und pflichtgemäßes Handeln darstellen kann.[21] Im Gegensatz zu Legalitätspflichten, welche per se gelten, sind die Vorgaben aus dem jeweiligen Standard u.a. dann verpflichtend, wenn

[17] Siehe dazu *Scherer* in *Scherer/Fruth* (Hrsg.) „Integriertes Compliance-Management mit GRC“, 2. Auflage, 2017
[18] Compliance von A-Z, 2. Auflage 2015
[19] Vgl. Hauschka/Moosmayer/Lösler-*Herb*, Corporate Compliance, 3. Auflage 2016, § 19. Compliance in der Einkaufsorganisation, Rn. 45 a.E
[20] Vgl. auch weiterführend: *Mössner, Kerner*: Praxisbeitrag: Einführung konzernweiter Standards für die Geschäftspartner-Prüfung, aus CCZ 2011, 182.
[21] Vgl. *Scherer/Fruth (Hrsg.)*, Governance-Management, Band 1, 2015, Kapitel 1.3: Der Einfluss von Standards und des Anerkannten Standes von Wissenschaft und Praxis auf die Organhaftung – am Beispiel der ISO 19600 (2014) Compliance-Managementsystem, S. 78 ff..

sich ein Unternehmen für seine Einführung -z. B. als interne verbindliche Vorgabe- entschieden oder vertraglich gegenüber Dritten (z. B. Kunden) verpflichtet hat.

Standards dienen Zertifizierungsstellen als Prüfungsgrundlage.

Es gibt eine Vielzahl von („Insel“-) „Managementsystemen“, die in unterschiedlichen Standards abgebildet sind.

Wenngleich die diversen Managementsysteme unterschiedliche Zielsetzungen verfolgen, können doch durchaus ähnliche Anforderungen festgestellt werden. Dies gilt vor allem im Zusammenhang mit „ausgelagerten Prozessen oder Dienstleistungen“.

Hier verlangen alle Standards, dass ausgelagerte Prozesse oder Dienstleistungen so überwacht werden **müssen**, dass die Konformität an Produkte und Leistungen sichergestellt wird.
Somit dient die Überwachung auch der Einhaltung der eigenen Complianceverpflichtungen.

4.1 ISO 9001:2015: Qualitätsmanagementsystem

Inhalt

8.4 Steuerung von extern bereitgestellten Prozessen, Produkten und Dienstleistungen

8.4.1 Allgemeines

*Die Organisation **muss sicherstellen, dass extern bereitgestellte Prozesse, Produkte und Dienstleistungen den Anforderungen entsprechen.***

*Die Organisation **muss Steuerungsmaßnahmen** bestimmen, die für extern bereitgestellte Prozesse, Produkte und Dienstleistungen durchzuführen sind, wenn:*

a) Produkte und Dienstleistungen von externen Anbietern für die Integration in die organisationseigenen Produkte und Dienstleistungen vorgesehen sind;

b) Produkte und Dienstleistungen den Kunden direkt durch externe Anbieter im Auftrag der Organisation bereitgestellt werden;

*Die Organisation **muss** Kriterien für die Beurteilung, Auswahl, Leistungsüberwachung und Neubeurteilung externer Anbieter bestimmen und anwenden, die auf deren Fähigkeit beruhen, Prozesse oder Produkte und Dienstleistungen in Übereinstimmung mit den Anforderungen bereitzustellen. Die Organisation **muss** dokumentierte Informationen zu diesen Tätigkeiten und über jegliche notwendigen Maßnahmen aus den Bewertungen aufbewahren.*

8.4.2 Art und Umfang der Steuerung

*Die Organisation **muss** sicherstellen, dass extern bereitgestellte Prozesse, Produkte und Dienstleistungen die Fähigkeit der Organisation, ihren Kunden beständig konforme Produkte und Dienstleistungen zu liefern, nicht nachteilig beeinflussen.*

*Die Organisation **muss**:*

*a) **sicherstellen, dass extern bereitgestellte Prozesse unter der Steuerung ihres Qualitätsmanagement-sytems verbleiben;***

b) sowohl die Maßnahmen zur Steuerung festlegen, die sie beabsichtigt für einen externen Anbieter anzuwenden, als auch die Maßnahmen zur Steuerung, die sie beabsichtigt für die Ergebnisse anzuwenden;

c) berücksichtigen:

1) die potentiellen Auswirkungen der extern bereitgestellten Prozesse, Produkte und Dienstleistungen auf die Fähigkeit der Organisation, beständig die Kundenanforderungen sowie zutreffende gesetzliche und behördliche Anforderungen zu erfüllen;

2) die Wirksamkeit der durch den externen Anbieter angewendeten Maßnahmen zur Steuerung;

d) die Verifizierung bzw. andere Tätigkeiten bestimmen, die notwendig sind, um sicherzustellen, dass die extern bereitgestellten Prozesse, Produkte und Dienstleistungen die Anforderungen erfüllen.

8.4.3 Informationen für externe Anbieter

*Die Organisation **muss** die Angemessenheit der Anforderungen vor deren Bekanntgabe gegenüber externen Anbietern sicherstellen.*

*Die Organisation **muss** den externen Anbietern ihre Anforderungen in Bezug auf Folgendes mitteilen:*

a) die bereitzustellenden Prozesse, Produkte und Dienstleistungen;

b) die Genehmigung von:

1) Produkten und Dienstleistungen;

2) Methoden, Prozessen und Ausrüstungen;

c) die Kompetenz, einschließlich jeglicher erforderlichen Qualifikation von Personen;

d) das Zusammenwirken des jeweiligen externen Anbieters mit der Organisation;

e) die Steuerung und Überwachung der Leistung des jeweiligen externen Anbieters, die von der Organisation eingesetzt werden;

f) die Verifizierungs- oder Validierungstätigkeiten, die die Organisation oder deren Kunde beabsichtigt, beim jeweiligen externen Anbieter durchzuführen.

Rechtliche Beurteilung

Sofern (global) **die herrschende Meinung in Wissenschaft und Praxis** diese Vorgaben (als wesentlicher Bestandteil der ISO 9001) **als bewährt anerkennt und sogar beachtet**, stellen diese Vorgaben den „Anerkannten Stand von Wissenschaft und Praxis" dar. Über die Herleitung, dass ein gewissenhafter Geschäftsführer (§ 43 GmbHG), Vorstand (§ 93 AktG), Kaufmann (§ 347 HGB) den „Anerkannten Stand von Wissenschaft und Praxis" beachten muss, wird eine **Rechtsverbindlichkei**t ausgelöst:

Weltweit sind über 1,1 Mio. Unternehmen nach ISO 9001 (Qualitätsmanagement) zertifiziert und eine weitere sehr hohe Zahl beachtet den Standard, ohne sich zertifizieren zu lassen. Damit lässt sich **in vorliegendem Fall von einem „Anerkannten Stand"** sprechen.

4.2 ISO 19600:2014: Compliance-Managementsystem

Inhalt

Deutsche Version:

8.3 Ausgegliederte Prozesse

*Die Organisation sollte sicherstellen, dass **ausgegliederte Prozesse gesteuert und überwacht** werden.*

*Das Ausgliedern betrieblicher Tätigkeiten einer Organisation entbindet die Organisation in der Regel nicht von ihrer gesetzlichen Verantwortung oder ihren bindenden Verpflichtungen. Im Falle der Ausgliederung von Tätigkeiten einer Organisation, muss die Organisation **wirksame Prüfungen (Due Diligence) vornehmen**, um sicherzustellen, dass ihre Standards und ihr Bekenntnis zu Compliance dadurch nicht vermindert werden. **Steuerungen von Vertragsnehmern** sollten erfolgen, um sicherzustellen, dass der Vertrag wirksam eingehalten wird (z. B. durch die Leistungsbewertung von Drittparteien).*

*Die Organisation sollte Compliance-Risiken in Verbindung **mit anderen drittparteienbezogenen Prozessen** in Betracht ziehen, wie z. B. bei der Lieferung von Waren und Dienstleistungen und beim Vertrieb von Produkten, und **Steuerungen umsetzen**, wo notwendig (z. B. mittels bindender Verpflichtungen in Vertragsklauseln).*

Englische Version:

8.3 Outsourced processes

*The organization should ensure that **outsourced processes are controlled and monitored.***

Outsourcing of an organization's operations usually does not relieve the organization of its legal responsibilities or compliance obligations.

If there is any outsourcing** of the organization's activities, the **organization needs to undertake effective due diligence to ensure that its standards and commitment to compliance will not be lowered.

***Controls over contractors should also be in place** to ensure that the contract is complied with effectively (e.g. third-party performance appraisals).*

The organization should *consider compliance risks related to other third-party-related processes, such as supply of goods and services and distribution of products, and* ***put controls in place****, as necessary (e.g.compliance obligations in contractual clauses).*

Rechtliche Beurteilung

Wie oben 4.1

4.3 COSO I:2013: Internal Control

Inhalt

Appendices/ B. Roles and responsibilities/External parties/Outsourced Service Providers

External Parties

A number of external parties can contribute to the achievement of the entity's objectives, whether by performing activities as ***outsourced service providers*** *or by providing data or analysis to functional/operational personnel. In both cases, functional/operational management always retains full responsibility for internal control.*

Outsourced Service Providers

Many organizations outsource business functions*, delegating their roles and responsibilities for day-to-day management* ***to outside service provider****s. Administrative, finance, human resources, technology, legal, and even select internal operations can be executed by parties outside the organization, with the objective of obtaining access to enhanced capabilities at a lower cost.*

For example, a financial institution may outsource its loan review process to a third party, a technology company may outsource the operation and maintenance of its information technology processing, and a retail company may outsource its internal audit function.

While these external parties execute activities for or on behalf of the organization, management ***cannot abdicate its responsibility to manage the associated risks. It must implement a program to evaluate those activities performed by others*** *on their behalf to assess the effectiveness of the system of internal control over the activities performed by outsourced service providers.*

Rechtliche Beurteilung

Wie oben 4.1

4.4 ISO 37001:2016: Antikorruption

8.5 Verwirklichung von Kontrollen zur Korruptionsbekämpfung durch gesteuerte Organisationen und durch Geschäftspartner

[…]

8.5.2 In Bezug auf Geschäftspartner *[…]* ***muss die Organisation Verfahren wie folgt verwirklichen:***

a) die Organisation muss bestimmen, ob der Geschäftspartner Kontrollen zur Korruptionsbekämpfung eingerichtet hat, die das relevante Korruptionsrisiko führen und steuern.

b) wenn ein Geschäftspartner keine Kontrollen zur Korruptionsbekämpfung eingerichtet hat oder es nicht möglich ist nachzuweisen, ob er sie eingerichtet hat:

> *1) wenn durchführbar,* ***muss die Organisation vom Geschäftspartner die Verwirklichung von Kontrollen*** *zur Korruptionsbekämpfung für die relevante Transaktion, das relevante Projekt oder die relevante Tätigkeit* ***erfordern****; oder […]*

ANMERKUNG *Siehe A.13 für Anleitung.*

8.6 Verpflichtungen zur Korruptionsbekämpfung

Für Geschäftspartner, *die mehr als ein niedriges Korruptionsrisiko darstellen,* ***muss die Organisation Verfahren verwirklichen, die, soweit durchführbar, erfordern:***

a) ***dass sich Geschäftspartner dazu verpflichten, Korruption*** *durch oder im Auftrag oder zum Vorteil des Geschäftspartners in Verbindung mit der relevanten Transaktion, dem relevanten Projekt, der relevanten Tätigkeit oder Beziehung* ***zu verhindern;***

b) ***dass die Organisation in der Lage ist, die Beziehung mit dem Geschäftspartner im Fall von Korruption*** *durch oder im Auftrag oder zum Vorteil des Geschäftspartners in Verbindung mit der relevanten Transaktion, dem relevanten Projekt, der relevanten Tätigkeit oder Beziehung* ***zu beenden;*** *[…]*

A.13 Verwirklichung des Managementsystems zur Korruptionsbekämpfung durch gesteuerte Organisationen und Geschäftspartner

A.13.1 Allgemeines

A.13.1.1 *Der Grund für die Anforderung (8.5) liegt darin, dass sowohl gesteuerte Organisationen als auch Geschäftspartner ein Korruptionsrisiko für die Organisation darstellen können. […]*

A.13.3 Geschäftspartner

A.13.3.1 *[…]*

A.13.3.2 *[…] unternimmt die Organisation die folgenden weiteren Schritte nach 8.5:*

a) ***Die Organisation muss bestimmen, ob der Geschäftspartner angemessene Kontrollen zur Korruptionsbekämpfung einsetzt****, welche das relevante Korruptionsrisiko führen und steuern. Die Organisation sollte dies nach der Durchführung angemessener gebührender Sorgfalt festlegen. Diese gebührende Sorgfalt könnte beispielsweise beinhalten,* ***dass vom Geschäftspartner gefordert wird, der Organisation zu erklären (bei einem Treffen oder schriftlich), ob er angemessene Steuerungen einsetzt, beschreibt, worin diese Steuerungen bestehen und angemessene Kopien von Dokumenten bereitstellt, um nachzuweisen, dass er diese Steuerungen ausführt.*** *Die Organisation bemüht sich zu überprüfen, dass diese Steuerungen das relevante Korruptionsrisiko für die Transaktion zwischen der Organisation und dem Geschäftspartner führen und steuern. Die Organisation muss nicht nachweisen, dass der Geschäftspartner Steuerungen über seine erweiterten Korruptionsrisiken ausübt. Es sei angemerkt, dass* ***sowohl die Schritte, welche die Organisation unternehmen muss, um diese Steuerungen zu überprüfen*** *als auch das Ausmaß der Steuerungen für das relevante Korruptionsrisiko* ***angemessen und verhältnismäßig sein sollten.*** *[…]*

b) ***Wenn die Organisation feststellt, dass der Geschäftspartner keine angemessenen Kontrollen*** *zur Korruptionsbekämpfung, welche die relevanten Korruptionsrisiken führen und steuern,* ***einsetzt oder es nicht möglich ist zu überprüfen ob er diese Kontrollen einsetzt****, dann* ***unternimmt die Organisation die folgenden weiteren Schritte:***

> *1) Wenn durchführbar (siehe A.13.7), muss die Organisation von dem Geschäftspartner fordern, Kontrollen zur Korruptionsbekämpfung hinsichtlich der relevanten Transaktion, dem Projekt oder der Tätigkeit zu verwirklichen.*
>
> *2) Wenn es nicht durchführbar ist […]*

A.13.3.3 Ob es für die Organisation durchführbar ist, von einem nicht-gesteuerten Geschäftspartner die Verwirklichung von Kontrollen einzufordern *oder nicht, hängt von den Umständen ab. Zum Beispiel:*

a) ***Sie wird üblicherweise durchführbar sein, wenn die Organisation maßgeblichen Einfluss auf den Geschäftspartner ausübt****.* ***Beispielsweise, wenn die Organisation einen Vertreter bestimmt, um sich in ihrem Auftrag an einer Transaktion zu beteiligen*** *oder* ***einen Unterauftragnehmer mit großem Arbeitsumfang bestimmt****. In diesem Fall wird die Organisation üblicherweise in der Lage sein, die Verwirklichung von Kontrollen zur Korruptionsbekämpfung zu einer Bedingung der Vereinbarung machen.*

b) Sie wird üblicherweise nicht durchführbar sein, wenn die Organisation keinen bedeutenden Einfluss auf den Geschäftspartner hat. Zum Beispiel: […]

c) Sie wird üblicherweise nicht durchführbar sein, ***wenn der Geschäftspartner nicht über die Ressourcen oder die Sachkenntnis zur Verwirklichung von Kontrollen*** *verfügt.*

A.13.3.4 *Die durch die Organisation geforderten Arten von Kontrolle hängen von den Umständen ab. […] darf die Organisation beispielsweise die folgenden Schritte unternehmen:*

a) Im Falle eines Geschäftspartners mit erheblich hohem Korruptionsrisiko mit einem großen und komplexen Arbeitsumfang ***könnte die Organisation von dem Geschäftspartner fordern, Steuerungen zu verwirklichen,*** *die denen in dieser Internationalen Norm gleichwertig sind, entsprechend dem Korruptionsrisiko, das er für die Organisation darstellt.*

*b) Im Fall eines Geschäftspartners mittlerer Größe und mittlerem Korruptionsrisiko **darf die Organisation** von **dem Geschäftspartner fordern, einige Mindestanforderungen** zur Korruptionsbekämpfung bezüglich der Transaktion **verwirklicht zu haben, beispielsweise** eine Politik zur Korruptionsbekämpfung, Schulung für seine relevanten Beschäftigten, **eine leitende Person** mit Verantwortlichkeit für die Einhaltung der Transaktion, **Überwachung von Schlüsselzahlungen** und eine **Berichtslinie.***

*c) Im Fall kleiner Geschäftspartner, die einen ganz bestimmten Arbeitsumfang haben (beispielsweise ein Vertreter oder kleiner Lieferant) **darf die Organisation Schulung für relevante Beschäftigte fordern sowie Überwachung über Schlüsselzahlungen** und Geschenke und Bewirtung. Die Steuerungen brauchen nur bei der Transaktion zwischen der Organisation und dem Geschäftspartner zum Einsatz kommen (obwohl der Geschäftspartner in der Praxis Steuerungen bezüglich seines ganzen Geschäfts eingesetzt haben kann). Obenstehendes sind lediglich Beispiele. **Das wichtige Thema für die Organisation** ist die Identifizierung der wichtigsten Korruptionsrisiken bezüglich der Transaktion und so weit durchführbar, **zu fordern, dass der Geschäftspartner angemessene und verhältnismäßige Kontrollen** über diese Korruptionsrisiken verwirklicht hat.*

A.13.3.5 Die Organisation wird diese Anforderungen** nicht-gesteuerten Geschäftspartnern **üblicherweise als Voraussetzung für die Zusammenarbeit** mit dem Geschäftspartner **und/oder als Teil des Vertragsdokuments auferlegen.

A.13.3.6** Die Organisation ist nicht verpflichtet, die vollständige Einhaltung mit diesen Anforderungen durch den nicht-gesteuerten Geschäftspartner zu überprüfen. **Allerdings sollte die Organisation angemessene Schritte unternehmen, sich selbst von der Einhaltung des Geschäftspartners zu überzeugen (z. B. durch Anforderung von Kopien der relevanten Dokumente zu Politiken des Geschäftspartners)**. In Fällen von hohem Korruptionsrisiko (z. B. ein Vertreter) darf die Organisation **Überwachungsverfahren verwirklichen, z. B. Berichte und Recht für Audits.

