Scherer / Fruth (Hrsg.)

Die digitale Transformation von Normen, Richtlinien und Standards

- ISO 9001 (2015) (QM)
- ISO 19600 (2014) (Compliance)
- COSO I (2013) (Compliance)
- IDW PS 980 (2011) (Compliance)
- ISO 37001 (Anti-Korruption)
- ISO 31000 (2018) (Risk)
- IDW PS 981 (2017) (Risk)
- IDW PS 982 (2017) (IKS)
- IDW PS 983 (2017) (Revision)
- DIIR Nr. 3 (2016) (Interne Revision)
- PAS 99 (2012) (Integriertes Managemententsystem)

zielführend anwenden!

1. Auflage 2018

GMRC INTERNATIONAL INSTITUTE FOR GOVERNANCE, MANAGEMENT, RISK & COMPLIANCE

Impressum:

Scherer / Fruth (Hrsg.)

Die digitale Transformation von Normen, Richtlinien und Standards

- ISO 9001 (2015) (QM)
- ISO 19600 (2014) (Compliance)
- COSO I (2013) (Compliance)
- IDW PS 980 (2011) (Compliance)
- ISO 37001 (2016) (Anti-Korruption)
- ISO 31000 (2018) (Risk)
- IDW PS 981 (2017) (Risk)
- IDW PS 982 (2017) (IKS)
- IDW PS 983 (2017) (Revision)
- DIIR Nr. 3 (2016) (Interne Revision)
- PAS 99 (2012) (Integriertes Managementsystem)

zielführend anwenden!

1. Auflage 2018
Herausgeber:
Prof. Dr. Josef Scherer

RiAG Klaus Fruth
Frischecker Str. 12, 94065 Waldkirchen

GMRC-Verlag
GMRC-Verlag-GbR
Verlag für Governance, Management, Risk & Compliance
Prof. Dr. Josef Scherer und RiAG Klaus Fruth

Deggendorf 2018

ISBN: 978-3-947301-13-3

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Wichtiger Hinweis:

Diesem Aufsatz „Die digitale Transformation von Normen, Richtlinien und Standards"

liegt das vertiefende Werk
Scherer / Fruth (Hrsg.), „Unternehmensführung 4.0":
Integriertes Managementsystem (IMS) „on demand" mit Governance, Risk und Compliance (GRC),

1. Auflage 2018,
als e-Book (Erscheinungstermin ca. 10/2018) zugrunde.

Scherer

Die digitale Transformation von Normen, Richtlinien und Standards

1. Einführung

Nahezu jedes (Prozess-) Themenfeld eines Unternehmens / einer Organisation, wie z.B. Risiko-, Compliance-, Personal-, Einkaufs-, Vertriebs-, IT-, etc. -Management, ist mittlerweile nicht nur juristisch über Anforderungen aus Gesetzgebung, Rechtsprechung und (internen) Richtlinien infiltriert[1], sondern auch in vielzähligen Standards diverser Standard-Familien (ISO, COSO, IDW, DIIR, etc.) „genormt".[2]

Fast täglich entstehen neue Anforderungen: Im Bereich von Gesetzgebung, Rechtsprechung, Stand der Technik und Richtlinien seien exemplarisch die DSGVO (2018) auf europäischer und das BDSG (2018) auf deutscher Ebene u. a. mit der Forderung, den „*Stand der Technik"* einzuhalten, genannt. Dies zeitigt Auswirkungen auf die interne IT-Asset-Benutzungs-, Informationssicherheits- und Datenschutzrichtlinie.

Der *Bundesgerichtshof* nahm 2017[3] unter Verweis auf wissenschaftliche Literatur ausführlich Stellung zu den Anforderungen an ein enthaftendes Compliance-Managementsystem und das *Bundesverfassungsgericht* stellte 2018 mit einem Beschluss den Anonymitätsschutz bei Compliance-Ombudsleuten vor neue Herausforderungen[4].

Im Bereich der Standards erschien im März 2018 die ISO 31000:2018 für Risikomanagement-Systeme.

Da sie nicht zertifizierbar, etwas „generisch formuliert" und ohne „High Level Structure" strukturiert ist, erarbeitet die Austrian Standards International eine wohl 2019 erscheinende zertifizierbare und sehr pragmatische ausgestaltete ÖNORM 4900 ff..

Das Deutsche Institut für Normung (DIN) als Mitglied der ISO überarbeitet derzeit die ISO 19600 für Compliance-Managementsysteme in Richtung Zertifizierbarkeit und entwirft Standards für „Governance of Organizations" (Unternehmensführung) und Whistleblowing[5].

Neu erschienen 2018 die ISO / DIN 45001 zur Arbeitssicherheit und internationale Nachhaltigkeitsstandards.

Das Institut der Wirtschaftsprüfer in Deutschland komplettierte unlängst die IDW PS-980er-Reihe zu einem „Insel-Paket" für Compliance (PS 980), Risikomanagement (PS 981), Internes Kontrollsystem (IKS) (PS 982) und Revision (PS 983).

Diese Aufzählung ließe sich noch erschreckend erweitern.

---

[1] *Scherer*, Compliance beherrscht die klassische Betriebswirtschaft – Buchbeitrag in: *Scherer/Fruth (Hrsg.),* Anlagenteil zu Governance-Management, Band II (Standard & Audit), 2016.

[2] Vgl. *Scherer*, Die „Welt(en) der Überwacher": Enormes Potenzial für Effektivität, Effizienz und Wertbeiträge bei Governance, Risk und Compliance, FIRM Jahrbuchbeitrag, 2017, S. 79-81 (www.gmrc.de).

[3] Urteil des *BGH* vom 9.5.2017, AZ. 1 StR 265/16

[4] *BVerfG,* Beschluss vom 27.6.2018 – 2 BvR 1405/17, …: Es ging hier um die Rechtmäßigkeit der Beschlagnahme von Akten einer im Zusammenhang mit dem Diesel-Abgasskandal mit internen Ermittlungen beauftragten ausländischen Kanzlei durch die Staatsanwaltschaft.

[5] Der Verfasser ist Mitglied in den genannten Gremien.

All diese Normen, Richtlinien und Standards enthalten Anforderungen an eine pflichtgemäße, gewissenhafte Leitung von Unternehmen und sonstigen Organisationen, sind über Assessments diverser Arten (Testierungen, Zertifizierungen, Audits, internal investigations, Revisions-Prüfungen, etc.) bzgl. Umsetzungsreifegrad zu bewerten und stellen bei Missachtung Haftungsfallen für Management und Mitarbeiter und die Quellen vielfältiger Risiken dar.

Deutlich wird aufgrund dieser kontinuierlichen internen und externen Veränderungen, dass ein starres Organisationssystem zum Scheitern verurteilt ist.

Nur ein äußerst flexibles System, das es ermöglicht, schnell, ohne fremde Hilfe und kostengünstig Prozessabläufe und die vielen damit vernetzten Komponenten einer Organisation an neue Anforderungen anzupassen, kann effektiv sein.

Angemerkt sei, dass Standards nicht die *primäre* Orientierungsgröße für Unternehmen/Organisationen darstellen:

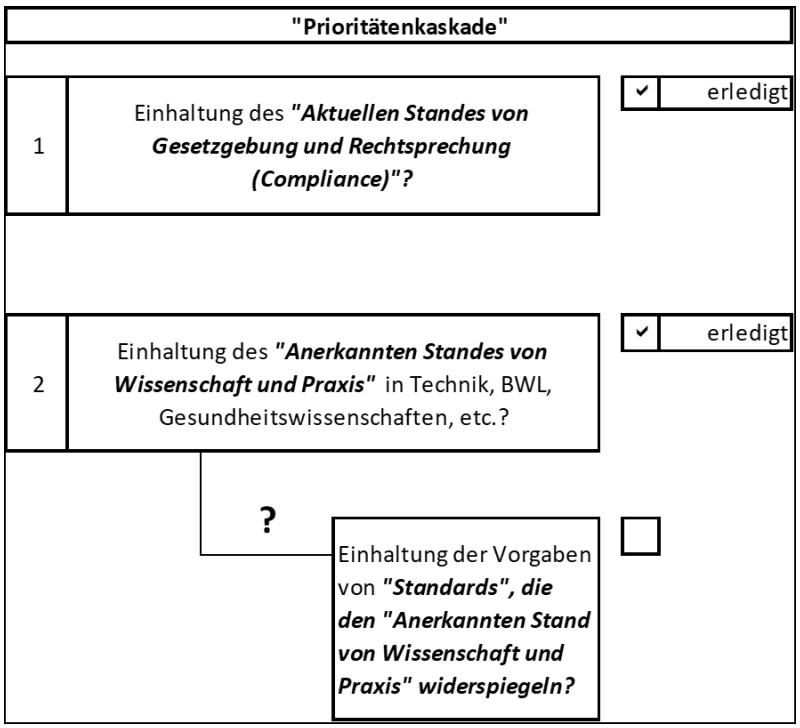


Abbildung 1: Prioritätenkaskade.

Zunächst sind die zwingenden Vorgaben vom Gesetzgeber und Rechtsprechung und ergänzend der „anerkannte Stand von Wissenschaft und Praxis“ maßgeblich, sofern der Gesetzgeber nicht eine höhere Entwicklungsstufe vorschreibt: So wird z.B. im IT-Sicherheitsgesetz, im Bundesdatenschutzgesetz (n. F. 2018) und in der Datenschutzgrundverordnung der „*Stand der Technik*“ als höhere Entwicklungsstufe unter den „Technikklauseln“ gefordert.[6]

[6]Vgl. *Scherer*, Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis“ auf Organhaftung und Corporate Governance – am Beispiel der ISO 19600 (2015) Compliance-Managementsystem, CCZ 2015, S. 9-17 (www.gmrc.de).