A.13.3.7** Da Kontrollen zur Korruptionsbekämpfung für ihre Verwirklichung einige Zeit benötigen können, ist es für die Organisation wahrscheinlich angemessen, seinen Geschäftspartnern **Zeit zur Verwirklichung** solcher Kontrollen **einzuräumen.** Die **Organisation könnte in der Zwischenzeit mit dem betreffenden Geschäftspartner weiterarbeiten**, **jedoch wäre das Fehlen solcher Kontrollen ein Faktor bei** der Risikobeurteilung und der **gebührenden Sorgfalt.

Rechtliche Beurteilung

Wie oben 4.1

Hinweis: Es gibt noch sehr viele aktuelle weitere Standards, die alle - in Unterpunkten - im wesentlichen gleiche Anforderungen an Aufsicht/Überwachung/Kommunikation bei ausgelagerten Leistungen stellen.

Darüber hinaus existieren bereits seit längerer Zeit **besondere Standards, die sich *ausschließlich* mit der Überwachung bei Auslagerungen beschäftigen:**[22]

[22] Scherer/Fruth (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk und Compliance (GRC), 2016, S. 69 ff..

5. Spezielle Standards bei Auslagerungen / Delegationen

(Prüfungs-)Standards bei Auslagerungen

Für Auslagerungen (auch im Rahmen eines Unternehmensverbundes/Konzerns zwischen Mutter und Töchtern) gibt es bereits **spezielle Prüfstandards, um den Delegationsempfänger zu bewerten.**

Beispielsweise im Bereich der IT-Dienstleistungen oder für rechnungslegungsrelevante Geschäftsprozesse zum Nachweis eines funktionierenden internen Kontrollsystems nach dem international anerkannten Prüfungsstandard **ISAE 3402, SSAE 16 (früher SAS 70) oder IDW PS 331 bzw. 951.**

6. Zwischenergebnis

Es besteht mittlerweile nicht nur die Befugnis, sondern sogar die **Pflicht**, bei Delegationen **auch auf Selbstständige** (!) diese sorgfältig auszusuchen, zu instruieren, zu kontrollieren, zu überwachen und mit ihnen eng zu kommunizieren.

Zahlreiche Maßnahmen wurden mittlerweile – auch über die Verbreitung als Anforderungen in QM-Standards **– zum „anerkannten Stand in Wissenschaft und Praxis".**

Im Bereich der Organisations- und Delegations-Gesetzgebung und -Rechtsprechung ist dies längst verbreitet. In den Bereichen des Arbeits- /Sozialversicherungs- und Strafrechts, die sich mit der in den letzten Jahrzehnten eingesetzten Realität von supply chain management, globaler Vernetzung (Industrie 4.0), Risk und Compliance kaum beschäftigen, lösen oft bereits solche Schlagwörter oder festgestellte Maßnahmen die Assoziation zur „Scheinselbstständigkeit" und entsprechende Haltungen und Vorgehensweisen aus.

De lege lata ist dies jedoch (mittlerweile) nicht mehr zulässig.

De lege ferenda sollte hier Klarheit geschaffen werden, um das Risiko einer nicht zeitgemäßen Rechtsanwendung nicht – unzulässigerweise – den wirtschaftlich Tätigen aufzuerlegen.

Bei Delegationen / Auslagerungen bestehen auch gegenüber Selbstständigen Kontroll-, Überwachungs-, Informations- und gegebenenfalls auch Weisungsrechte oder sogar auch –Pflichten.

Bei Ausübung dieser Pflichten durch den Delegierenden verböte es sich, dies zu seinen Lasten als Indikator für Scheinselbstständigkeit bzw. „Eingliederung in die betriebliche Organisation" zu werten. Hierfür verbleiben also nur sonstige, nach wie vor anerkannte Indikatoren.

7. Die „interested parties“ des Delegationsempfängers

7.1 Die „interested parties“ des Lieferanten / Leistungserbringers / Delegationsempfängers bei Outsourcing / Delegation

Der Kunde ist eine von vielen „interested parties (intern und extern)“ eines externen Delegationsempfängers / Suppliers.

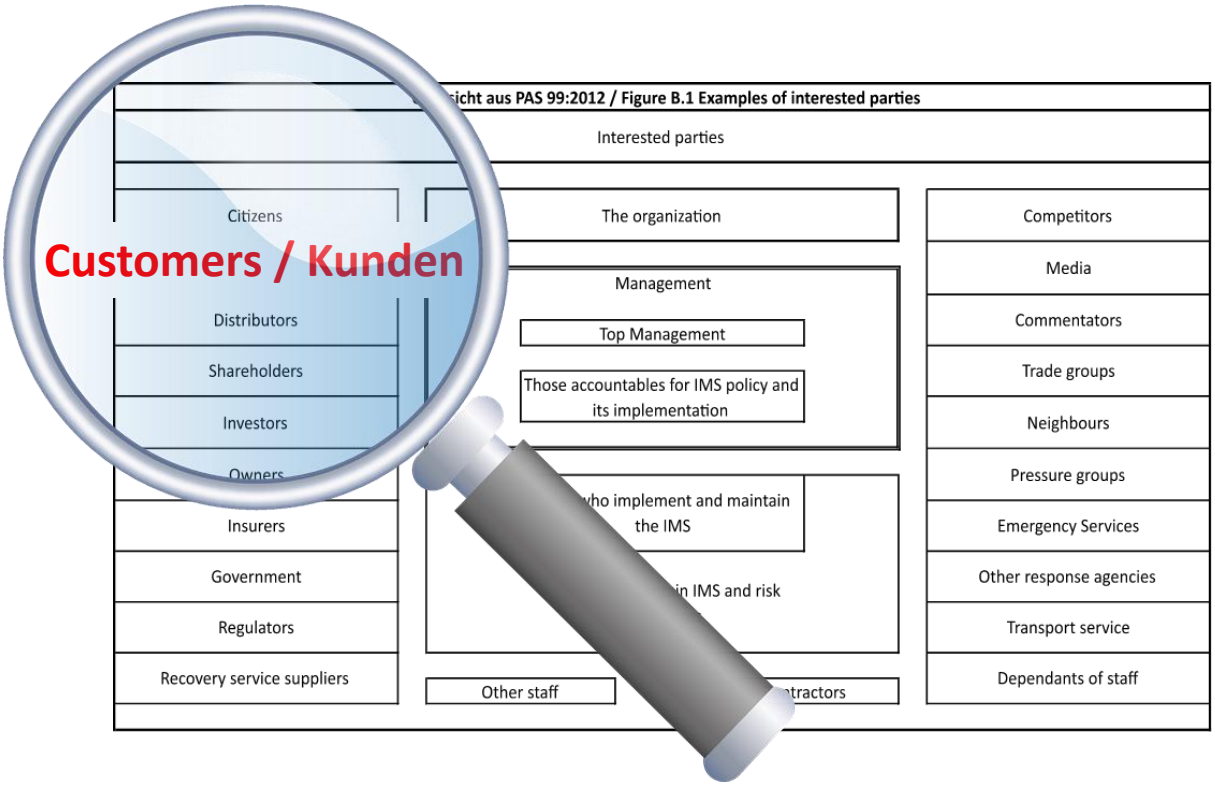


Abbildung 1: Vgl. „interested parties“: Aus PAS 99:2012, S. 16.

7.2 Überwachungsfunktionen beim Kunden in Bezug auf Delegationsempfänger

Der Kunde selbst hat diverse Abteilungen, die den Lieferanten überprüfen:

Einkauf, Qualitätsmanagement, Risikomanagement, Compliance Management, Finanzen, Revision, etc.

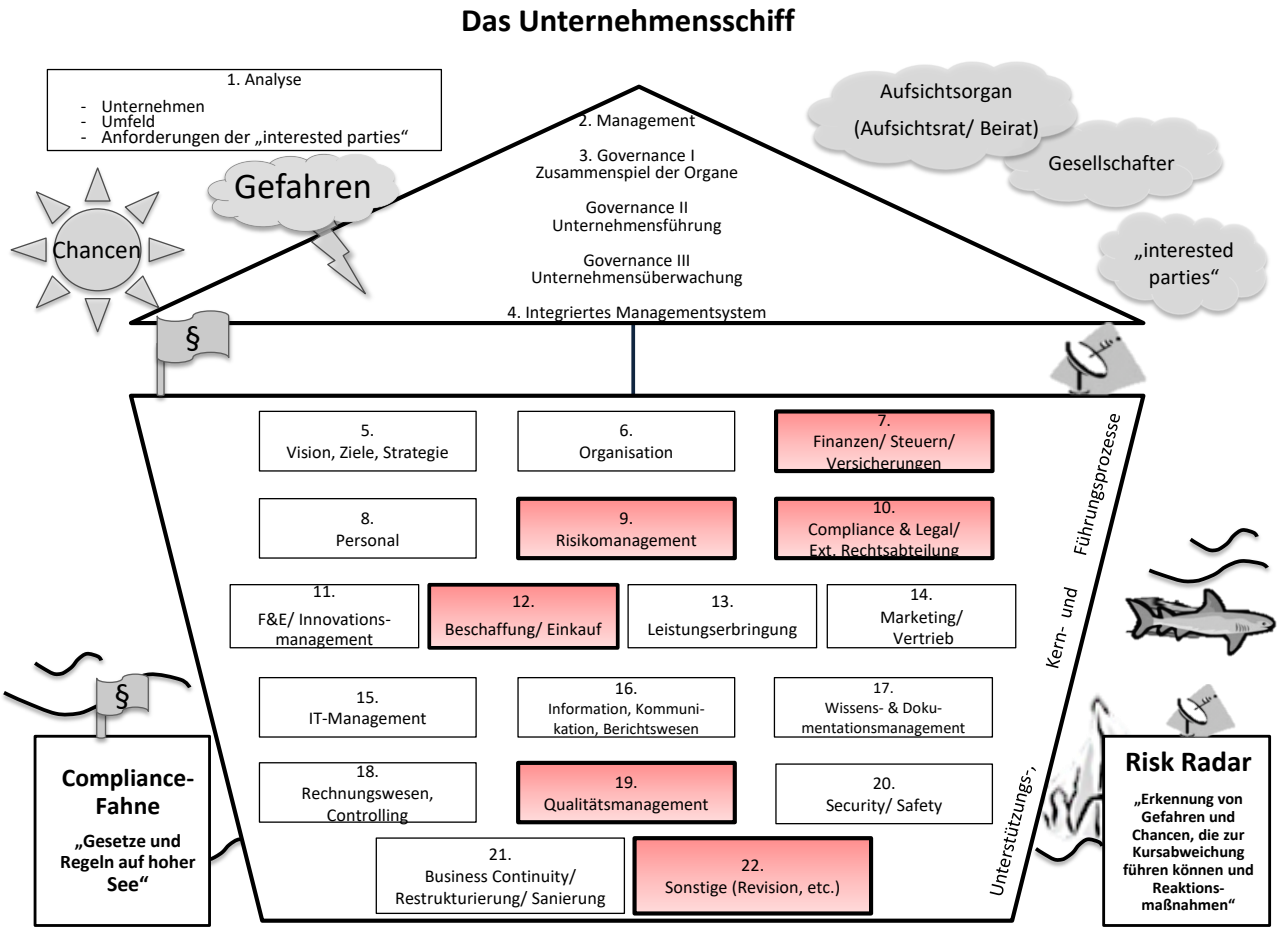


Abbildung 2: Das Unternehmensschiff und die den Delegationsempfänger überwachenden Funktionen![23]

Hier besteht beim Delegierenden / Kunden / Auftraggeber durch **Konzentration auf eine Funktion**, die den Lieferanten überprüft**, bereits erhebliches Einsparpotenzial!**

[23] Vgl. *Scherer / Fruth (Hrsg.),* Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2017: Abbildung 4

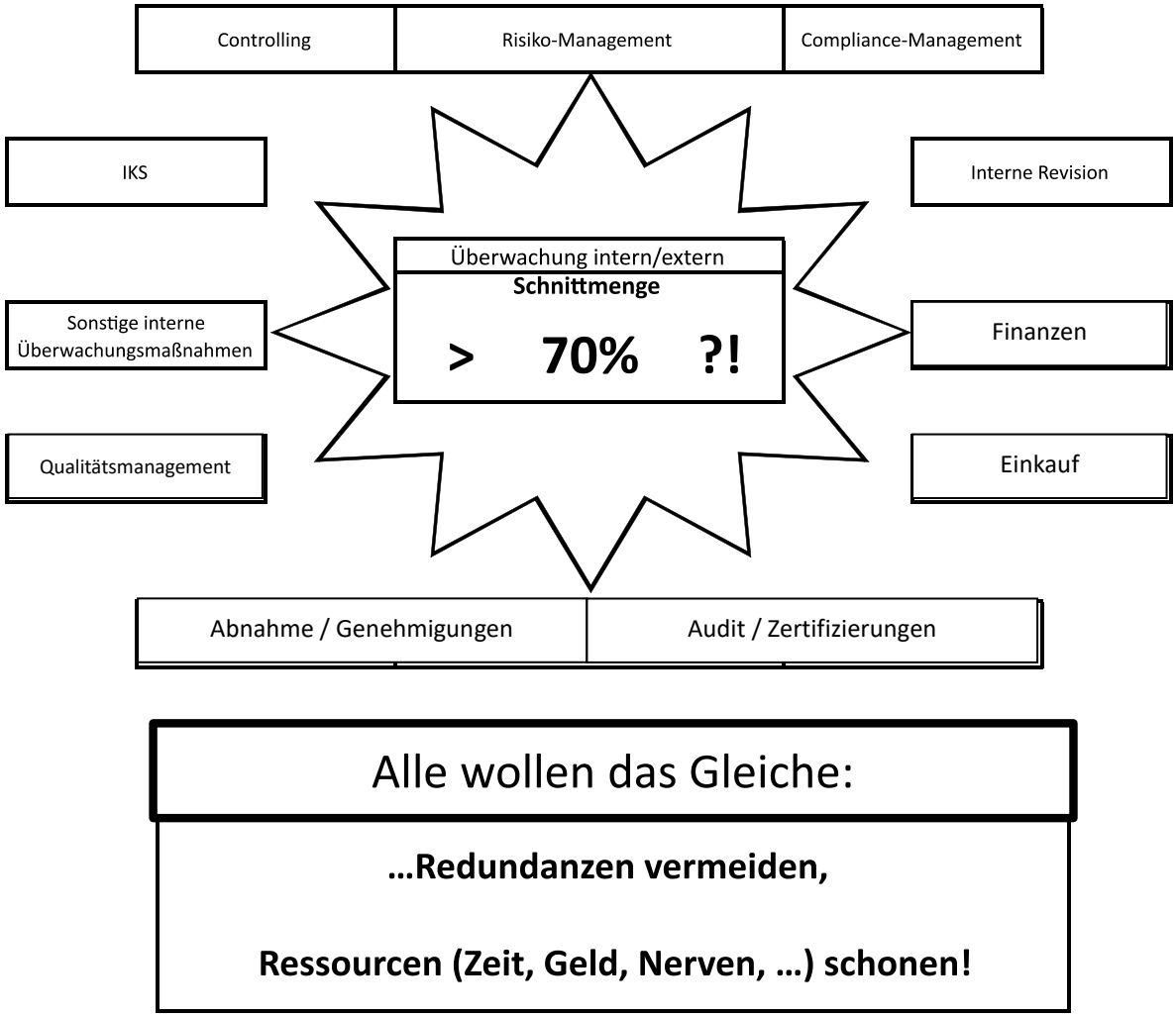


Abbildung 3: Schnittstellen und Einsparungspotenzial im Steuerungs- und Überwachungsmanagement beim Kunden in Richtung Delegationsempfänger.[24]

7.3 Sonderproblem: Der Endkunde des Delegierenden als „interested party“: „Gesetzte“ Lieferanten / Subunternehmer

Sofern der Endkunde seinen Lieferanten / Delegationsempfänger dezidiert vorgibt, welcher Subunternehmer zu wählen ist und welche Verpflichtungen in jeglicher Hinsicht ihm aufzuerlegen sind, besteht beim Auftraggeber / Delegierenden nur ein sehr eingeschränkter Spielraum in Bezug auf seinen Delegationsempfänger.

Insbesondere z.B., wenn die weiterzugebenden Pflichten sehr weitreichend sind. Diese Weitergabe stellt jedoch keine „Eingliederung in die betriebliche Organisation“ des Delegierenden dar.

Problematisch auch für den Delegierenden, dass seine **Verantwortung für Delegationsempfänger** bei „gesetzten Lieferanten“ meist in keiner Weise reduziert ist/wird.

[24] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2017: Abbildung 85

8. Lieferanten-Scoring nach Wichtigkeit

Abbildung 4: Scoring des Delegationsempfängers nach Wichtigkeit[25]

Mittels Scoring (z.B. ABC-Analyse) werden die Lieferanten / Delegationsempfänger und ihre Produkte / Leistungen nach „Wichtigkeit“ bewertet.

[25] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2017: Abbildung 137: Musterprozessvisualisierung QM / 4.3.7 / EKAUF2 / Lieferantenmanagement.

9. „Neues Lieferantenmanagement“

Beim Lieferanten wird seit längerer Zeit bei den good-practice-Unternehmen nicht mehr – wie früher – nur nach Preis, Qualität, Service und Liefertreue bewertet, sondern auch Risikolage (z.B. Ausfallrisiko) und Compliance.

Zwar wurde in Lehre und Beratung über Jahre das **Lieferantenmanagement** mit lediglich den drei Anforderungen Kosten (effizient), Zeit (fristgerecht) und Qualität vor- und nachgebetet.

Und die **ISO 9001:2015(Qualitätsmanagementsystem)** stellt auch in der neuen Version überwiegend Qualität und Service als Kundenanforderungen bzw. neue (oder nicht neu, vgl. ISO 9004) Anforderungen der „interested parties“ dar.

Es wird daher längst zu Recht gefordert, das „Anforderungs-Dreieck“ in ein **Vieleck („Polygon“, („Pentagramm“ *Mayrhofer*))** zu transformieren, um den heutigen Governance-Anforderungen u. a. mit Risiko- und Compliancemanagement, gerecht zu werden.[26]

Geradezu paradox in der neuen **ISO:9001:2015** ist die Forderung nach einem risikobasierten Ansatz einerseits und andererseits die falsche und „gefährliche“ Aussage: „***Obwohl Risiken und Chancen bestimmt und behandelt werden müssen, gibt es keine Anforderung für ein formelles Risikomanagement oder einen dokumentierten Risikomanagementprozess. (…)“***
Diese Aussage ist wohl der Angst vor der Konkurrenz der Risikomanagement-Standards oder vor der für Qualitätsmanagement völlig neuen Materie, insbesondere, wenn man Compliance-Risiken mit einbezieht, geschuldet.