Die Abgrenzung von „Stand der Technik“ zu „Anerkannten Regeln“ etc. hat das *BVerfG* geklärt:

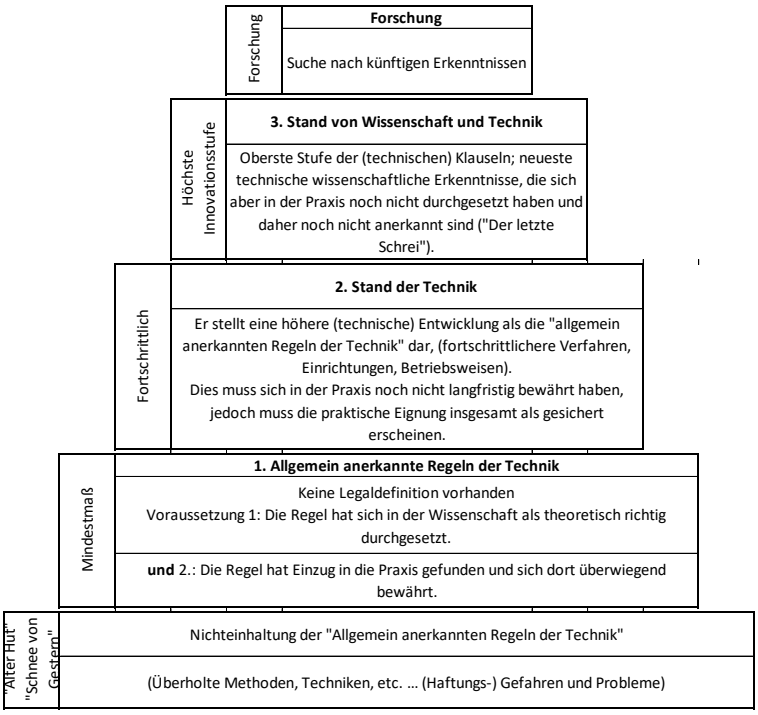


Abbildung 2: Einordnung und Definition von „Technikklauseln“ nach *BVerfG* (Kalkar-Entscheidung)

Sofern Standards den geforderten Entwicklungsstand widerspiegeln oder „strenger“ sind, ist es sinnvoll, sich angemessen an passenden Standards zu orientieren. Falls aber Standards weniger oder gar Widersprechendes zum anerkannten Stand oder Gesetz/Rechtsprechung vorgeben, ist es gefährlich, sie umzusetzen:[7]

Beispiels-Fall: „Eishockey-Puck und Sicherheitsstandards“[8]:

„*Besteht trotz Einhaltung der Vorgaben der maßgeblichen DIN-Normen die naheliegende Möglichkeit, dass (…) Rechtsgüter anderer verletzt werden können, so ist der zur Verkehrssicherung Verpflichtete gehalten, die erkennbare Gefahrenquelle im Rahmen der Zumutbarkeit zu beseitigen, insbesondere dann, wenn die Veranstaltung die nicht nur geringe Wahrscheinlichkeit eines Unfalls mit der Gefahr nicht unerheblicher Verletzungen mit sich bringt.“*

In den Ausführungen des Gerichts finden sich moderne Methoden der Risikobewertung mit den Komponenten „*Eintrittswahrscheinlichkeit*“, „*Erkennbarkeit*“ und „*Schadenspotenzial*“!

[7] Vgl. *Scherer*, Wieviel Standard braucht der Mensch? – Zum Anwendungsbereich von Standards, 2018 (www.gmrc.de).

[8] Hinweisbeschluss des *OLG Nürnberg* vom 6.7.2015, Az. 4 U 804/15.

Ein weiteres **Beispiel**: In Bankenkreisen ist der „Anerkannte Stand von Wissenschaft und Praxis“ wohl schon wesentlich anspruchsvoller, als es die „*MaRisk*“ fordert.

Der Aufbau dieser vielen Standards differiert zum Teil sehr stark, die Inhalte dagegen glücklicherweise weniger.[9]

Um die Anwendung zu erleichtern, entschloss sich die ISO bereits 2012, die sogenannte „*High Level Structure“* (*HLS*) einzuführen:

ISO-Standards für N.N.-Managementsysteme sollten alle einen ähnlichen Aufbau mit 10 Unterpunkten aufweisen[10]:

1. Anwendungsbereich
2. Normative Verweisungen
3. Definitionen, etc.

Etwas anders strukturiert wurde der „*Vier-Block-Aufbau*“ beim *Universal-Standard der „Deggendorfer Schule“* des *Instituts für Governance, Management, Risk& Compliance an der Technischen Hochschule Deggendorf*, da dieser Universal-Standard nicht nur die ISO-Standards, sondern auch COSO, IDW, DIIR, etc. in einem Integrierten Managementsystem (IMS) „on demand“ synoptisch „verschmilzt“. [11]

Welche Struktur nun logischer / sinnvoller / besser für ein Integriertes System geeignet ist, sei an dieser Stelle dahingestellt, da all die existierenden Strukturen *eine gemeinsame Schwachstelle* aufweisen:

Sie sind *streng linear* aufgesetzt (HLS: Punkt 1 bis 10, Universal-Standard: Block 1-4, …) so wie unsere *Denkweise* seit Tausenden von Jahren - unser *Gehirn* selbst jedoch arbeitet nicht linear, sondern vernetzt:

2. Exkurs: Partielle, vollständige und vernetzte Schrift- und Informationssysteme im Wandel der Zeit

2.1. Das erste Datenverarbeitungssystem

Durch die wachsende Komplexität der Gesellschaften nach der „landwirtschaftlichen Revolution“ (vor ca. 10.000 Jahren) kam Daten und Zahlen eine kongruent steigende

[9] Vgl. *Scherer/Fruth* (Hrsg.), Handbuch: Integriertes Managementsystem (IMS) „on demand“ mit Governance, Risk und Compliance (GRC), 2018.

[10] 2018 erschien der sehr prominente ISO-Standard für Risiko-Managementsysteme (ISO 31000:2018) und wies überraschenderweise keine High Level Structure mehr auf.

[11] Vgl. *Scherer/Fruth* (Hrsg.), Universal-Standard Compliance-Managementsystem des International Institute for Governance, Risk & Compliance der Technischen Hochschule Deggendorf, 2016 (www.gmrc.de).

Bedeutung zu. Eine revolutionäre Erfindung für die Menschen dieser Zeit, die sich zuvor noch als Jäger und Sammler keine Zahlen oder dergleichen merken mussten, war die Erfindung der Schrift durch die Sumerer – ein erstes Datenverarbeitungssystem.[12]

2.2. Exkurs: Partielle und vollständige Schriftsysteme

Als „*Technik zur Speicherung und Verarbeitung von Information mittels physischer Zeichen*“[13] wird zwischen vollständigen und partiellen Schriftsystemen unterschieden. *Vollständige* Schriftsysteme ermöglichen es, die gesprochene Sprache nahezu lückenlos wiederzugeben. Exemplarisch seien an dieser Stelle die lateinische Schrift, altägyptische Hieroglyphen oder Braille genannt. *Partielle* Schriftsysteme hingegen sind eher als Zeichensysteme zu betrachten. Mithilfe dieser Zeichensysteme lassen sich „*nur ganz bestimmte Informationen aus klar definierten Bereichen erfassen*“[14], wie zum Beispiel die mathematische Schrift. Die bereits genannte sumerische Schrift war zunächst ebenfalls ein partielles Schriftsystem. Ca. 3000 v. Chr. entwickelte sich daraus die sogenannte Keilschrift zum vollständigen Schriftsystem.

Weitere vollständige Schriftsysteme entstanden beispielsweise in China um das Jahr 1200 v. Chr.[15]

2.3. Datenflut, Archivierung und Auffinden von abgelegten Informationen: Unterschied zwischen der Methodik des Gehirns und der Bürokratie

Die wachsenden Möglichkeiten der Niederschrift brachten jedoch das gleichermaßen steigende Problem der fehlenden / mangelhaften Datenverarbeitungssysteme mit sich. Während im Gehirn unvorstellbare Mengen an Informationen gespeichert[16] und trotz loser Verknüpfungen[17] in Sekundenschnelle abgerufen werden können, sind für ein funktionierendes Datenverarbeitungssystem Kataloge und Ordner-/Suchsysteme sowie Verantwortliche, die sie zu bedienen wissen, von Nöten.[18] Insbesondere Letztere

---

[12] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.155 ff.: *„Damit sprengten die Sumerer die physischen Fesseln des Gehirns […]. Das Datenverarbeitungssystem, das die Sumerer erfanden, nennt sich „Schrift““.*

[13] *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.155 ff.

[14] *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.156 ff.

[15] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.158 ff.