Zur Begründung wird in offiziellen Schulungsunterlagen[27] angeführt, die ISO 9001:2015 beziehe sich mit dem „risikobasierten Ansatz“ vor allem auf die Gefahr von Fehlern bei Produkten und Dienstleistungen und nicht auf die Gefahren für ein Unternehmen, wie die ISO 31000 (Risikomanagement).

Dass diese Begründung bzw. **diese Interpretation nicht zeitgemäß und sinnvoll** ist, zeigt sich am Beispiel des ***modernen* Lieferantenmanagements** in der Praxis und der Anforderung in ISO 9001:2015 unter Pkt. 8.4 *„Kontrolle extern bereitgestellter Produkte und Dienstleistungen“*:

Ein modernes, gewissenhaft agierendes Unternehmen bewertet Lieferanten seit längerer Zeit nicht mehr ausschließlich nach Liefertreue, Qualität und Preis (- so auch das alte Prozessdreieck zur Bewertung von Prozessen), sondern betrachtet auch die Themen Compliance und Risikomanagement beim Lieferanten (und verifiziert dies immer häufiger mit fundierten Audits vor Ort):

Die ISO 9001:2015 hat primär die ***Erfüllung der Kundenanforderungen*** zum Ziel. Sie betrachtet daher das Unternehmen, das ein QM-System implementiert (und auditieren/zertifizieren lässt), als „Lieferant“ von Produkten/(Dienst-) Leistungen an den/die Kunden.

[26] Vgl. *Mayrhofer*, Governance Prozess Pentagramm, auf RiskNET im Internet unter: https://www.risknet.de/themen/risknews/governance-prozess-pentagramm/a5a0dcb3f503fe9264b352f336b845f7/ (letzter Zugriff: 14.08.2015).
[27] Vgl. *Gietl/Lobinger*, QM Überblick über die ISO 9001:2015, S. 11 in TÜV SÜD Akademie GmbH, Lehrgang Qualitätsmanagement Fachkraft QMF-TÜV (3/2015): *„Ein komplettes Risikomanagement ist nach ISO 9001:2015 ausdrücklich nicht gefordert. Die Maßnahmen zum Risikohandling sollen sich vor allem auf die Gefahr von Fehlern bei Produkten und Dienstleistungen beziehen und nicht auf die Gefahren für ein Unternehmen, wie es in der ISO 31000 (Risikomanagement) angedacht ist.“*

*„Die **Anforderungen des/der Kunden** bestehen aber – spätestens seit den zahlreichen Insolvenzen im Lieferantenbereich seit der Finanzkrise 2008 ff. und der **Anfälligkeiten einer supply-chain** bei Ausfall eines beliebigen Gliedes der Kette – nicht mehr lediglich in Liefertreue, Qualität und Preis, sondern als eigenes (!) Top Risiko des gesamten Kunden-Unternehmens in einer **stabilen Lieferkette**. **Dies kann beim Lieferanten jedoch nur durch ein auf sämtliche Risiken abzielendes Risikomanagement gewährleistet werden**, zumal die Ursachen für die Unfähigkeit des Lieferanten, vereinbarungsgemäß zu liefern, in jedem Bereich (vgl. „22 Felder") seines Unternehmens oder im Umfeld begründet sein können. Zahlreiche Beispiele finden sich täglich in der Presse[28]. Auch Compliance-Risiken spielen hierbei eine wesentliche Rolle: Diese können beim Lieferanten z.B. einen Produktions-, Verkaufs-, Ausfuhr-Stopp oder gar die Insolvenz verursachen (vgl. Müller-Brot in Freising: Hygienemangel führt zur Insolvenz)."*[29]

Darüber hinaus werden **Compliance-Verstöße bei Lieferanten / Delegationsempfänger** (z.B. Mindestlohnverstöße, Kinderarbeit, etc.) sehr schnell zu **existenziellen Reputationsrisiken beim Auftraggeber** führen.

10. Was wollen alle Überwacher wissen?

Was wollen alle „four lines of defense" wissen?[30]

1. Angemessene Ziele und Kennzahlen (Plan)

(Beispiele: Pflichtziele und fakultative Ziele (business-judgment-rule):

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 (line of operation) (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 und Act)

(**Beispiel**: Das „Lines of defense-Modell")

[28] Vgl. auch *Scherer* et al., Den Rücken frei: No risk, much fun!, Praxiswissen Risikomanagement und Compliancemanagement, 2007 mit den Top-Risiken in diversen Unternehmensbereichen.
[29] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk & Compliance, 2016, S. 21
[30] Vgl. auch *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2. Auflage, 2017, Pkt. 4.2.2 / CRP 3.1.4

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

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

11. In welchen Bereichen müssen die Lieferanten / Delegationsempfänger ordnungsgemäß agieren?

Welche Bereiche stehen für eine Prüfung / Bewertung durch den Kunden / Delegierenden zur Auswahl?

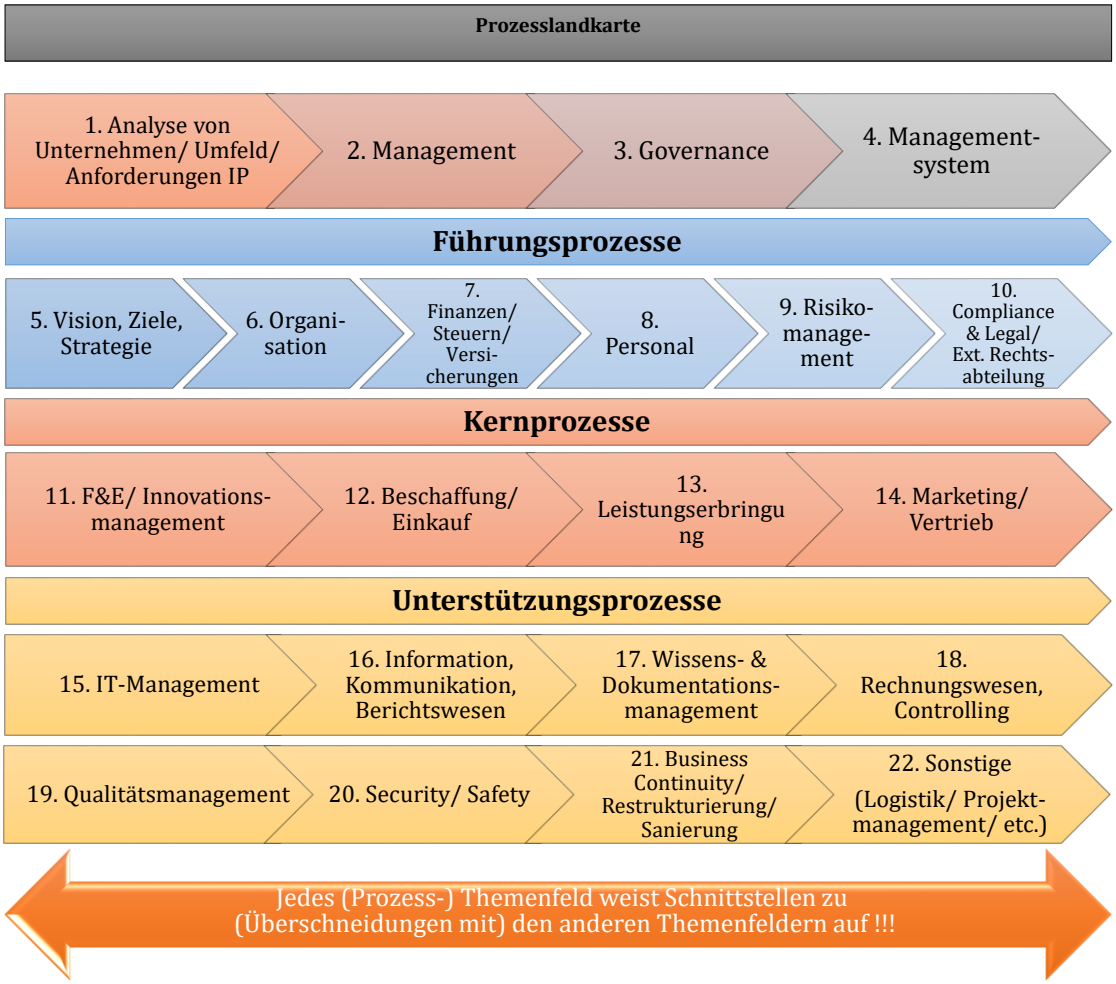


Abbildung 5: Prozesslandkarte.[31]

[31] Vgl. Scherer / Fruth (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2017: Abbildung 45:

12. Welche Bereiche des Lieferanten / Delegationsempfängers sind prüfungsrelevant?

Vor allem Produktion / Leistungserstellung, Qualitätsmanagement, Risikomanagement, Compliance Management des Lieferanten? Oder auch Finanzen, Organisation, Personal?

Oder sogar noch weitere Themen?

Nachhaltigkeit? Arbeitsbedingungen? Umwelt?

Wichtig:

Ursachen für existenzielle Probleme beim Delegationsempfänger, die zu großen Problemen beim Kunden / Auftraggeber führen mögen, **können in allen (Prozess-) Themenbereichen schlummern** (vgl. Müller-Brot: Hygiene-Mangel).

Daher: **Die Relevanz des abzuprüfenden Themas ist zu bewerten.**

Beim Delegationsempfänger stehen ca. 22 Themenfeldern zur Auswahl.

13. Wie kommt der Kunde / Delegierende effizient an Infos über den Lieferanten?

Vor großangelegtem Risiko-Check-Anfragen bei Lieferanten steht die Prüfung:

Wie wichtig ist das delegierende Unternehmen für den Lieferanten?

Bekommt es die gewünschten Infos überhaupt?

Sollte die „Wichtigkeit“ des eigenen Unternehmens für den Delegationsempfänger hoch genug sein, erfolgt **zunächst eine Arbeitsteilung intern:**

Zusammenführung der der internen Überwachungsfunktionen (Qualitätsmanagement, Risiko, Compliance Management, etc.) zu *einer* einzigen Lieferanten-Scoring Funktion!

Vergleiche auch die Redundanz in den jeweiligen ISO Standards Unterpunkt 8.4: Überprüfung des Lieferanten:

- ☐ ***ISO 19600:2014: 8.3 Outsourced processes***
- ☐ ***COSO I:2013: Appendices / B. Roles and Responsibilities / External parties / Outsourced Service Providers***
- ☐ ***ISO 37001:2016: 5.3.2 Funktion für die Compliance mit der Korruptionsbekämpfung / 8.5 Verwirklichung von Kontrollen zur Korruptionsbekämpfung durch gesteuerte Organisationen und durch Geschäftspartner***

☐ ***ISO 9001:2015: 8.4 Steuerung von extern bereitgestellten Prozessen, Produkten und Dienstleistungen***

14. Diverse Abstufungen (Tiefe) der Informationen

Erstellung eines *einzigen* Lieferanten-Checks!

Dabei ist bzgl. der Tiefe der Untersuchung die „Angemessenheit“ zu wahren!

Worum muss sich ein Unternehmer kümmern?									
Nr.	**Welches (Prozess-)Themenfeld des Lieferanten könnte überprüft werden?**	**Gibt es dafür Soll-Vorgaben (z.B. ISO-Standards)? Welche? Z.B.:**	**Gibt es Zertifikate?**	**Gibt es Checklisten?**	Was ist seitens des Überwachers sinnvoll?	Vorlage Zertifikate?	Weitere Dokumente?	Audit vor Ort?	Stresstest?
1	Analysen von Unternehmen Umfeld und interested parties	GoP	✘	Checkliste Unternehmens-analyse					
2	Management (fachliche und persönliche Kompetenzen)	IDW PS 720	✘	Checkliste Kompetenzen					
3	Governance I (Zusammenspiel der Organe)	DCGK	✘	Checkliste Governance					
	Governance II (Unternehmensführung GoU)	COSO II	✘	Checkliste Governance					
	Governance III (Unternehmensüberwachung GoÜ)	COSO I	✘	Checkliste Governance					
4	Managementsystem	PAS 99	✘	Checkliste Management-system					
5	Vision / Ziele / Strategie / Planung	GoP	✘	Checkliste Vision / Ziele / Strategie / Planung					
6	Organisation	ISO 9001	✘	Checkliste Organisation					
7	Finanzen / Steuern / Versicherung	COSO I	✘	Checkliste Finanzen / Steuern / Versicherung					
8	Personal	ISO 30400	✘	Checkliste Personal					
9	Risiko-Management	ISO 31000	✘	Checkliste Risiko					
10	Compliance & Legal / (externe) Rechtsabteilung	ISO 19600	✘	Checkliste Compliance					
Etc.	Etc.		✘	Etc.					

15. Effizienz durch Zertifikate

Es empfiehlt sich das Einfordern von Kombi-Zertifikaten, die viele Fragen der Überwacher abbilden.

Und die Durchführung von Stichproben, ob die zertifizierten Themenbereiche tatsächlich wirksam (gelebt werden) oder nur implementiert sind.

16. Exkurs: Zertifikats-Dschungel und die Lösung: Ein zertifiziertes „Integriertes Managementsystem“ beim Delegationsempfänger als Nachweis gegenüber den Kunden / Delegierenden[32]

Alle „Überwacher“ müssen sich an sehr ähnlichen Referenz- oder Sollgrößen orientieren

Jeder „Überwacher“ müsste sich aufgrund der Legalitätspflichten primär an Rechtsprechung und Gesetz, „Anerkanntem Stand von Wissenschaft und Praxis“, sowie sekundär an aktuellen Standards mit daraus abgeleiteten Kennzahlen orientieren.

Dass Standards nur Mindestanforderungen darstellen und die Gerichte z.B. bei konkreten Gefährdungssituationen trotz Einhaltung von Standards mehr verlangen, ist gängige Rechtsprechung.

Nachfolgende Abbildung zeigt,

- ☐ **um welche Bereiche der Lieferant / Delegationsempfänger** (bzw. seine Leitungsorgane) **sich kümmern muss** (alle Führungs-, Kern- und Unterstützungsprozesse).
- ☐ Außerdem, **welche Eigenschaften diese Bereiche / Prozesse** erfüllen müssen („Soll-Anforderungen“) und
- ☐ **an welchen Referenzgrößen** (Soll) sich der **Soll-Ist-Vergleich** jeweils zu orientieren hat.

[32] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2. Auflage, 2017, S. 303 – 318

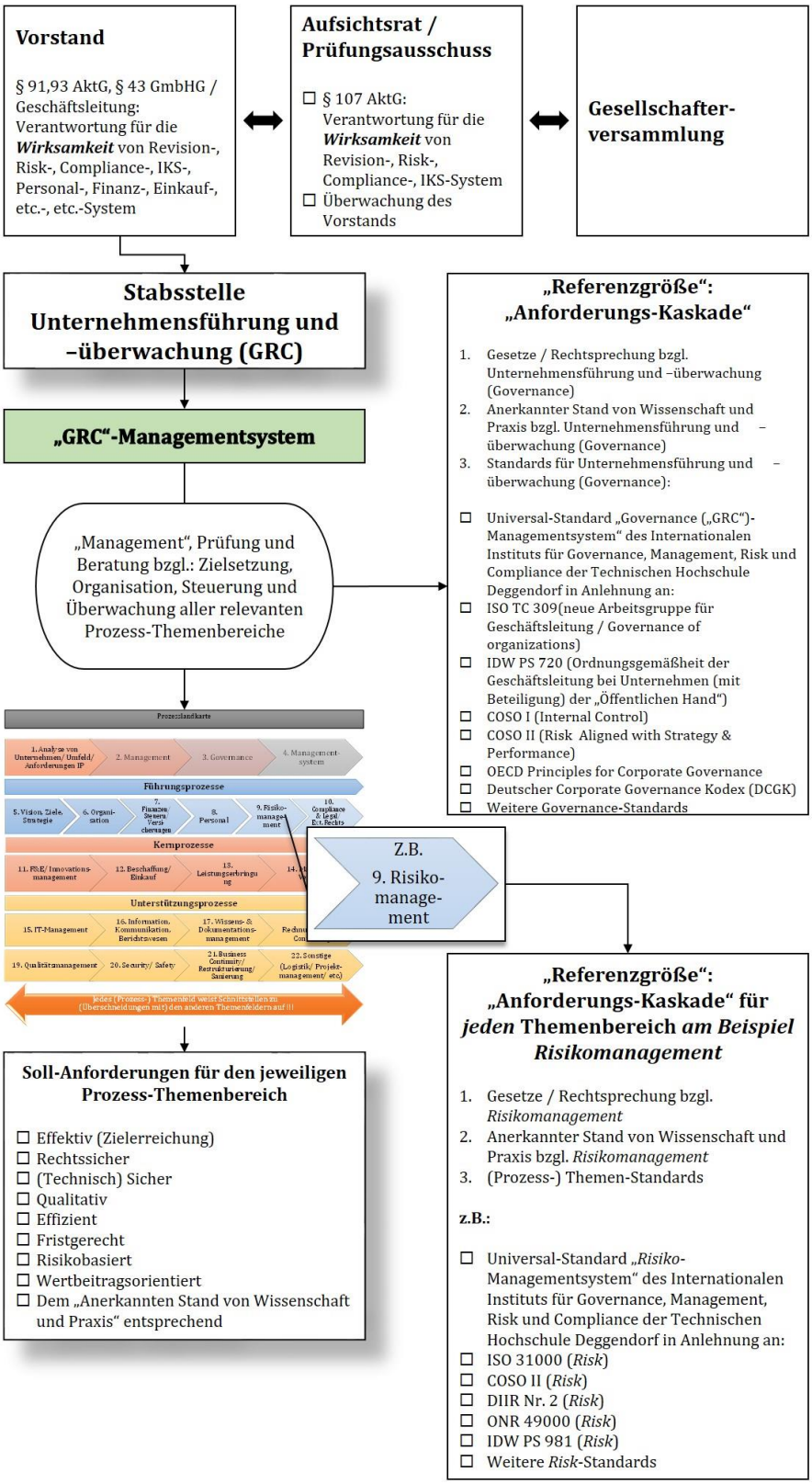


Abbildung 6: Überwachung diverser Bereiche und Orientierung an Referenzgrößen. [33]

[33] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2. Auflage, 2017: Abbildung 22

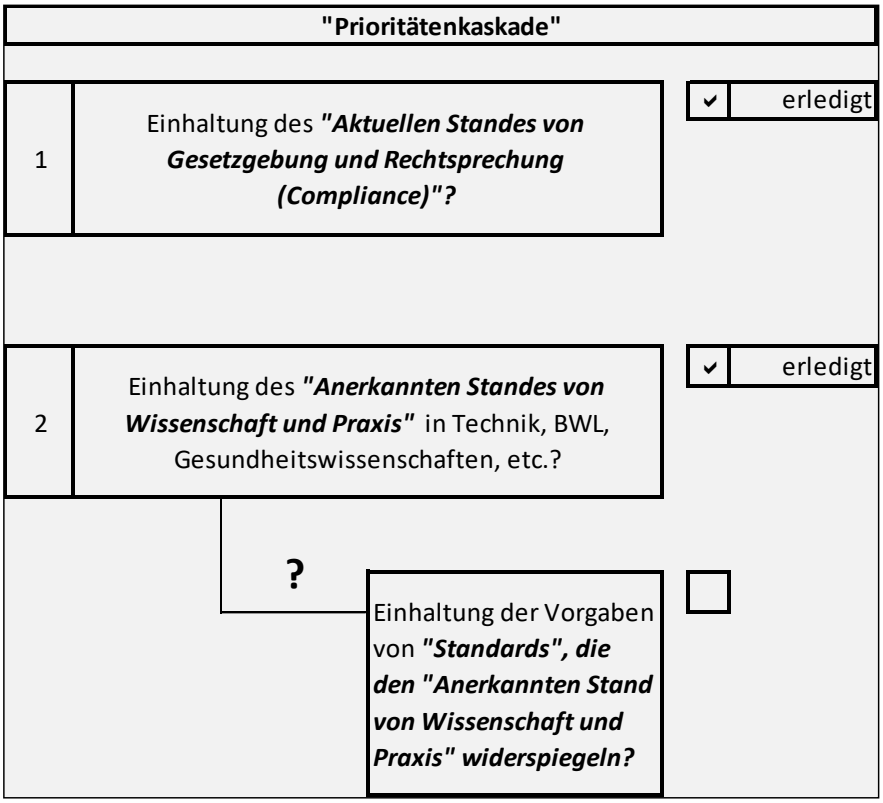


Abbildung 7: Prioritätenkaskade.

Ein nachvollziehbares Bewertungsschema muss bei allen Überwachern letztendlich zu den wesentlichen Urteilen, wie „legal/illegal“, „gut/schlecht“, „angemessenen/nicht angemessenen“ oder Ähnlichem führen.

Aktuelle Trends in Gesetzgebung, Rechtsprechung und Standardisierung

Gesetzgebung und Rechtsprechung durchdringen mittlerweile nahezu jede unternehmerische Aktivität und regeln sogar, wie ein Unternehmer (pflichtgemäß) zu denken und entscheiden hat [(vgl. die sog. Business Judgment Rule (§ 93 Abs. 1 S. 2 AktG), die auch auf GmbH-Geschäftsführer Anwendung findet)].

Ebenso werden mittlerweile nahezu alle Prozessthemenfelder eines Unternehmens von **„*Standards*“** erfasst, die zeigen wollen, was **„Anerkannter Stand von Wissenschaft und Praxis“,** also die Messlatte für pflichtgemäßes und richtiges Handeln ist.

Überwachung und Bewertung (Performance Evaluation) eines Delegationsempfängers

Die Überwachung und Bewertung eines Delegationsempfängers an sich erfolgt primär intern durch diverse idealerweise „gebündelte“ Funktionen (Controlling, Compliance, Internes Audit, IKS, Revision (vgl. auch die „Three lines of defense)), kann aber auch Gegenstand externer Überwachung (Aufsichtsrat, Behörden, „second“ und „third party“(Zertifizierungs-) Audits, etc.) sein.

Die Auflösung zahlreicher Redundanzen durch Implementierung, Auditierung und Zertifizierung eines Integrierten „Kombi-Managementsystems - on demand“

Es gibt eine **Vielzahl interner und externer Prüfungs-/Überwachungs-/Audit-/Konformitätsbewertungs-Funktionen**, vgl. oben. Diese gehen leider in der Praxis nicht konzertiert, sondern nebeneinander agierend vor, **obwohl sie alle im Wesentlichen das Gleiche wollen:**

Die richtigen Ziele und Transparenz über die Anforderungen, um Unternehmensziele zu erreichen. Passsende, auf diese Ziele abgestimmte Kennzahlen und gelebte Prozesse, die mit den diversen Muss- und Soll-Anforderungen angereichert sind, um den beabsichtigten Output zu gewährleisten. Außerdem ein angemessenes und wirksames Steuerungs- und Überwachungssystem.

Die in der Praxis feststellbaren unzähligen – redundanten - Aktionen kosten erhebliche Ressourcen:

Nachfolgend wird das „Überwachen von allen Seiten“ lediglich *am Beispiel Risikomanagement* dargestellt:

„COSO-Welt“

Von Seite „SOX“ (Sarbanes Oxley Act) und der **COSO-Welt** kommend, agieren national und international **Wirtschafts- und Abschlussprüfer** mit eigenen Prüfstandards (z.B. **IDW/IAS**), die z.T. zwischen **Konzeptionierungs-/Angemessenheits- und Implementierungs- sowie Wirksamkeitsprüfung** differenzieren.

„Wirtschafts- und Abschlussprüferwelt“

Hinweis: Es ist bei den Wirtschaftsprüfungen zwischen Pflichtprüfungen im Rahmen der Abschlussprüfung (z.B. Risiko-, Chancen- und Prognosebericht / Risikofrüherkennungssystem) und sonstigen Prüfungen (z.B. Risiko-Managementsystem nach IDW PS 981) zu differenzieren.

Für die **„Wirtschaftsprüfungs-Welt“** ist z.B. IDW EPS 981:2016 (Risiko-Managementsysteme) oder IDW PS 341 (Risiko-Früherkennungssystem) relevant, genauso aber auch COSO II:2004 (Enterprise Risk Management) bzw. künftig COSO II:2017 (?) (Risk Aligned with Strategy and Performance).
„ISO-Welt“

Für Third-Party-Audits (z.B. Zertifizierungen für Kunden, weil gefordert, oder um damit zu werben) bietet die internationale **ISO-Welt** für Managementsysteme meist ***Wirksamkeits*zertifizierungen / -audits** an (wobei ISO 31000:2009 (neue Version soll 2017/2018 erscheinen) nicht zertifizierbar ist, weshalb für die Zertifizierung durch grundsätzliche ISO-Zertifizierer auch andere Standards (z. B. ONR 49000 (Risiko-Managementsystem) herangezogen werden:

So als „Vorreiter" vom Verfasser in Kooperation mit TÜV 2010 in Deutschland erstmalig praktiziert.

„Welt der Revision"

Nicht zu vergessen die **„Welt der Revision"**: deutsch (z.B. Deutsches Institut für Interne Revision(DIIR), aber auch global (z. B. Institute of Internal Auditors – IIA). So gibt es auch hier beispielsweise einschlägige Audit-Standards, z. B. DIIR Nr. 2:2014 (Prüfung des (Compliance-)Risikomanagements).

„Welt der Controller"

Ebenso die **Controller mit eigenen Controlling-Standards** (z. B. die Grundsätze ordnungsgemäßer Planung (GoP) oder „Controlling-Standards").

„Aufsichts- und Überwachungs-Behörden-Welt"

Die Welt der Revision, aber z.B. auch die **„Welt der Behörden**" (z.B. Aufsichtsbehörden oder Staatsanwaltschaft) hinterfragen die *Wirksamkeit*, beruhend auf angemessenem Konzept und Implementierung.

Sinnvoll scheint hier eine Harmonisierung mit dem Ziel: „best of both/ three/four/… worlds".

Der Beweis, dass alle nahezu das Gleiche (nicht Dasselbe!) verlangen:

Beispiel: „Interested parties-Analyse"

Am Beispiel der Komponenten **„Anforderungen der interested parties"**, die nahezu von jedem Standard gefordert wird, lässt sich die einfache Möglichkeit zu Auflösung von Redundanzen gut aufzeigen:

Die neue Forderung bzgl. „interessierter Gruppen" im ISO 9001:2015 Qualitätsmanagement-Standard

Aufgrund der veränderten technologischen Umwelt, die durch neue Möglichkeiten der Kommunikation **erhöhte Präsenz und Transparenz** gerade auch bei Ereignissen gewährleistet, die zu enormen **Reputationsrisi-**

ken führen, **verdient das Thema „interested parties" in der Praxis wesentlich stärkere Beachtung**. Dies spiegelt sich auch in den Anforderungen von „Industrie 4.0" und den neueren Standards (ISO / IDW / G20/OECD Principles of Corporate Governance / etc.) wider:

Die erstmalige Forderung der ISO 9001: 2015 bzgl. der „interessierten Gruppen" in der ISO 9001: 2015 (Qualitätsmanagementsystem) lautet:

„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Aufgrund ihres Einflusses bzw. ihres potentiellen Einflusses auf die Fähigkeit der Organisation zur fortlaufenden Bereitstellung von Produkten und Dienstleistungen, die die Anforderungen der Kunden und die zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen, muss die Organisation:

***a) die interessierten Parteien**, die für ihr Qualitätsmanagementsystem relevant sind, **b) die Anforderungen dieser interessierten Parteien**, die für ihr Qualitätsmanagementsystem relevant sind, **bestimmen**."*

Anmerkung: Es fehlt m.E. als Anforderung im Standard, die bestimmten Anforderungen zu bewerten (mit angemessenen Risikomanagementmethoden!) und daraus abgeleitete erforderliche Maßnahmen umzusetzen. Erst dann wird aus dieser Anforderung eine „Fourth line of defense" (Überwachung durch „interested parties": Sozialisation der Governance- Überwachung (im Zeitalter von „Industrie 4.0"): **Durch Business Partner und sonstige „interested parties**" (z.B. Lieferanten / Kunden /Betriebsrat / Mitglieder der externen Überwachung (Aufsichtsrat / Behörden (Zoll / Staatsanwaltschaft / Gewerbeaufsichtsamt, etc.) / externe Auditoren / etc.) / Öffentlichkeit / Medien / etc.) **kann ein erheblicher Druck in Richtung Governance-konformes Verhalten auf Unternehmen und Mitarbeiter ausgeübt werden**. Wenn auf allen Seiten ein mainstream und „common sense" zu Governance-konformen Handeln besteht und gelebt wird, tut sich der Einzelne schwer, auszuscheren.

Pflicht oder freiwillig?
Diese in der ISO 9001:2015 erstmalig genannte Forderung stellt eine *Pflichtanforderung* dar: Da die „interessierten Gruppen", wie Behörden, Regulierer, Kunden, etc., erheblichen Einfluss auf die Existenz des Unternehmens/ der Organisation ausüben können (z. B. Auftragsentzug, Produktionsstopp, Sanktionen, ...), gehört es zu den *Pflichten* eines gewissenhaften Unternehmers (§§ 43 GmbHG, 93 AktG, 107 AktG, 347 HGB, etc.), die relevanten Gruppen und deren Anforderungen zu bestimmen und gegebenenfalls entsprechende erforderliche Maßnahmen durchzuführen.

Beispiel: Das Abstellen von Hygienemängel (bei wiederholter Monierung durch die Aufsichtsbehörde) ist lediglich reagierend und kann zu spät kommen und sogar eine Insolvenz auslösen (Fall: Brotfabrik in *Freising*). Richtig ist, - im Vorfeld - zu wissen, welche Anforderungen diese Behörde an das Unternehmen stellt und diese angemessen zu erfüllen.

In dem angesprochenen Fall wurde nicht nur Anklage gegen die ehemaligen Geschäftsführer vor der Strafkammer des Landgerichts *Landshut* erhoben, sondern seitens der Staatsanwaltschaft sogar gegen den ehemaligen **Produktionsleiter** und den **Qualitätsbeauftragten** ermittelt.

Gegenüberstellung (Synopse) mit anderen Standard-Texten, die das Gleiche (nicht das Selbe) fordern:

ISO 19600: 2014 (Compliancemanagement):

„4.2 Understanding the needs and expectations of interested parties

The organisation should determine: - the interested parties that are relevant to the compliance management system; and the requirements of these interested parties".

(**Anmerkung:** Auch hier nur die Empfehlung, die interessierten Gruppen und deren Anforderungen zu bestimmen, nicht jedoch, sie angemessen zu bewerten und erforderliche Maßnahmen umzusetzen!)

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

(…) hat sich der Prüfer mit dem rechtlichen und wirtschaftlichen Umfeld,(…) zu befassen (vgl. Tz. A29)."

Ähnlich **IDW PS 981: 2017 (Risiko-Managementsystem):**

„7.3.1 Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichen und wirtschaftlichen Umfeld".

ONR 192050: 2013 (Compliance-Management-Systeme):

Hier ist keine entsprechende Anforderung ersichtlich.

COSO I: 2013 (Internal Control):

Hier ist keine entsprechende ausdrückliche Forderung ersichtlich. Jedoch existieren Anforderungen, die zumindest mittelbar auch die „interessierten Gruppen" betreffen:

*„Beurteilt **Veränderungen in externer Umwelt. Prinzip 15**: Die Organisation **tauscht sich mit Externen** über die Funktionsfähigkeit des IKS*

Aus Fokuspunkt 63 Kommuniziert mit externen Ansprechpartnern.

64 Ermöglicht Kommunikation nach außen.

*65 **Kommuniziert externe Beurteilungen dem Aufsichtsorgan.***

PAS (Public Available Standard / British Standards Institution) 99: 2012 (Integriertes Management System)

„4.2 Understanding the needs and expectations of interested parties
The organization shall determine:

a) the interested parties that are relevant to the integrated management system;

b) the requirements of these interested parties.

The organization should determine what interested parties are impacted on by the activities and what reasonable requirements need to be controlled to meet those expectations. These requirements should be accommodated within the integrated approach and the scope of the IMS requirements. The emphasis should be on the customer satisfaction and customer from for quality, the worker for occupational health and safety, society for environment, etc.

The organization should establish, implement and maintain a process to determine any legal requirements relating to its activities, products and services that are relevant to the scope of the management systems. These requirements should be taken into account (and any compliance necessary) when establishing, implementing and maintaining its MSS. The organization should communicate relevant information on legal and other requirements to persons working under the control of the organization and other relevant interested parties (see Figure B. 1)."

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

Die interessierten Parteien sind natürliche oder juristische Personen, die zur Wertschöpfung der Organisation beitragen oder auf andere Weise an den Tätigkeiten der Organisation interessiert oder davon betroffen sind.

Das Erfüllen der Erfordernisse und Erwartungen der interessierten Parteien trägt zum Erreichen eines nachhaltigen Erfolgs der Organisation bei.

Darüber hinaus sind die Erfordernisse und Erwartungen der einzelnen interessierten Parteien unterschiedlich, sie können im Widerspruch zu denen anderer interessierter Parteien stehen oder können sich sehr schnell ändern. Die Mittel, durch die die Erfordernisse und Erwartungen der interessierten Parteien ausgedrückt und erfüllt werden, können eine große Formenvielfalt, einschließlich Zusammenarbeit, Kooperation, Verhandlung, Auslagern, annehmen oder auch das Beenden einer Tätigkeit sein."

Auch DRS 20 (Lageberichterstattung (vgl. die Punkte 3, 37 und 59 des DRS 20), OECD Richtlinien für Corporate Governance u.v.m enthalten ähnliche Forderungen.

Ebenso läuft es mit allen anderen Standardkomponenten (vgl. den „Katalog der Komponenten eines Standards")

Weitere Beispiele:

Unternehmensanalyse:

Auch die Forderung nach Durchführung einer **Unternehmensanalyse (organization's internal context)** findet sich in nahezu jedem Standard. Diese als einzelne darstellbaren redundanten Anforderungen sind jeweils nur ein einziges Mal (!) abzuarbeiten.

Weiteres Beispiel:

Prozessabläufe:

Jede Überwachungsfunktion (Controlling / Risikomanagement / Compliance / Audits / Revision / etc.) verlangt **dokumentierte Prozessabläufe**, die diverse Anforderungen (effektiv, qualitativ, rechtssicher, technisch sicher, effizient, etc.) erfüllen.

Ein einziges **Prozess-Audit** kann den erforderlichen Soll-/Ist-Abgleich durchführen und - z. B. via Einstellung der Ergebnisse in einen Datenraum mit ausgewählten Zugangsberechtigungen - alle genannten / involvierten Funktionen informieren.

Einsparungspotenzial:

Hinweis:
Bei der Vielzahl der aufgeführten Überwachungsmaßnahmen gibt es **eine riesige Überschneidung und damit enormes Einsparungspotenzia**l, wenn z.B. durch eine zentrale Funktion – abgestimmt mit den übrigen Themengebieten – die immer wieder gleichen Checks (Dokumenten-,/ Prozess-,/ workflow-Prüfungen / Interviews / etc.) durchgeführt und die Erkenntnisse verteilt werden.

Eine noch bessere Möglichkeit, **den Überwachungsaufwand erheblich zu reduzieren:**

Mitarbeiter, die eigenverantwortlich vernünftig, zuverlässig und motiviert arbeiten!

Da **Zielabweichungen** jedoch nicht nur von Mitarbeitern, die sich nicht „vernünftig" verhalten, verursacht werden, sondern **auch von anderen Einflüssen** (z.B. Umsatzrückgang durch Umfeldentwicklungen), hat das Steuerungs- und Überwachungssystem in diesen Bereichen die herausfordernde Aufgabe**, entsprechende Entwicklungen frühzeitig zu erkennen und Gegensteuerungsmaßnahmen aufzuzeigen.**

Schließlich sollten **Überwachungs- und Kontrollmaßnahmen soweit wie möglich automatisiert** werden, um nicht unverhältnismäßig personelle Ressourcen bei gleichzeitiger
Fehleranfälligkeit menschlichen Verhaltens zu binden:

So können **Standardabweichungen** gut maschinell festgestellt und an geeignete Mitarbeiter zur Überprüfung der Ursachen und Durchführung von Maßnahmen zur künftigen Fehlervermeidung ausgesteuert werden.