[16] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 164 ff.: *„Niemand weiß, wie wir das schaffen, doch es ist allgemein bekannt, wie erstaunlich effizient die Suchmaschine unseres Gehirns ist. Außer wenn wir versuchen, uns daran zu erinnern, wo wir die Autoschlüssel hingelegt haben.“*

[17] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 164 ff.: *„Die Schreiber lernten […] Techniken zur Erfassung, Suche und Verarbeitung von Information, die sich ganz erheblich von der Denkweise unseres Gehirns unterscheiden. Im Gehirn ist alles lose miteinander verknüpft. […] In der Bürokratie muss dagegen alles klar auseinandergehalten werden.“*

[18] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.164 ff.: *„Um ein funktionierendes Datenverarbeitungssystem zu schaffen, […] waren Kataloge und Suchsysteme erforderlich, und vor allem pedantische Beamte, die sie benutzten.“*

sind für das Funktionieren von Systemen dieser Art entscheidend. Beamten und Buchhaltern wird nachgesagt, sie würden wie Aktenschränke denken, was für die Handhabung der niedergeschriebenen Informationen sehr nützlich sei.[19]

Im Zuge der wachsenden Popularität von Datenverarbeitungssystemen ließ sich jedoch eine Tendenz weg vom natürlichen menschlichen, ganzheitlichen Denken[20] hin zu Bürokratie und Kästchendenken erkennen.[21]

2.4. Unterstützung der „bürokratischen Methode“ durch Erfindung der mathematischen Schrift

Die Entwicklung der partiellen Schriftsysteme hin zu vollständigen Schriftsystemen verringerte die Bedeutung der mathematischen Zeichen als partielles Schriftsystem nicht. Gegenteiliges trat ein: Die mathematische Schrift etablierte sich zur „vorherrschenden Weltsprache“[22]. Nahezu alle Staaten, Unternehmen u.v.m. greifen darauf zurück und können damit jede Information mit beispielloser Geschwindigkeit und Effizienz verarbeiten. Zudem findet eine natürliche Selektion statt, indem Informationen, die sich nicht in die mathematische Schrift überführen lassen, außer Acht gelassen werden – was auf der anderen Seite der Fähigkeit von Regierungen, Organisationen, etc., in Zahlen zu sprechen, neue Bedeutung und Wichtigkeit beimisst.[23]

2.5. *BPMN 2.0* als partielles Schriftsystem für Geschäftsprozess- und Workflowmanagement?

Business Process Model and Notation (BPMN) ist ein Industriestandard, der weltweit zur grafischen Darstellung und Modellierung von Geschäftsprozessen eingesetzt wird. Dabei wird eine logische und grafische Abfolge („partielles Schriftsystem“) einzelner Aktivitäten mit Information mittels physischer Zeichen, die die jeweils gesprochene

---

[19] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.164 ff.: *„Damit das System funktioniert, müssen die Hüter der Schubladen so umprogrammiert werden, dass sie nicht mehr wie Menschen denken, sondern wie Beamte und Buchhalter. Seit frühesten Zeiten weiß jeder, dass Beamte und Buchhalter nicht wie Menschen denken. Sie denken wie Aktenschränke.“*

[20] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.164 ff.: *„Das ist vielleicht die wichtigste Auswirkung der Schrift auf die Geschichte der Menschheit: Ganz allmählich veränderte sie die Denkweise und Weltsicht der Menschen.“*

[21] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.164 ff.: *„Im Laufe der Jahrhunderte wurde der Unterschied zwischen der bürokratischen Datenverarbeitung und der natürlichen menschlichen Denkweise immer größer.“*

[22] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.166 ff.: *„Obwohl die mathematische Schrift immer ein partielles Schriftsystem blieb, hat sie sich zur vorherrschenden Weltsprache entwickelt.“*

[23] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.166 ff.: *„Wer Einfluss auf die Entscheidungen von Regierungen, Organisationen und Unternehmen nehmen will, muss daher lernen, in Zahlen zu sprechen. Experten tun alles, um selbst Vorstellungen wie „Armut“, „Glück“ oder „Ehrlichkeit“ in die Zahlensprache zu übersetzen“.*

Sprache nahezu lückenlos wiedergibt, ergänzt. Durch den Trend der letzten Jahrzehnte, sich wirtschaftlich international auf einige wenige Sprachen zu einigen (chinesisch, englisch, spanisch), kann ein hoher Standardisierungsgrad erreicht werden.

Die einzelnen Aufgaben und Aktivitäten, die innerhalb eines Geschäftsprozesses festgelegt werden, werden als „Tasks“ bezeichnet. Der Durchlauf eines Geschäftsprozesses, bei dem sukzessive Tasks durchgeführt werden, wird durch Entscheidungen („Gateways“) und Kontrollen („Sequenzfluss“) begleitet. Mithilfe dieser Modellierungs-Objekte lassen sich auch mehrere parallele Abläufe erzeugen, die anschließend an passender Stelle synchronisiert und zusammengeführt werden. Sogenannte „Pools“ definieren den Rahmen eines Geschäftsprozesses oder werden zur Darstellung unternehmensübergreifender Prozesse einzelner Geschäftspartner verwendet. Die Zuständigkeiten und Verantwortlichkeiten der Prozessbeteiligten lassen sich mit „Swimlanes“ (Bahnen im Schwimmbad) darstellen. Außerdem können zusätzliche Daten in ein Prozessdiagramm integriert werden, welche die Prozessbeteiligten mit Wissen zu Erfüllung ihrer Tätigkeiten versorgen. Diese Daten bilden eine Basis für Workflowmanagement-Systeme. Neuartige Technologien erlauben die Interpretation der BPMN und der integrierten Daten und ermöglichen damit die Automatisierung der Geschäftsprozesse, auch „(Human-)Workflowmanagement“ genannt. Damit wurde durch die Verbindung von vollständigen und partiellen Schriftsystemen ein neuer Reifegrad im Informationsmanagement erreicht.

2.6. Nutzung der mathematischen Schrift zu „gehirnähnlichen“ Methoden der Vernetzung von Informationen

Einen revolutionären Fortschritt in der mathematischen Schrift stellt das binäre Zeichensystem dar, das nur aus der 0 und der 1 besteht und alle Wörter und Informationen, die in einem Rechner eingegeben werden, in eine bestimmte Aneinanderkettung dieser beiden Ziffern übersetzt.[24] Auf Basis dieses Systems wird im Forschungsgebiet der „Künstlichen Intelligenz“ (KI) versucht, „eine neue Art der Intelligenz zu schaffen“[25].

Auch gerade neu entwickelte „Quanten“-Chips von *Google* schaffen eine noch nie da gewesene Form der Datenverarbeitung.

[24] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.166 ff.

[25] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.157 ff.: *„Aber damit ist das Ende der Geschichte noch längst nicht erreicht. Das Forschungsgebiet der „künstlichen Intelligenz“ versucht inzwischen, eine neue Art der Intelligenz zu schaffen, die nur auf dem binären Zeichensystem der Computer basiert und ganz ohne menschliches Zutun funktioniert. […]“*

3. Von der Menschheitsgeschichte zum vernetzten Alltag im digitalen Zeitalter

Im Bereich Managementsysteme sind wir bisher jedoch noch nicht darauf gekommen, wirklich vernetzt zu denken und zu arbeiten. Auch unsere Unternehmen / Organisationen waren schon immer komplex vernetzte Organismen, wenngleich sie zumeist klassisch linear organisiert geführt wurden.

Seit die Themen „Prozessorientierte Organisation“[26] und „Industrie 4.0“ populär wurden, fällt auf, dass die herkömmlichen Strukturen und Denkweisen nicht mehr in die „4.0-Welt“ passen.

Auch bzgl. der diversen *Komponenten* (z.B. Definitionen, Richtlinien, Kompetenzen, rechtliche Vorgaben, „Tone from the Top“, etc.) eines beliebigen N.N.-Managementsystems ist es für die „*Wirksamkeit*“ (das „Gelebt-werden“) nicht zielführend, wenn diese – wie sehr häufig in der Praxis anzutreffen - in Standards, Handbüchern oder Excel-Tabellen, etc. -streng linear dargestellt- einen „Dornröschenschlaf“ in Schubladen, Intranet oder Wissensdatenbanken abhalten, bis sie ein Auditor oder Wirtschaftsprüfer für die kurze Zeit eines Audits oder einer Testierung vorübergehend scheinbar zum Leben erweckt.

Vielmehr müssten diese Aktivitäten zur Erfüllung der diversen Anforderungen (aus Recht, Stand der Technik oder Standards) so in die Prozessabläufe integriert werden, dass die *Wirksamkeit* gewährleistet (und dokumentiert) ist.[27]

Die Anforderungen an digital transformierte Managementsystem-Standards ist also einerseits, die Inhalte (Anforderungen/Komponenten) verständlich und strukturiert, aber andererseits auch (digital) in Prozessabläufen vernetzt abzubilden.

Dies ist möglich und wird bereits praktiziert, ist damit also „Stand der Technik“:

4. Interpretation der *High Level Structure* der ISO und des „*Vier-Block-Aufbaus*“in Richtung prozessorientierte Organisation

4.1 Der *Vier-Block-Aufbau* der Deggendorfer Schule als Basis für System- und Standard-übergreifende Bewertungen

Der *Vier-Block-Aufbau der „Deggendorfer Schule“* geht davon aus, dass in allen existierenden (QM-, Risk-, Compliance-, Nachhaltigkeits-, Informationssicherheits-, etc.-) Managementsystem-Standards (auch außerhalb von ISO: z.B. bei COSO, IDW, DIIR, etc.) ähnliche Inhalte / Komponenten zu finden sind und versucht, den gemeinsamen Nenner darzustellen:

[26] Vgl. *Scherer/Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk und Compliance (GRC), 2016, S. 89 ff.