Datenräume für die „interested parties":

Neu, aber sicher sehr sinnvoll – und bereits von zahlreichen Unternehmen praktiziert – ist es, einen **Datenraum mit den üblicherweise von allen internen und externen „interested parties" überschneidend gewünschten Informationen**, z.B. geordnet nach Funktions- oder Themenbereichen einzurichten. Zugehörige – sorgfältig ausgewählte – Dokumente sind ebenfalls einzustellen. Anschließend bekommen die zu autorisierenden Interessenten exklusive **Zugangsberechtigungen**, nachdem sie entsprechende Geheimhaltungserklärungen unterzeichnet haben. Beispielsweise können (positive) externe Auditergebnisse / Zertifikate / Mitarbeiterwissensbilanz, Kennzahlen etc. eingestellt werden. Damit würden keine Betriebsgeheimnisse preisgegeben, sondern **positive PR** betrieben.

Die vielen redundanten und analogen Anforderungen / Komponenten lassen sich auch wunderbar einem aus den diversen sehr ähnlichen gängigen Standards der diversen „Überwacher-Welten" komprimierten **„Universal-Kombi-Standard („on demand")** zuordnen (und mit einem **„Kombi-Zertifikat**" testieren):

„(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System, statt unzähliger „Inseln“ am Beispiel „Compliance-Managementsystem“

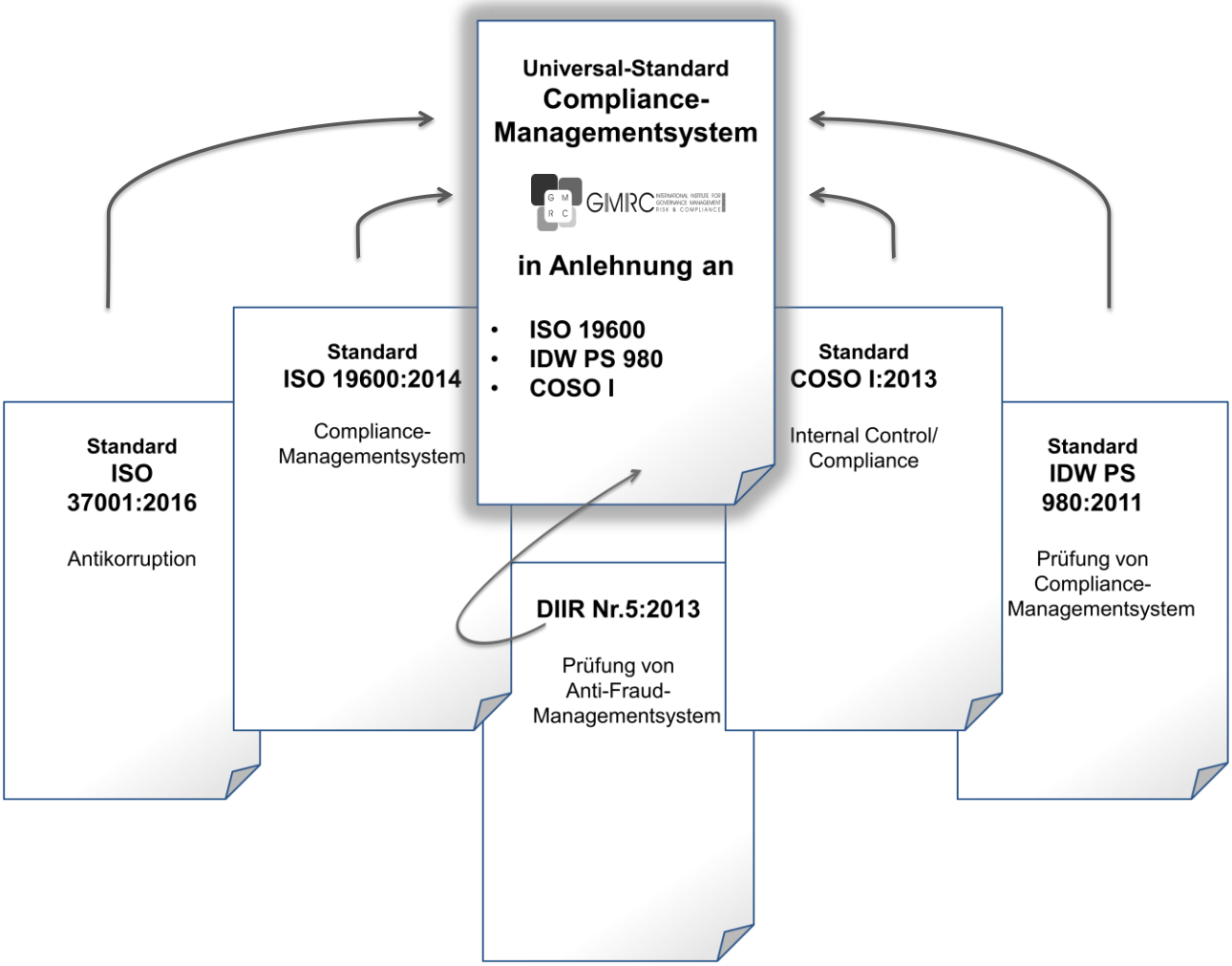


Abbildung 8: „(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System statt unzähliger „Inseln“ (1)

Hier: Die vielen – sehr ähnlichen – Standards diverser Anbieter (ISO / COSO / IDW / DIIR / etc.) werden auf *einem einzigen* (Themen-)Universal-Standard „verschmolzen“. Dieser „Universal-Standard“ bringt also inhaltlich eigentlich nichts Neues, sondern strukturiert, versucht, die jeweils beste Formulierung abzubilden und verweist über Synopsen auf die jeweiligen Fundstellen in den kommerziellen Standards (vgl. www.gmrc.de / Universal-Standard).

„(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System statt unzähliger „Inseln“ am Beispiel Risiko-Managementsystem

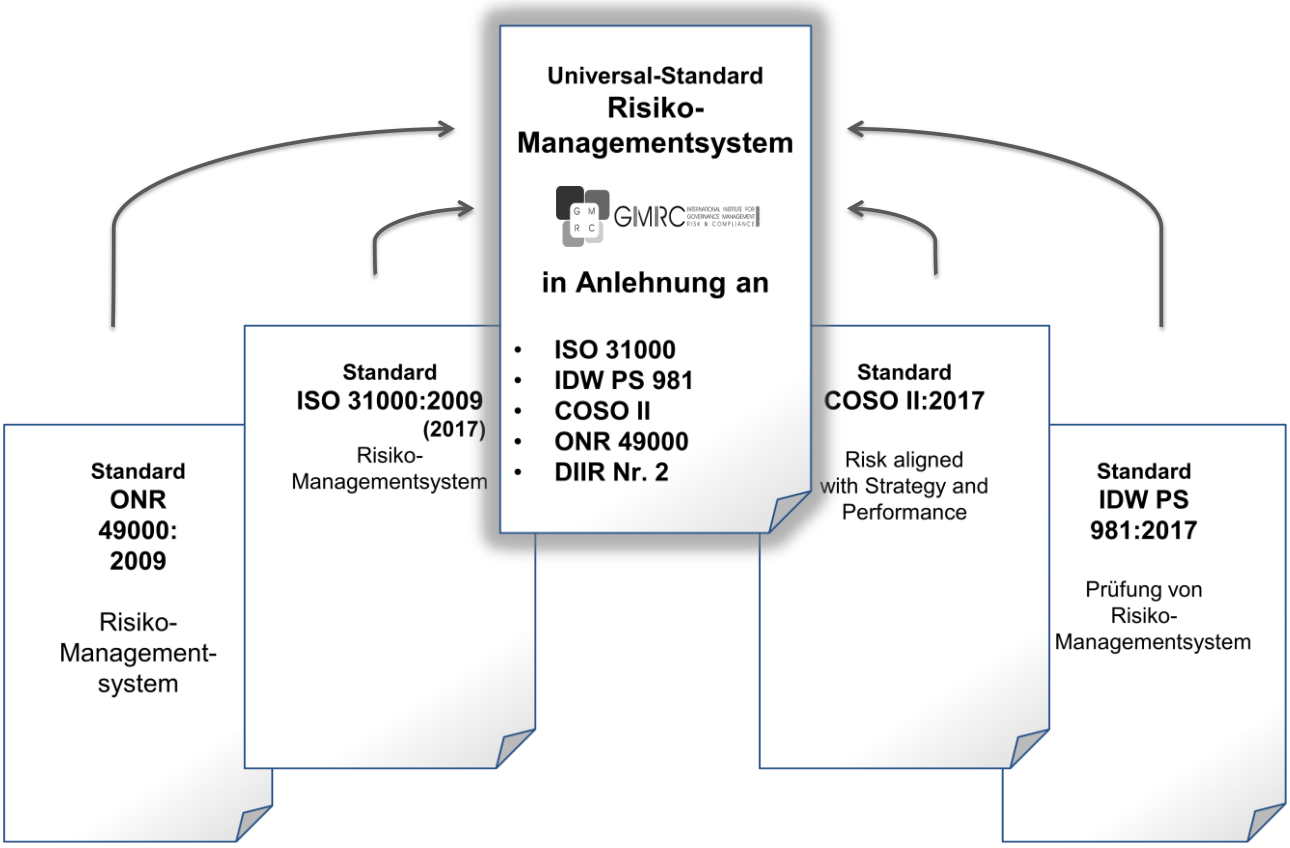


Abbildung 9: „(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System statt unzähliger „Inseln“ (2)

Vgl. oben: auch hier Verschmelzung: Diverse Risiko-Managementsystem-Standards auf *einen einzigen* Rsiko-Managementsystem-Universal-Standard

„(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System statt unzähliger „Inseln“ am Beispiel Revisions-Managementsystem

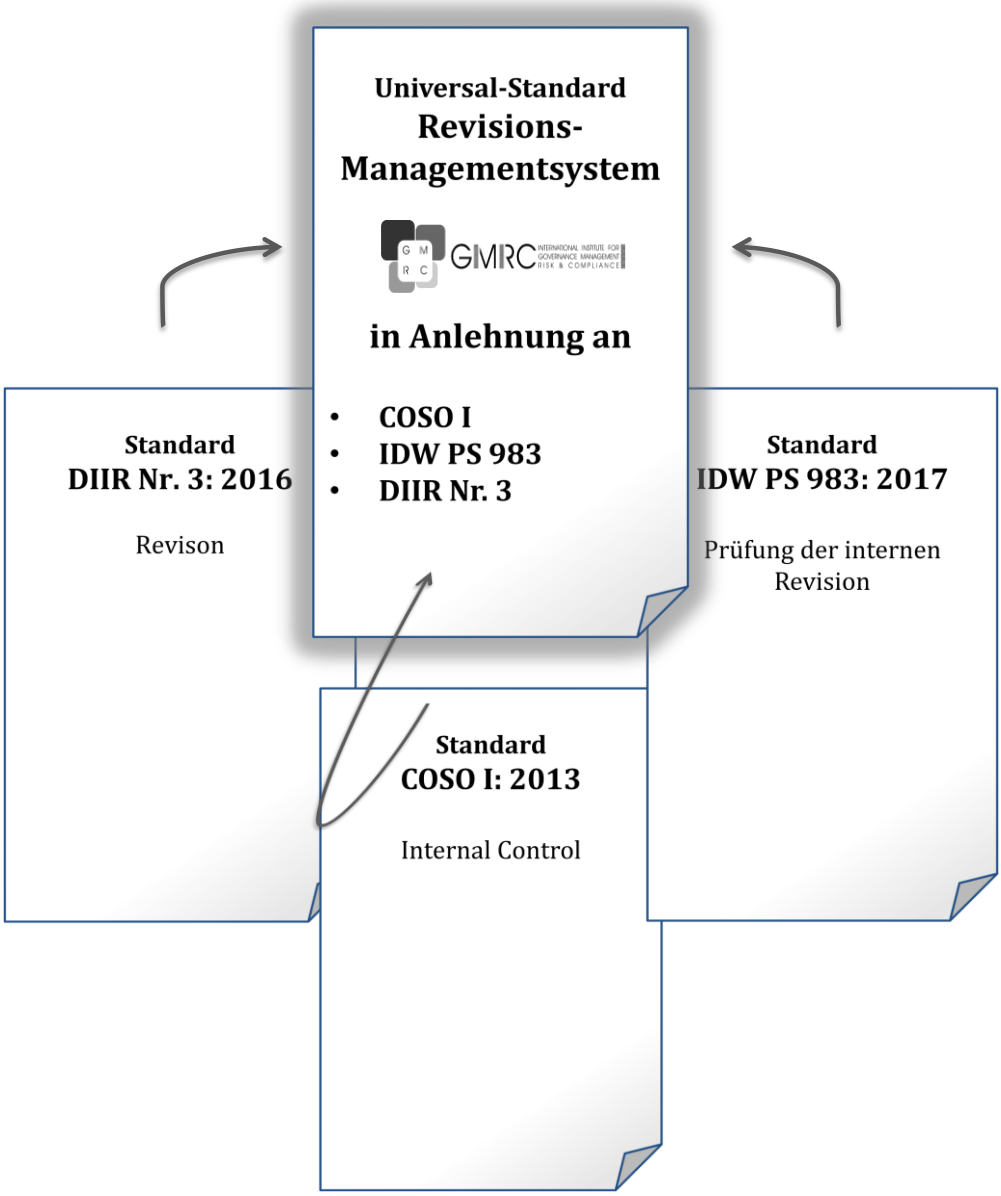


Abbildung 10: „(Kombi-) Universal-Standard und „Kombizertifikat“ für ein integriertes System statt unzähliger „Inseln“ (3)

Vgl. oben: auch hier Verschmelzung: Diverse Revisions-Managementsystem-Standards auf *einen einzigen* Revisions-Managementsystem-Universal-Standard

Dadurch ließe sich viel sparen:

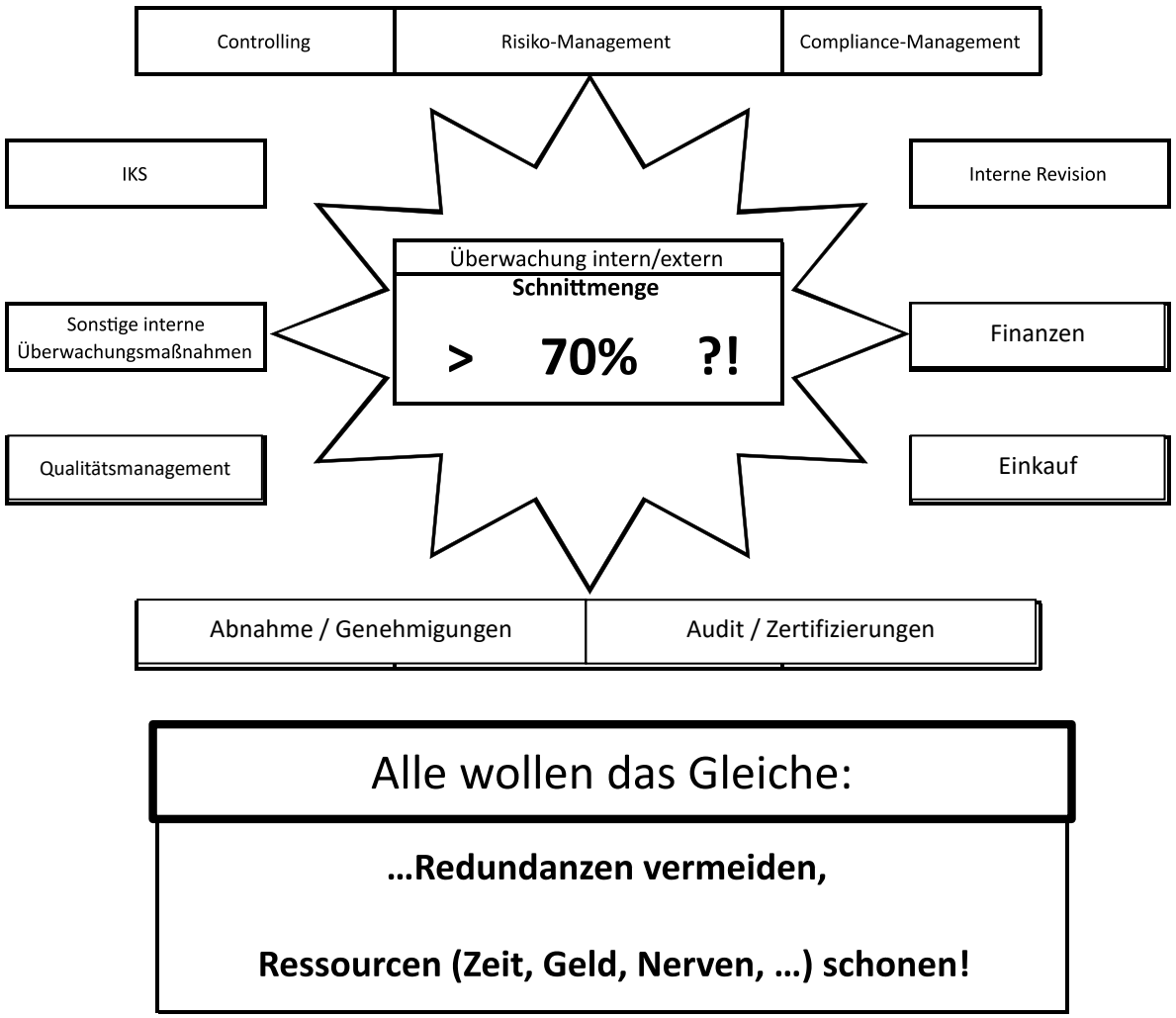


Abbildung 11: Schnittstellen und Einsparungspotenzial im Steuerungs- und Überwachungsmanagement.

Diese Methode bietet sich nicht nur für „Steuerungs- und Überwachungs-System-Inseln“ an, sondern für alle „Managementsystem-Inseln“:

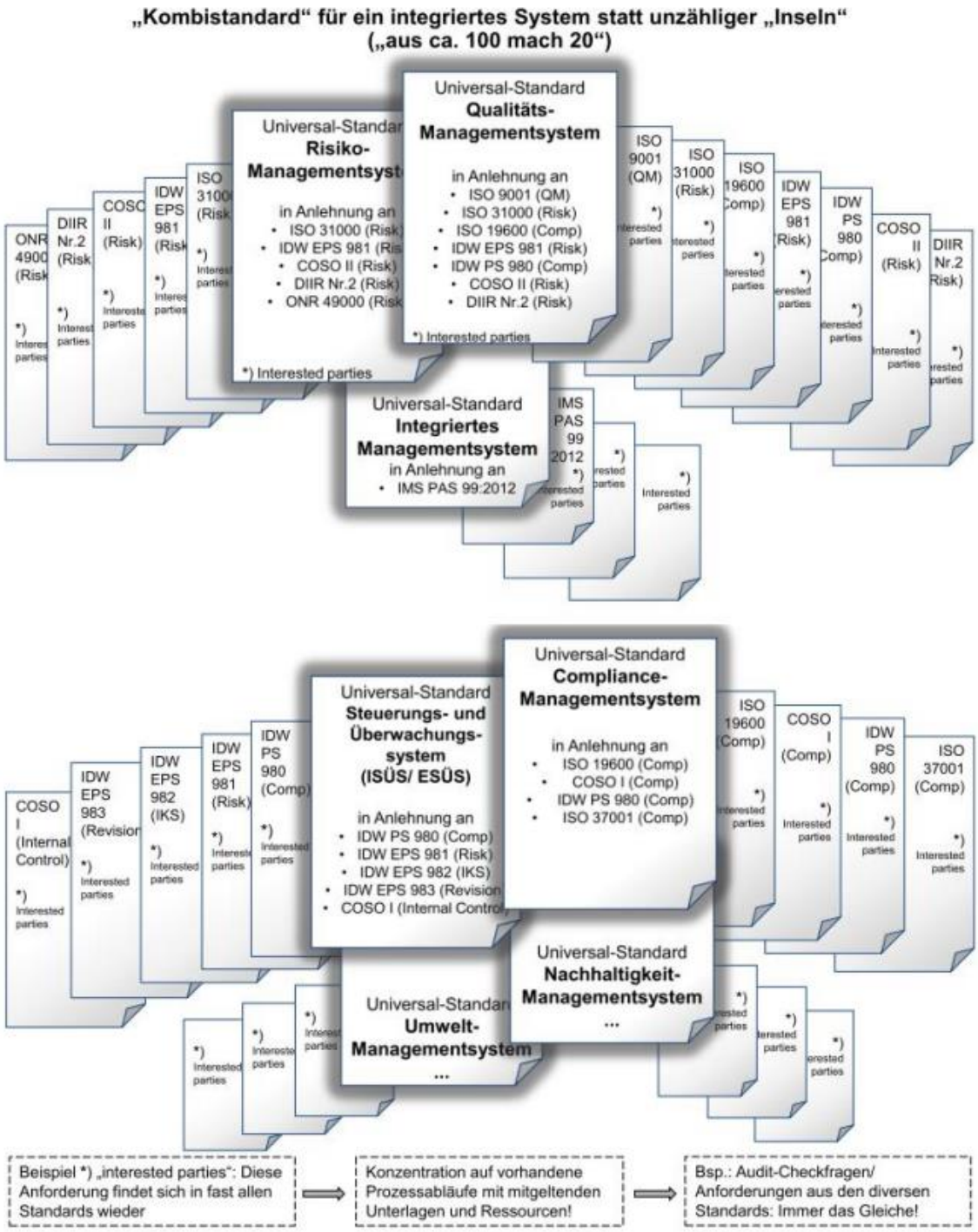


Abbildung 12: Kombistandards („aus 100 mach 20“).

Da die vielen Überwachungsfunktionen viele redundante Referenzgrößen und Standards benutzen, lassen sich diese zunächst (prozess-)themenbezogen (z. B. für ein Risiko- oder Compliance- oder Qualitäts- oder Personal-Managementsystem) von mehreren einzelnen (prozess-)themengleichen Standard auf einen N.N.-Universal-Standard komprimieren.

Ebenso ist sogar die „Komprimierung" unterschiedlicher (Prozess-)Themen-Standards auf einen „Meta-Kombi-IMS-Universal-Standard" „on demand" („welche Managementsystem-Inseln sollen verschmolzen werden?") möglich: Sowohl für die Implementierung, aber auch die Auditierung und Zertifizierung.

„(Kombi-) Universal-Standard und „Kombizertifikat" für ein integriertes System statt unzähliger „Inseln" („aus 20 mach 1")

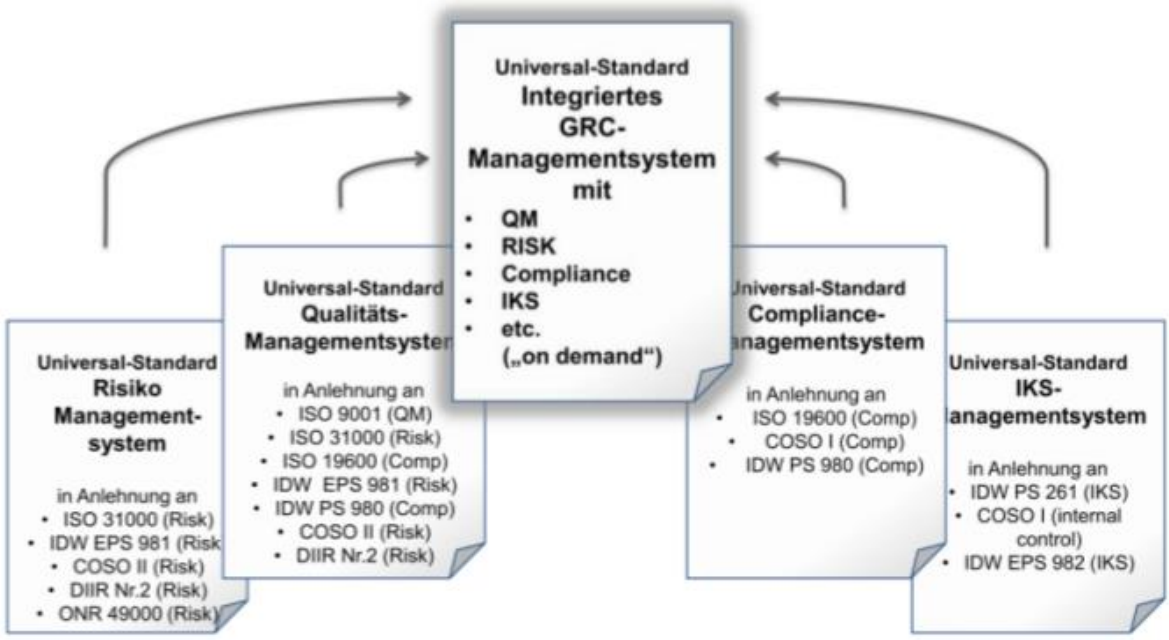


Abbildung 13: (Kombi-) Universal-Standard und Kombistandard-GRC-Managementsystem („aus 20 mach 1").

17. Exkurs: [34] Wollen diese Transparenz nicht auch andere „interested parties“ des Delegations-empfängers? Viele Fliegen mit einer Klappe schlagen!

Die vielen „Welten der vielen Überwacher“ im „lines of defense“-Modell: „Einer arbeitet - 20 überwachen!“

"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 und Zielvereinbarung)	Bericht/ Reporting an Aufsichtsrat und Gesellschafter
2nd line	Controlling	Controller	Konzeptionierung/ Implementierung/ Wirksamkeit	Soll-Ist-Abgleich, Kennzahlenermittlung, usw.	Controlling-Standards	Reporting
	IKS (rechnungslegungsbezogen)	Wirtschaftsprüfer	Konzeptionierung/ Implementierung/ Wirksamkeit	Soll-Ist-Abgleich, Kennzahlenermittlung, usw.	IDW PS 261 IDW E PS 982	Testat/ Bericht
	Compliance	Compliance-Officer	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	IDW PS 980? ISO 19600? COSO I?	Bericht/ Reporting an Aufsichtsrat und Geschäftsleitung
		Wirtschaftsprüfer	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	IDW PS 980	Testat
		Externer Zertifizierer	Konzeptionierung/ Implementierung/ Wirksamkeit	Dokumentenprüfung/ Beobachtung/ Interviews	in Anlehnung an ISO 19600 (nicht zertifizierbar) ISO 37001 (Anti-Korruption)	Zertifikat
		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	?	?

[34] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2. Auflage, 2017, S. 300 + 301

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!	Recherche in unterschiedlichen Formen: bis hin zu "whistle blowing"; auch: Daten entwenden und veröffentlichen (Edward Snowden); Investigativer Journalismus: z.B. Einschleusen (Wallraff); Interviews (Mario Barth) usw.	z.T. anhand von Gesetzen, Standards, good/ best practice, z.T. völlig frei	medial: TV Radio Internet Presse Youtube 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.)
	...					
	...					

Abbildung 14: „Welten der Überwacher": Mehr als 20 (!) Funktionen wollen das Gleiche!

18. Ergebnis: IMS beim Delegationsempfänger: Gut für alle!

Ein integriertes Managementsystem on demand beim Lieferanten mit Zertifizierung bringt Transparenz und ist effizient für *alle*!

19. Wie bekommt der Delegierende / Auftraggeber das?

Z.B. über Qualitätssicherungsvereinbarungen:[35]

Sinn von Qualitätssicherungsvereinbarungen (QSV) ist es, zur regeln, wer von den Beteiligten welche Pflichten **in Bezug auf Qualitätssicherung und Sonstiges** hat, wann diese Pflichten als verletzt gelten und wie der Schaden zu verteilen ist; darüber hinaus sollen QSV helfen, Produktfehler und sonstige Pflichtverstöße zu vermeiden.

QSV sind in aller Regel Rahmenverträge, Gegenstand sind oft Kauf- und Werklieferverträge. QSV können bei mehrfacher Verwendung Allgemeine Geschäftsbedingungen (AGB) darstellen und unterliegen damit der AGB-Kontrolle der §§ 305 ff. BGB.

Die Qualitätssicherungsvereinbarung muss nicht nur abgeschlossen, sondern auch durchgeführt werden. Die konkreten Maßnahmen der Durchführung sind dabei am besten in Anhängen anzugeben. Dabei kann es neben den Qualitätssicherungsmaßnahmen, Warenausgangskontrolle und deren Dokumentation auch um weitere Pflichten und Nachweise zu sonstigen Themen (Compliance, Risikomanagement, etc.) gehen.

Zur Überprüfung der ordnungsgemäßen Durchführung muss dem Besteller das Recht eingeräumt werden, Audits durchzuführen.

Unbedingt muss auch geregelt werden, wie im Falle von Qualitätseinbrüchen **oder sonstigen Pflichtverstößen** verfahren werden soll.

Die kaufmännische Untersuchungs- und Rügeobliegenheit kann allenfalls bei bestehenden Qualitätssicherungsvereinbarungen ausgeschlossen werden. Dann muss beim Käufer aber zumindest eine Kontrolle anhand des Lieferscheins und auf erkennbare Transportschäden erfolgen.

Auch über Haftungsbegrenzungen (Achtung: Kontrolle anhand der §§ 305 ff. BGB möglich) und Verpflichtungen zum Abschluss von Haftpflichtversicherungen sollten Qualitätssicherungsvereinbarungen Aussagen enthalten.

Haftungsbegrenzungen sind lieferantenfreundlich. In der Regel werden daher keine Haftungsbegrenzungen diesen Ausmaßes, sondern Haftungsverteilungen vorgenommen. Zu denken ist dabei insbesondere an Haftungsfreistellungsklauseln, Beteiligung an Rückrufaktionen, etc.

[35] Vgl. *Scherer* at al., Wer den Schaden hat …, 2004, S. 29 -31

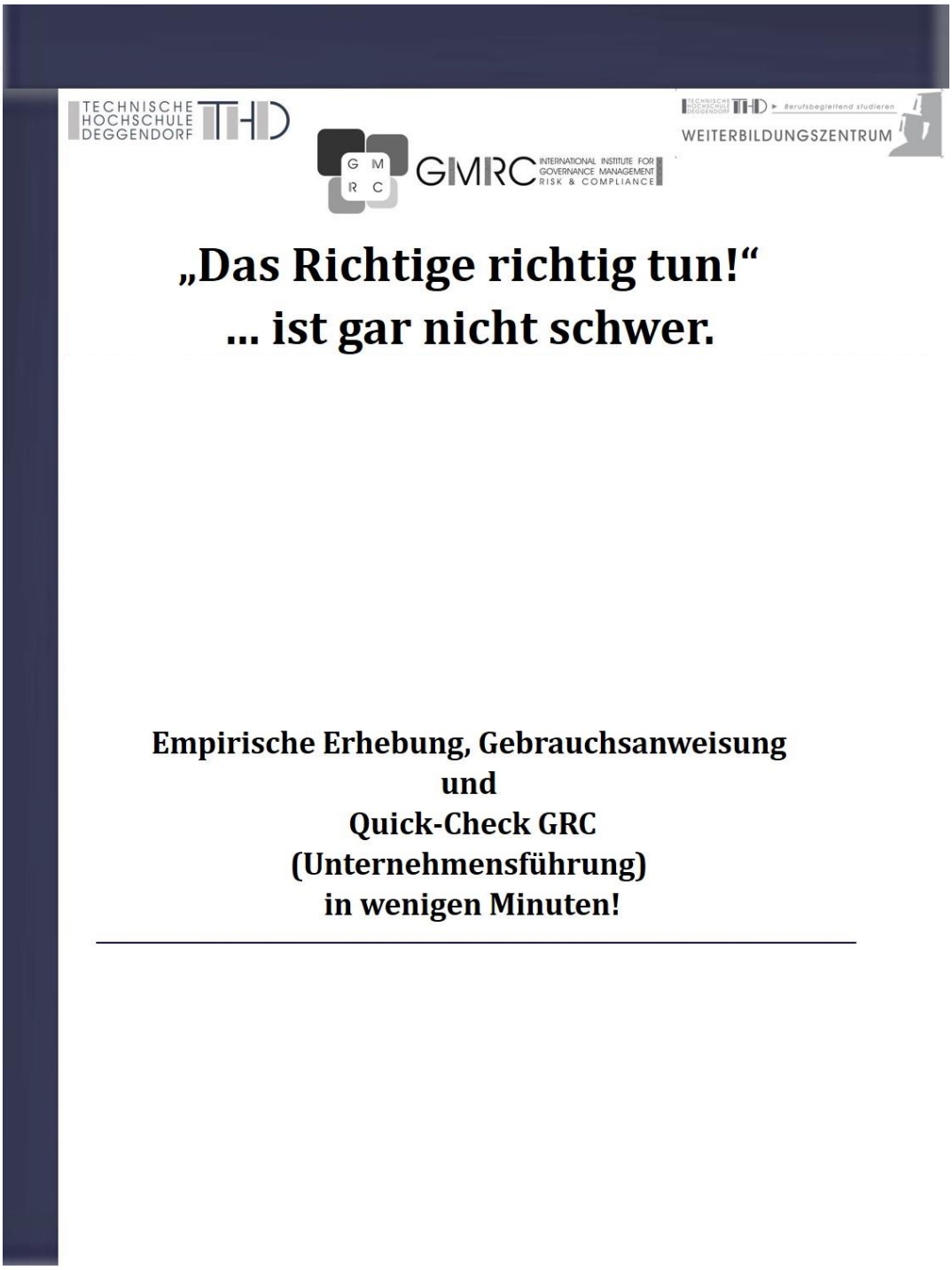
Tipps:

Jegliche vertragliche Risikoerhöhung gegenüber der gesetzlichen Haftungslage, zum Beispiel das Zugeständnis des Verkäufers, auf § 377 HGBzu verzichten, Verjährungsfristverlängerungen, etc. sind unbedingt mit dem Produkt-Haftpflichtversicherer abzustimmen. Ansonsten droht der Verlust des Versicherungsschutzes. Am besten ist es, sich derartige Risikoerhöhungen schriftlich absegnen zu lassen.

Die Dauer der QSV sowie Gerichtsstandsvereinbarungen, bei Auslandskontakt eventuell auch Rechtswahlklauseln sollten ebenfalls aufgenommen werden.

20. Beispiel für eine erste Risiko-Einschätzung beim Lieferanten / Delegationsempfänger

GRC-Quick-Check-Broschüre: Kostenlos anfordern bei josef.scherer@th-deg.de



21. Win Win für Kunden und Lieferanten[36]

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)*

Der Wertbeitrag stellt sich als **Differenz zwischen Aufwand und Nutzen dar**. Der ***Aufwand*** lässt sich oft sehr gut und eindeutig in Euro-Werten feststellen. Der tatsächliche **ideelle und finanzielle Nutzen** ist dagegen schwieriger zu benennen:

Ein positiver Wertbeitrag kann erst ab einem gewissen **Reifegrad** erreicht werden. Bei der Einführung eines z.B. **GRC-, Risk- oder Compliance-Managementsystems** ist entsprechend des Fortschritts entlang der P/D/C/A-Phase Reifegrad, Pflichterfüllungsgrad und Wertbeitrag zunächst im negativen Bereich und wächst kontinuierlich bis zur Sättigungsgrenze ins Positive (vgl. oben).[37]

Die Messung des Nutzens eines Integrierten Managementsystems erfolgt idealerweise zunächst (qualitativ) in einer verbalen Darstellung, die auch für eine weitere Sensibilität sorgt. Den verbal dargestellten **positiven Auswirkungen werden** anschließend **Geldbeträge (Zahlungsströme) zugeordnet**, wobei zu beachten ist, dass Wertbeiträge nur jeweils einmal in den verschiedenenThemenbereichen zur Verfügung stehen, also nicht mehreren Funktionen zugleich zugeschrieben werden können. Hier kann es zu „Verteilungsdiskussionen" kommen.

Die Messung des Wertbeitrages eines Integrierten Managementsystems ist komplex, aber methodisch möglich.

Ein anschauliches **Beispiel zur** (häufig als nicht durchführbar bezeichneten) **Messbarkeit von Wertbeiträgen** im Bereich GRC:

Bei einem direkt an den Hersteller liefernden Automotive-Zulieferer wurde auf Initiative der zuständigen Verantwortlichen für u.a. **Risikomanagement im Einkauf** bereits 2010 der Lieferantenmanagementprozess in Zusammenarbeit mit dem Verfasser um das ***Lieferantenausfall*****-Risikomanagement** angereichert. Die Motivation lag in den durch zahlreiche Lieferanteninsolvenzen und -krisen verursachten Kosten im Millionenbereich p.a. Durch Implementierung des *Lieferantenausfall*-Risikomanagements mit einem überschaubaren Aufwand wurden diese Kosten (für Verlagerungen, Zahlungen an Insolvenzverwalter, etc.) auf einen Bruchteil p. a. reduziert: *Messbarer* (finanzieller) Nutzen!

Ein hoher Wertbeitrag des Risikomanagements im Einkauf, der die Nachhaltigkeit des Unternehmens fördert und zeigt, dass Führung und Mitarbeiter den „Puls der Zeit" erkannt haben und sich am fortschrittlichen „*Stand*

[36] Vgl. *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance, 2017, S. 319 + 320
[37] Vgl. zum Thema Reifegrad auch die Anlagen zur ISO 9004, das COBIT-Reifegradmodell und viele weitere Abhandlungen zu diesem aktuellen und wichtigen Thema

der Technik“[38] orientieren. Dieses Projekt wird über eine vom Verfasser betreute Dissertation zum Thema *„Wertbeitrag von Risiko- und Compliancemanagement am Beispiel von Supply-Chain-Management*“ wissenschaftlich begleitet.