[27] *Scherer*, Managerenthaftung und digitale Transformation versus Unvernunft im Lichte aktueller Rechtsprechung des Bundesgerichtshofs, FIRM Jahrbuchbeitrag, 2018 (www.gmrc.de) und *Scherer/Fruth* (Hrsg.), Handbuch: Integriertes Managementsystem (IMS) „on demand“ mit Governance, Risk und Compliance (GRC), 2018.

So findet sich beispielsweise die von Auditoren, Wirtschaftsprüfern, Zertifizierern, QM-, Risk-, Compliance-Beauftragten, Revisioren und vielen weiteren zu prüfende Anforderung, die Ziele der „interested parties“ darzustellen, zu bewerten und gegebenenfalls Maßnahmen abzuleiten, nahezu in jedem Standard:

Die Gegenüberstellung (Synopse) als „*Beweis*“
für die zahlreichen Redundanzen / Analogien

ISO 19600:2014 (Compliance-Management)

„4.2 Understanding the needs and expectations of interested parties“

ISO 37001: 2016 (Antikorruption)

„4.2 Understanding the needs and expectations of interested parties“

IDW PS 980: 2011 (Compliance-Managementsystem)

„5.4.1. Prüfungshandlungen zur Risikobeurteilung

(40) 5.4.1.1. Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens“

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

PAS 99: 2012 (Integriertes Management System)

(Public Available Standard / British Standards Institution)

„4.2 Understanding the needs and expectations of interested parties“

ISO 9001: 2015 (Qualitätsmanagementsystem)

„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien“

ISO 9004: 2017 (Leiten und Lenken für den nachhaltigen Erfolg einer Organisation)

„Interessierte Parteien, Erfordernisse und Erwartungen“

Deutscher Rechnungslegungs Standard Nr. 20 (DRS 20): 2012

((Konzern-) Lageberichterstattung gem. §§ 289, 315, 342 HGB) „3.“/ „37.“/„59.“

COSO I: 2013 (Internal Control / Internes Steuerungs- und Überwachungssystem)

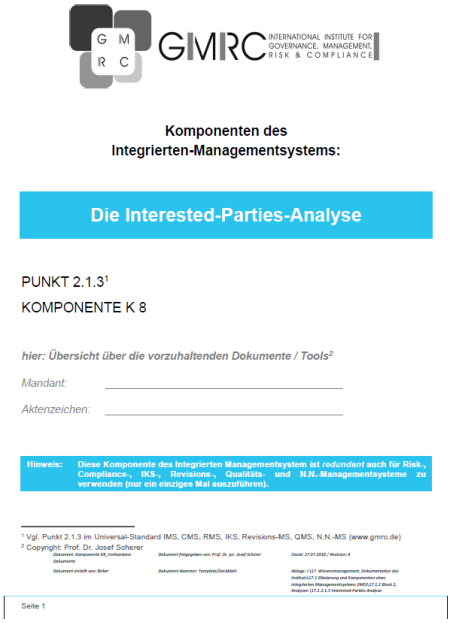
Prinzip 9

Die Organisation identifiziert und bewertet Veränderungen, die das Interne Kontroll-System wesentlich beeinträchtigen können.

Fokuspunkte:

35 Beurteilt Veränderungen in externer Umwelt.“

etc.



GMRC INTERNATIONAL INSTITUTE FOR GOVERNANCE, MANAGEMENT, RISK & COMPLIANCE

Komponenten des
Integrierten-Managementsystems:

Die Interested-Parties-Analyse

PUNKT 2.1.3[1]
KOMPONENTE K 8

hier: Übersicht über die vorzuhaltenden Dokumente / Tools[2]

Mandant: _____

Aktenzeichen: _____

Hinweis: Diese Komponente des Integrierten Managementsystem ist *redundant* auch für Risk-, Compliance-, IKS-, Revisions-, Qualitäts- und N.N.-Managementsysteme zu verwenden (nur ein einziges Mal auszuführen).

[1] Vgl. Punkt 2.1.3 im Universal-Standard IMS, CMS, RMS, IKS, Revisions-MS, QMS, N.N.-MS (www.gmrc.de)
[2] Copyright: Prof. Dr. Josef Scherer

Seite 1

Abbildung 3: K8 Interested Parties-Analyse.

Diese Komponente „*Interested parties-Analyse*“ ist also nur ein einziges Mal durchzuführen und erfüllt zugleich die Anforderungen zahlreicher Managementsystem-Inseln: Effektivität und Effizienz zugleich!

Den Kernbereich des *Universalstandards* bildet jedoch die Ablauforganisation, also die Führungs-, Kern- und Unterstützungsprozesse (nach *Porter*) des Unternehmens / der Organisation:

Diese Prozesse werden mit den Komponenten zur Erfüllung der relevanten Anforderungen in einem Integrierten Managementsystem „angereichert“ und zur Wirksamkeit geführt.