Auch ***Achleitner***, eine Koryphäe im Bereich private equity und investment, ist der Ansicht, dass **„Corporate Governance ein wichtiger Werttreiber“** wird/ist: [39]

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

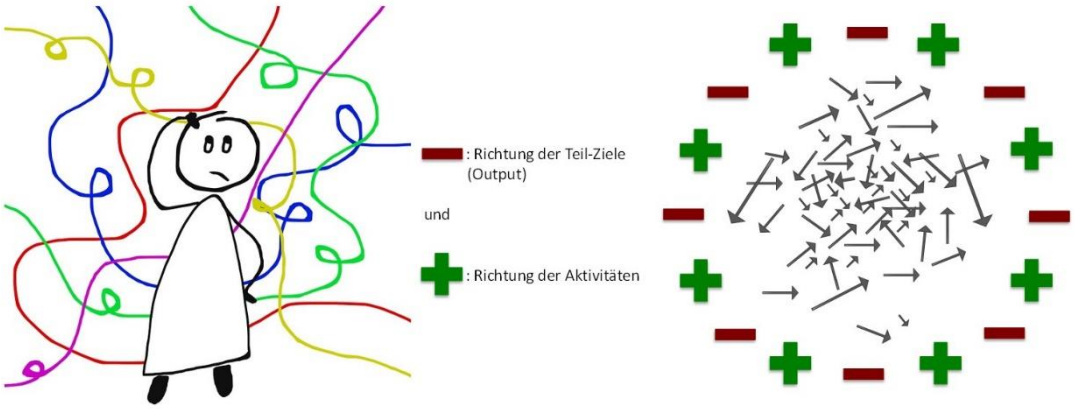
Eine gute Corporate-Governance-Praxis wird ein entscheidender Wettbewerbsfaktor in der Zukunft** (…) aus der Beteiligungspraxis hören sie, **dass es Fälle gibt, in denen die Corporate Governance zwei Drittel der Wertsteigerung der Firmen beisteuert. (…)“

[38] Vgl. *Scherer/Fruth*, Governance-Management, Band 1, 2014, Kap. 1.3. ff.
[39] *Achleitner*, TU München, (Entrepreneurial Finance), Handelsblatt, 30.06.2015, S. 28.

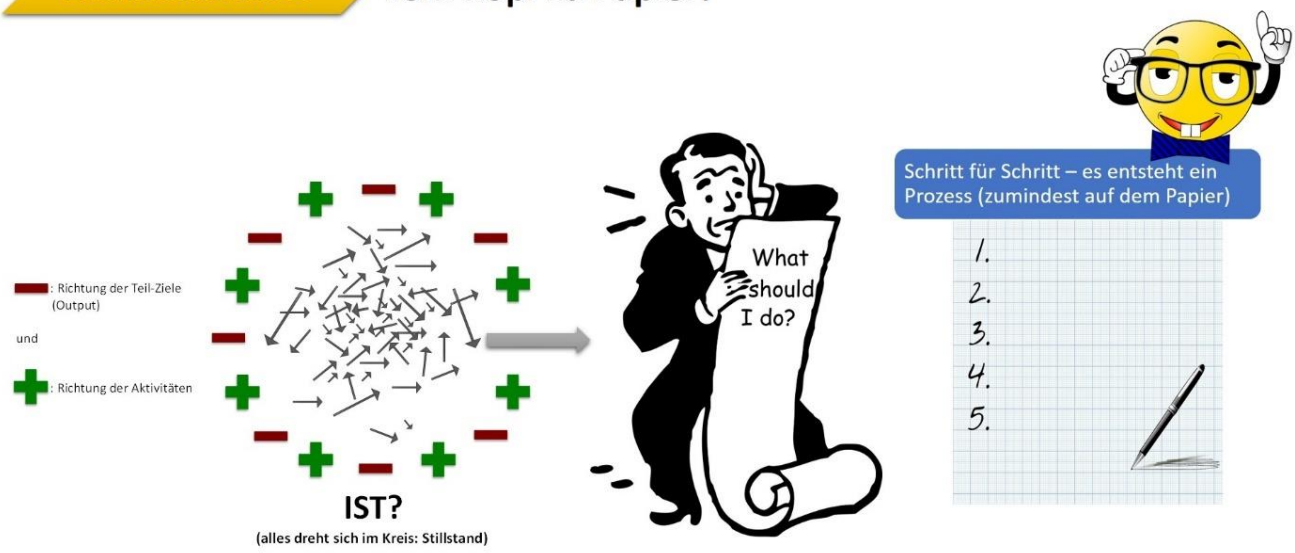
22. Ausblick: Digitalisierte Prozesse, Workflow Management mit ausgewählten Zugangsberechtigungen zu Datenräumen.

22.1 Die Evolution des Prozessmanagements *(Pasini)*

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

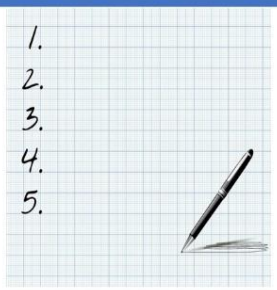


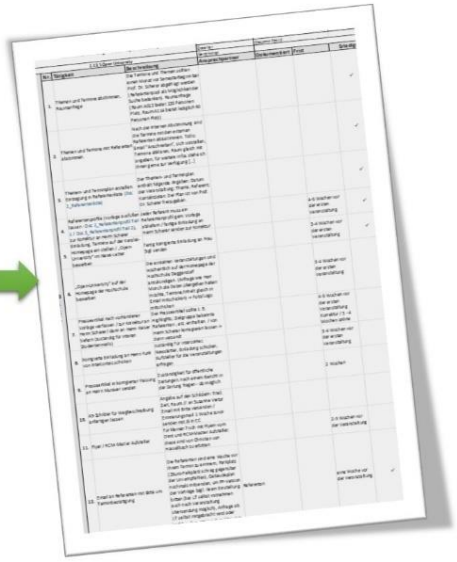
Evolutionsstufe 2 **Vom Kopf zu Papier!**



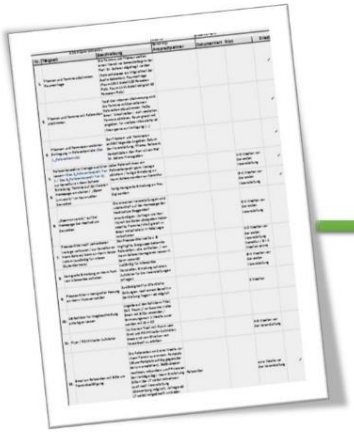
Evolutionsstufe 3 Vom analogen Papier zum digitalen Dokument/Tool!

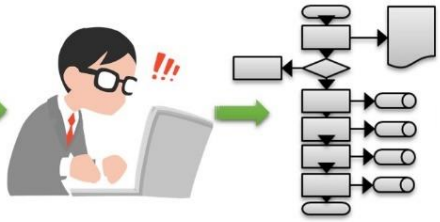
Handschriftlich dokumentierte Prozessschritte

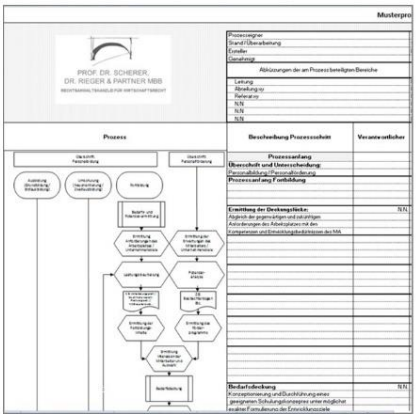




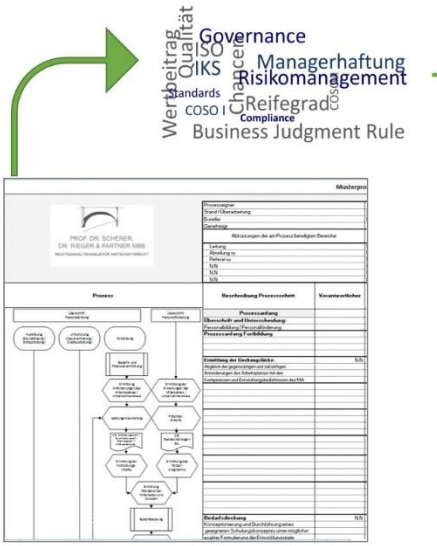
Evolutionsstufe 4 „Super Idee“ – Wieso nicht die Prozessschritte visualisieren!? Und dann auch noch alle relevanten Informationen, den einzelnen Prozessschritten anhängen!?

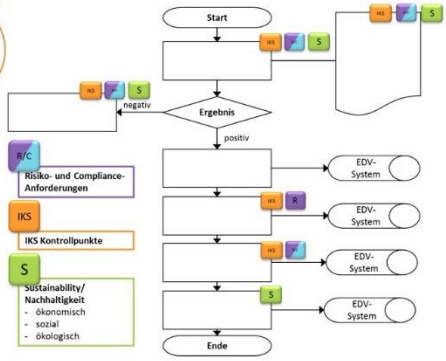




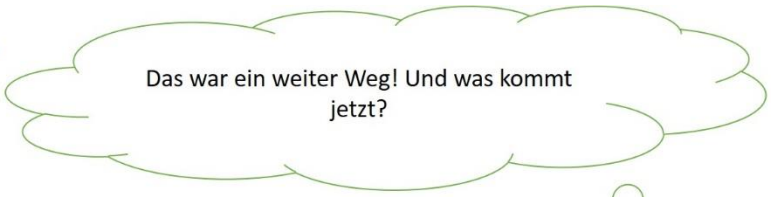


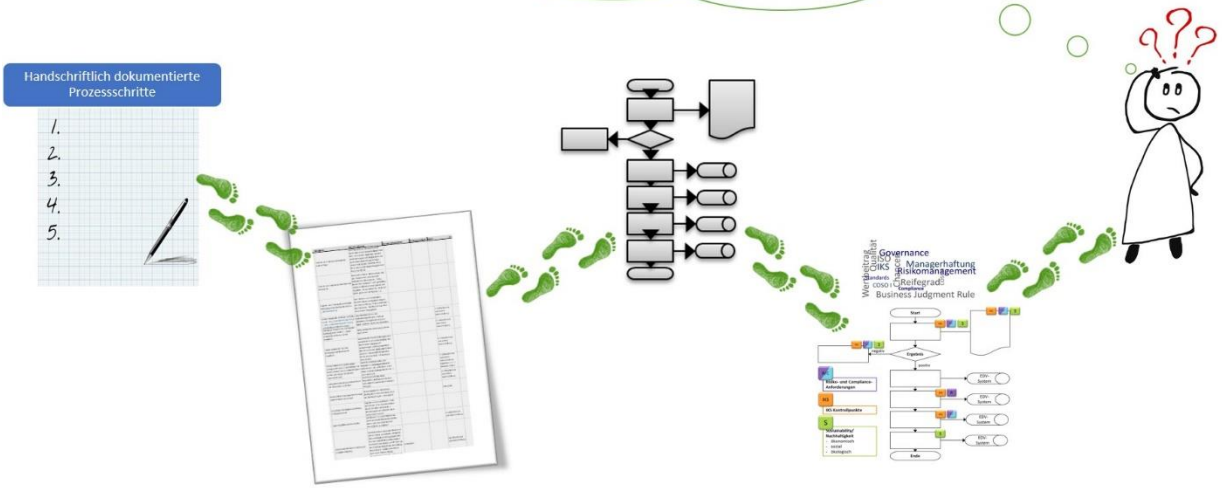
Evolutionsstufe 5 Angereicherte Prozesse? Wieso denn nicht?



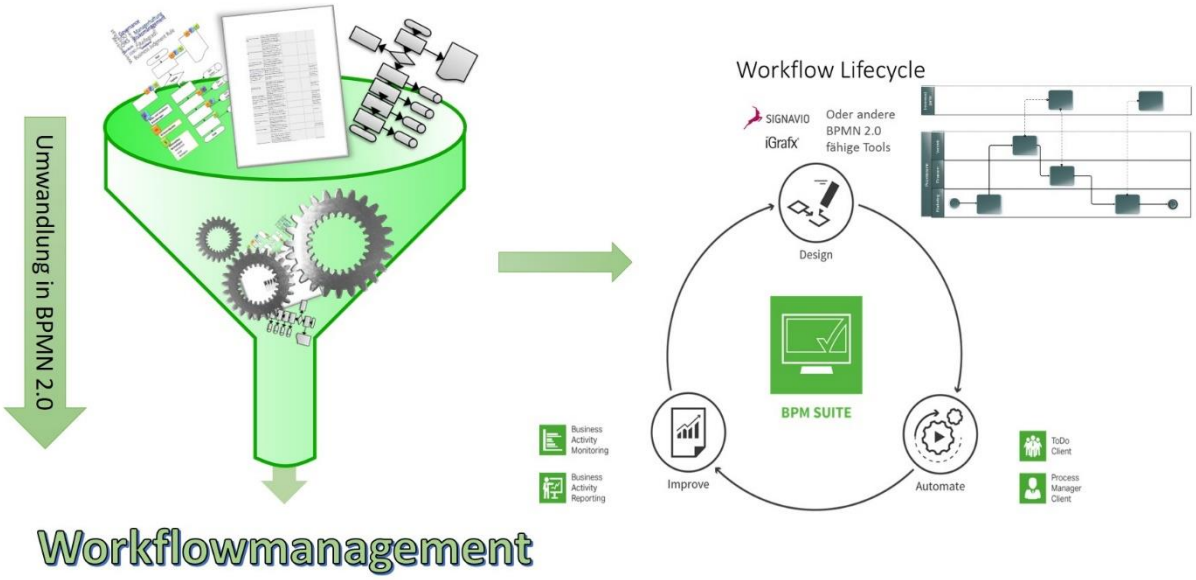


Evolutionsstufe ?





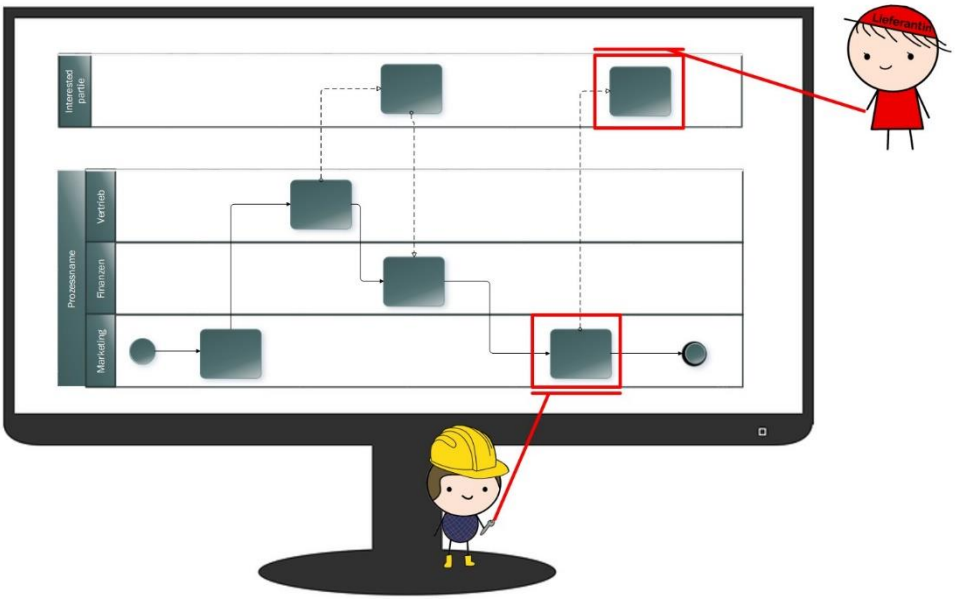
Evolutionsstufe 6 Den Prozess zum „Leben“ erwecken!



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!



22.2 Workflow Management-Prozesse mit Auswertungen, die Transparenz für Unternehmen und Business Partner ermöglichen: (In Zukunft möglicherweise) sogar in Echtzeit! *(Ludacka)*

Workflow-Management[40]

Einleitung

Die Praxis zeigt, dass Prozesse in vielen Unternehmen mit E-Mails, MS Office und mit Papierformularen gelebt werden. Die modellierten Prozesse, die im besten Fall bereits verbindlich für die Mitarbeiter definiert wurden, geraten dabei in den Hintergrund. Wie kann ein Unternehmen also Aktualität und Nachverfolgbarkeit der Prozesse sicherstellen?

Die Modellierung der Prozesse und das Erstellen von prozessbegleitenden Formularen („mitgeltende Unterlagen" z.B. Checklisten, Musterformulare, (IT-)Tools, etc.) **muss so einfach sein, *dass der Fachbereich seine Prozesse selbst verwalten kann*.** Eine übergeordnete Instanz, wie zum Beispiel das Qualitätsmanagement des Unternehmens, ist nicht agil genug, um der Dynamik der Prozesse gerecht zu werden. Eben aber diese Flexibilität sämtliche Änderungen sofort und selbst umsetzen zu können, ist der Schlüssel zu einem gelebten Prozessmanagement.

Allerdings ist das reine Design der Prozesse nicht ausreichend. **Solange diese nur im Intranet oder einem Handbuch schlummern**, ist eine Auskunft zu einzelnen Vorgängen oder Kennzahlen nur mit unverhältnismäßig hohem Aufwand oder gar nicht möglich.

Wenn die Prozesse aber im Sinne des „Human Workflowmanagement" ausführbar gemacht werden, ist die Einhaltung der Vorgaben durch die Verantwortlichen garantiert.

Die **Digitalisierung der Prozesse** ermöglicht darüber hinaus eine unternehmensinterne Informationslogistik. Konkret bedeutet das, dass E-Mails nur an diejenigen verteilt werden, die wirklich betroffen sind und dass Informationen prozessorientiert bereitgestellt werden. Nachverfolgbarkeit und Monitoring von Prozesskennzahlen sind dabei Nebenprodukte, die im Workflowmanagement als selbstverständlich erachtet werden.

Der Workflow Lifecycle

Im Bereich der „Human Workflows" geht es primär darum, Menschen durch den Prozess zu führen und sicherzustellen, dass der organisatorische Ablauf im Vordergrund steht. Diese ablaufkontrollierten Prozesse eignen sich besonders, **wenn der Faktor Mensch für die Prozesstreue maßgeblich ist.** Wenn man den Menschen und nicht die Daten in den Vordergrund stellt, ist es einfach möglich, Geschäftsprozesse End-to-End abzubilden und dabei die bestehende Organisation nicht zu vergessen. Mit diesem Ansatz bildet ein „Human

[40] Vgl. *Ludacka,* in *Scherer / Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit Governance, Risk & Compliance,2. Auflage, 2017, S 88 - 92

„Workflowmanagement System“, die organisatorische Klammer um die bestehende IT-Landschaft. Systeme, die im Prozess eine Rolle spielen, werden punktuell eingebunden, um die Effektivität im Prozessablauf weiter zu steigern. Man stößt in Prozessprojekten aber nicht ständig auf die Grenzen einzelner Systeme, sondern hat die Möglichkeit, den Prozess ganzheitlich zu betrachten und gleichzeitig zur Ausführung als Workflow zu bringen. **Die bereits vorhandene IT-Landschaft, wie z.B. SAP, Microsoft Sharepoint, etc., wird über Schnittstellen punktuell eingebunden** und ergänzt somit den Human Workflow.

Im Gegensatz dazu standen bisher technische und hoch integrative Workflows, die sich auf Transaktionen und Datenoperationen konzentrieren. Die Fachlichkeit des Prozesses geht dabei verloren und die Hoheit liegt bei der IT Abteilung. Die Konsequenz daraus ist, dass die IT eines Unternehmens mit Anforderungen aus den Fachbereichen überschüttet wird und die Fachabteilung selbst in die Abhängigkeit der Geschwindigkeit der IT gerät.

Aufgrund der sich immer schneller verändernden Vorgaben ist eine **compliance-konforme Arbeitsweise** oftmals nicht gewährleistet.

Der „Workflow Lifecycle“ greift die Ansätze der „Human Workflows“ auf und gliedert sich dabei in 3 verschiedene Phasen, die an den Plan/Do/Act/Check Zyklus angelehnt sind, siehe Abbildung.

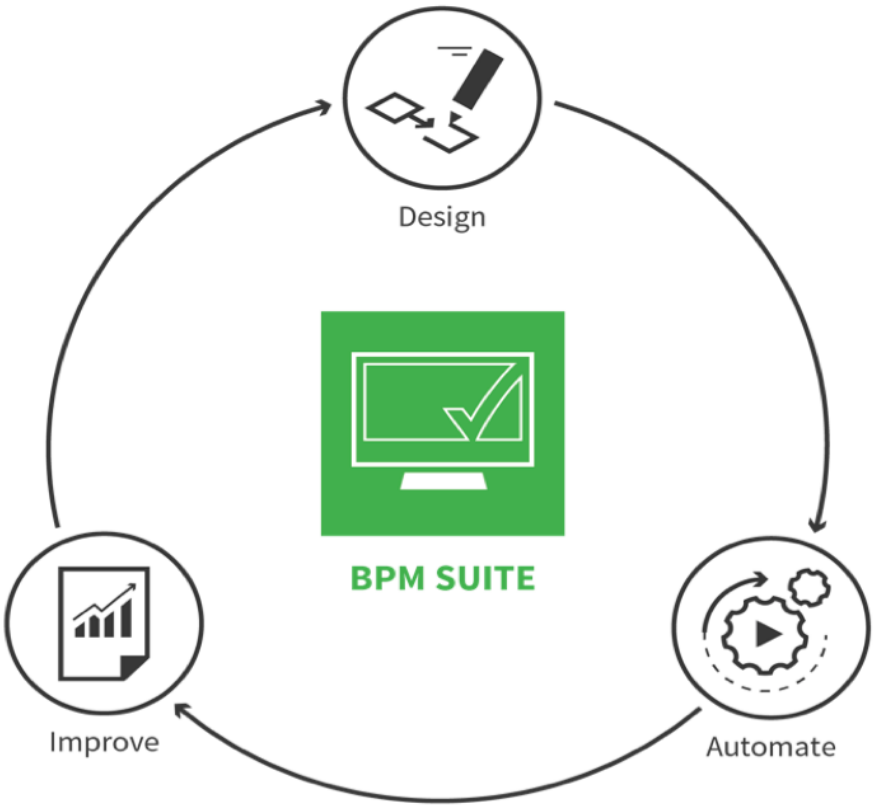


Abbildung 15: Der Workflow Lifecycle

Die Phasen “Design”, “Automate” und “Improve” beschreiben die Modellierung, die Ausführung und Optimierung des Prozesses. Dieser Lifecycle kann iterativ durchlaufen werden und stellt damit den gelebten kontinuierlichen Verbesserungsprozess (Plan/Do/Act/Check Zyklus) dar.

Phase „Design“ des Workflow Lifecycles

In der Phase „Design“ des Workflow Lifecycles geht es darum, alle Elemente des Workflows zu definieren und zu erarbeiten. Im Fokus steht hier zuerst der eigentliche Prozess, der als Prozessmodell abgebildet werden muss. Dabei wird auf jeden organisatorischen Bereich Rücksicht genommen, der im Prozess eine Rolle spielt. Der Prozessverlauf definiert Arbeitspakete und Kommunikation zwischen den Prozessbeteiligten. Im Prozess wird sämtliche Fachlichkeit abgebildet, jedoch wird gleichzeitig die Workfloworientierung berücksichtigt. Mit der Workfloworientierung ist gemeint, dass im Prozessmodell nicht sämtliche Aktivitäten abgebildet werden *müssen,* da man mit Hinblick auf das System modelliert, in dem der Workflow zukünftig ablaufen wird. So ist es beispielsweise nicht zwingend nötig, sämtliche Kommunikationsflüsse zwischen Akteueren bildlich darzustellen, wenn beispielsweise eine Informationsmail versendet wird. Auch die Abbildung einer fachlichen RACI Matrix ist bei der Darstellung eines Workflows nicht erforderlich, sondern dient eher zur vorhergehenden Prozessanalyse. Die Akteure werden schließlich vollautomatisch in den Kontext des Prozesses eingebunden.

Ein Prozessmodell mit Anspruch auf Automatisierung sollte einerseits fachlich nachvollziehbar und andererseits nicht mit technischen Details überfrachtet sein. Die **BPMN 2.0** erfüllt diesen Anspruch derzeit so, wie keine andere gängige Industrienorm. Andere Modellierungsnotationen, wie beispielsweise die EPK (Ereignisgesteuerte Prozesskette) oder die UML (Unified Modeling Language) erfüllen diesen Anspruch nicht gleichermaßen, da der Fokus entweder zu fachlich oder zu technisch ist. Ein UML Diagramm ist beispielsweise von einem Fachanwender nicht lesbar. Der EPK Darstellung hingegen fehlt es an Symbolik für technische Details.

Darüber hinaus ist es essentiell wichtig, dass es nur ein einziges Prozessmodell gibt, in dem Fachlichkeit und Technik gleichermaßen abgebildet werden. Sobald ein fachliches Prozessmodell in ein technisches Prozessmodell übersetzt werden muss, damit es ablauffähig wird, steht man vor den üblichen Problemen zwischen Fachbereich und IT. Die Orientierung an einem Prozessmodell löst diese Bremse und begünstigt zudem die agile Vorgehensweise des Workflow Lifecycles.

Die Digitalisierung von Geschäftsprozessen bedarf nicht nur einer Abbildung des ausführbaren Prozessmodells, sondern auch einer Informationslogistik während des Prozessablaufs. Die Informationen, die während eines Vorgangs für den Prozessbeteiligten sichtbar sind, sollten auf das Wesentliche reduziert werden. Gleichzeitig sollten Informationen möglichst einmalig elektronisch erfasst werden, ehe man sich **in den aktuell vorherrschenden Wildwuchs an E-Mails und begleitenden Dokumenten begibt**. Mit der Digitalisierung von Geschäftsprozessen ist nämlich nicht der Transfer von Papierformularen zu digitalen Formularen gemeint. Vielmehr geht es darum, **Informationen gezielt an diejenigen weiterzugeben, die an einem bestimmten Prozessvorgang beteiligt sind** und aktuell ein Arbeitsergebnis, auf Basis dieser Informationen, erbringen müssen. Dies widerspricht der **aktuellen Arbeitskultur der großen Emailverteiler und stundenlangen Abstimmungsmeetings.**

Um das gerade eben Erläuterte zu erreichen, bedarf es eines prozessbegleitenden Formulars, das logisch mit dem darunterliegenden Prozessmodell verbunden ist. Sprich der Informationsgehalt muss sich dem aktuellen

Prozessschritt und den involvierten Prozessbeteiligten anpassen. Gleichzeitig müssen Auswahlmöglichkeiten im Formular den darunterliegenden Prozessverlauf direkt beeinflussen können. Die Informationen steuern also den Prozess und umgekehrt. Die Erstellung eines solchen Formulars muss weitgehend per Konfiguration erfolgen, damit man innerhalb des Workflow Lifecycles agil bleibt. Einfache Änderungen müssen ohne Programmierung stattfinden, damit Fachbereiche auch größtenteils unabhängig von der IT optimieren können.

Zur Phase „Design" gehört aber auch die Berücksichtigung der bereits vorhandenen IT-Infrastruktur. Die Systeme, die Informationen zu den Prozessen zusteuern, gilt es optimal in den Prozessverlauf einzubinden. Diese Drittquellen, z.B. SAP oder Warenwirtschaftssysteme, können einerseits eine Rolle im Prozessablauf spielen, andererseits rückt auch hier das prozessbegleitende Formular wiederum in den Vordergrund. Die vorhandene IT-Landschaft wird üblicherweise durch typische Aktionen, wie „Erstellen", „Lesen", „Aktualisieren" und „Löschen" eingebunden. Auf diese Art und Weise ist es möglich Geschäftsprozesse End-To-End abzubilden ohne vor Systemgrenzen Halt machen zu müssen. Ein Produktentstehungsprozess beispielsweise kann in einem ERP- (Enterprise Resource Planning), DMS- (Document Management) oder PLM- (Product Lifecycle Management) System nicht gesamtheitlich abgebildet werden, da mindestens zwei der Systeme involviert sind. Diese oder weitere Systeme in reiner Dunkelverarbeitung ohne Prozessorientierung miteinander zu verbinden, löst typische Probleme wie Prozesstreue, Transparenz oder Termintreue nicht.

Phase „Automate" des Workflow Lifecycles

Ab sofort wird die theoretische Herangehensweise verlassen und der modellierte Prozess wird zum Leben erweckt. Ab hier befindet man sich auf der untersten operativen Ebene der theoretischen Welt einer übergeordneten Prozesslandschaft. Der Human Workflow Ansatz greift nun und stellt die prozessorientierte Arbeitsweise sicher.

Jeder Prozessschritt, der vorab modelliert wurde, wird nun tatsächlich an die verantwortlichen Prozessbeteiligten verteilt. Jeder organisatorische Bereich, der vorab als Swimlane modelliert wurde, wird nun tatsächlich zur Rechenschaft gezogen. Prozesszeiten, die man sich vorab theoretisch überlegt hat, gelten ab sofort als echte Liegezeit zur Erledigung eines Prozessschritts. Arbeitsanweisungen müssen nicht mehr in dicken Handbüchern nachgeschlagen werden, sondern werden rollenspezifisch und punktuell angezeigt. Vorgangsbezogene Informationen befinden sich nicht mehr an vielen unterschiedlichen Orten, sondern werden zentral abgelegt oder zumindest zentral referenziert. Antworten auf Fragen wie, „Wo steht der Prozessvorgang gerade?", müssen nicht mehr per Telefon oder Abstimmungsmeetings beantwortet werden. Informationsbedürftige werden automatisch informiert oder haben ab sofort genug Transparenz geschaffen, um sich ohne Abstimmung selbst informieren zu können. Compliance ist kein Sorgenkind mehr, sondern wird durch dynamische Einbindung von Komponenten zur Erfüllung der Anforderungen aus Gesetz / Rechtsprechung / intern verbindliche Regeln / Richtlinien (z.B. Zuwendungsrichtlinien, Datenschutzrichtlinien, etc.) sowie „Anerkanntem Stand von Wissenschfat und Praxis" und ggf. (Industrie-)Standards wie ISO / COSO / IDW / etc. sichergestellt. Auch die ersehnte Prozesstreue ist kein Wunschtraum mehr, da man die Ebene des theoretischen Prozessmodells verlässt. Eskalationen werden nicht mehr in Dezibel gemessen, sondern werden automatisch über zuvor definierte Eskalationswege eingeleitet. Prozessschritte können tatsächlich parallelisiert werden und Folgeschritte werden erst dann aktiv, wenn sämtliche Arbeitsergebnisse vorliegen.

Phase „Improve“ des Workflow Lifecycles

Welche Erkenntnisse erlangt man, wenn man einen Prozess als Human Workflow gesamtheitlich lebt? Mit dieser Frage beschäftigt sich das folgende Teilkapitel und rundet damit den Workflow Lifecycle ab.

Zunächst einmal erhält man tiefe Einblicke in die Kennzahlen der tatsächlichen Prozessvorgänge. Wenn ein Prozess nämlich nur anhand eines Prozessmodells und organisatorischen Bordmitteln, wie E-Mails, Dokumente und Abstimmungsmeetings gelebt wird, kann darüber keine verlässliche Auskunft gegeben werden. Mit diesen unzuverlässigen Informationen werden oftmals zyklische Prozessoptimierungen vorgenommen, jedoch bleiben diese auf theoretischer Ebene. Anhand von Bauchgefühlen lassen sich keine Prozessoptimierungen vornehmen, sondern nur anhand von Kennzahlen des gelebten Prozessgeschehens. Mit der Auswertung von Kennzahlen der Human Workflows ist es möglich, den theoretischen kontinuierlichen Verbesserungsprozess sowie die Anforderungen aus Steuerung und Überwachung in einen gelebten KVP zu wandeln.

Eine typische Kennzahl, die sich rein durch die Automatisierung eines Prozesses ergibt, ist die Prozessdurchlaufzeit. Man erhält nun Einblicke in die Zeiten eines jeden Prozessschritts eines jeden Prozessvorgangs. Auf diese Art und Weise können Engpässe im Prozessverlauf und Schwachstellen bei mangelhafter Termintreue offengelegt werden. Ein SOLL-IST Vergleich ist dabei ein selbstverständlicher Wertbeitrag, der Optimierungspotenzial sichtbar macht. Auch der Vergleich über Monate oder Jahre hinweg legt offen, welche Maßnahmen zu Verbesserungen im Gesamtprozess geführt haben.

Hinzu kommt die Transparenz über sämtliche Prozessvorgänge. Ein Prozessverantwortlicher weiß zu jedem Zeitpunkt über den Status eines jeden einzelnen Vorgangs und dessen aktuellen Bearbeiter Bescheid. Eskalationen laufen automatisch ab, jedoch kann natürlich auch manuell eingegriffen werden, z.B. indem Aufgabenpakete delegiert werden.

Im Gegensatz dazu weiß auch jeder Prozessbeteiligte, was er wann und wo zu tun hat. Darüber hinaus ist durch die transparente Prozessdarstellung gewährleistet, dass jeder Prozessbeteiligte weiß, welche Arbeitsergebnisse bereits vorliegen müssten und wer im Zweifelsfall warten muss, wenn man selbst aus der Zeit gerät. Durch die automatische Priorisierung der offenen Aufgaben nach verbleibender Zeit, ist dem Mitarbeiter zusätzlich Last von den Schultern genommen. Die Transparenz ist also nicht nur für den Prozessverantwortlichen förderlich, sondern auch für die Prozessbeteiligten, die dadurch den Gesamtzusammenhang und Abhängigkeiten besser verstehen können. Schnittstellen zwischen Abteilungen werden sichtbarer und regen zur Diskussion an.

Die Prozesskostenrechnung in Bezug auf die Ressource Mensch kann mit Hilfe von Human Workflowmanagement ebenfalls aufgestellt werden. Zur Erledigung eines jeden Prozessschritts können Angaben zu angefallenen Kosten im Bezug zur aktuellen Aufgabe erhoben werden. Diese Informationen liefern, in Ergänzung zu den materiellen Kosten, einen detaillierten Wertbeitrag zur gesamten Prozesskostenrechnung.

Diese **Kennzahlenerhebung und -analyse** helfen dabei, den Workflow zu plausibilisieren und stetig zu verbessern. Der Übergang in das erneute Überarbeiten des Prozessmodells und des prozessbegleitenden Formulars ist die logische Konsequenz. Wie sonst soll man auf die immer schneller greifenden internen und externen Veränderungen reagieren und gleichzeitig deren Einhaltung garantieren?

Zwischen-Fazit

Die ganzheitliche End-to-End Betrachtung von Geschäftsprozessen und deren Digitalisierung ist einer der wichtigsten Aspekte in einer sich immer schneller drehenden Geschäftswelt. Geschäftsmodelle und -verfahren ändern sich häufiger als bisher und erfordern damit auch eine erhöhte Flexibilität in den Geschäftsprozessen. Der Workflow Lifecycle und eine Technologie wie z.B. *TIM* bieten Unternehmen eine agile Herangehensweise, um komplexe und gleichzeitig flexible Prozesse zu managen.

Anmerkung: Diese mögliche Transparenz über pflichtgemäßes Handeln durch Workflow Management erfolgt revisionssicher unter Wahrung von Beteiligungs- oder Informationsrechten von Betriebsrat oder Personalvertretung sowie der Anforderung des Datenschutzrechts.

23. Fazit:

„Bulletpoints“:

- ☑ **Die Pflicht zu Supplier-screening / Überwachung des Delegationsempfängers ist *rechtlich* nicht neu.**
- ☑ **Neu jedoch sind die zunehmend umfassenderen Anforderungen in Gesetzen und Standards.**
- ☑ **Neu sind auch die organisatorischen Umsetzungen in good-practice-Unternehmen.**
- ☑ **Einige Rechtsgebiete (Sozialversicherungs-, Arbeits- und Strafrecht) und Rechtsanwender (Zoll / Sozialversicherungsträger / Staatsanwaltschaft) verkennen, dass die Erfüllung von Organisationspflichten keine Indizwirkung für Scheinselbstständigkeit oder „betriebliche Eingliederung“ zeitigen kann.**
- ☑ **Ein wirksames (gelebtes) „Integriertes Managementsystem“ beim Delegationsempfänger ist für diesen und für den Delegierenden zugleich effektiv und effizient.**
- ☑ **Eine Bündelung der vielen Überwachungsfunktionen schafft enorme Wertbeiträge.**
- ☑ **Workflow Management ermöglicht dem Delegationsempfänger, aber auch dem Delegierenden revisionssichere Transparenz über pflichtgemäßes Handeln in Echtzeit.**