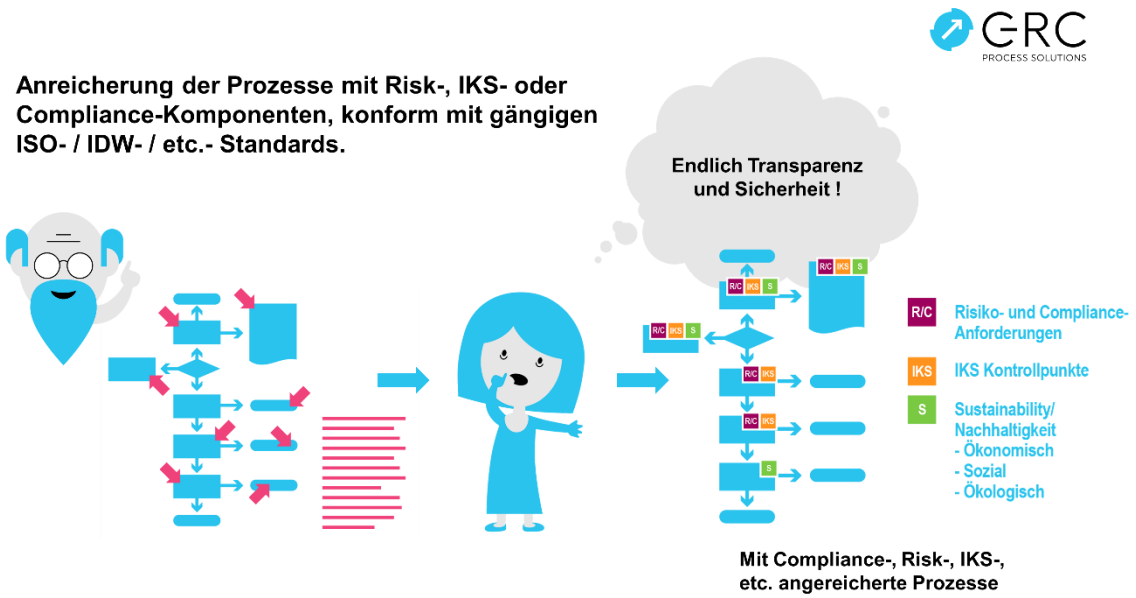


Abbildung 4: Anreicherung der Prozesse.

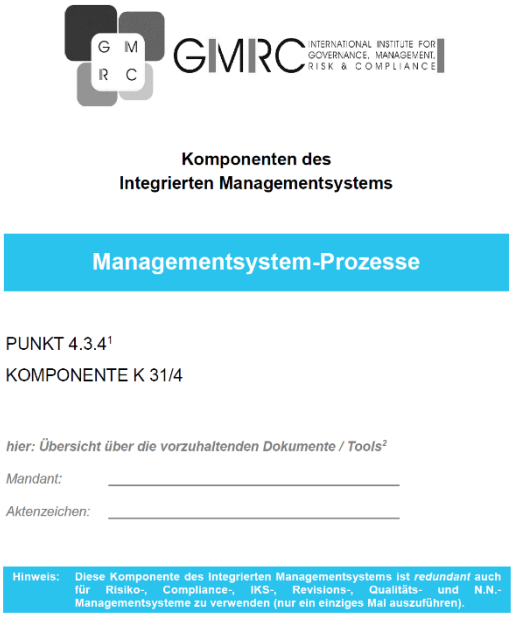


Abbildung 5: K31/4 Managementsystem-Prozesse.

Zur Komponente „*Managementsystem-Prozesse*“ zählen unter anderem Checklisten, Modellierungen der Managementsystem-Prozesse, Ernennungsbeschlüsse für die Prozessverantwortlichen, u.v.m.

Managementbewertung / Management Review

Schließlich fordern die vielen diversen Standards und somit im Rahmen von Assessments auch Wirtschaftsprüfer, Auditoren, Sonderbeauftragte, etc. im Rahmen der Berichterstattung unter anderem von der Geschäftsleitung, jährlich eine *Managementbewertung (Management Review)* in Bezug auf beispielsweise das Risiko-, Compliance- oder N. N.-Managementsystem zu erstellen.

Auch hier können Normen und Standards „verschmolzen“, Redundanzen und Analogien für Effektivität *und* Effizienz genutzt werden:

Aus einzelnen aufwändigen Insel-Bewertungen wird eine komprimierte *GRC-Berichterstattung*.[28]

[28] Vgl. Anlage 1: Muster für eine Managementbewertung (Management Review) bzgl. Risiko- und Compliance-Managementsystem in Anlehnung an ISO 19600, ISO 31000, IDW PS 980, IDW PS 981, ÖNORM D 4901

4.2 „Interpretation“ der High Level Structure (HLS) in ISO-Standards in Richtung „prozessorientierte“ Organisation

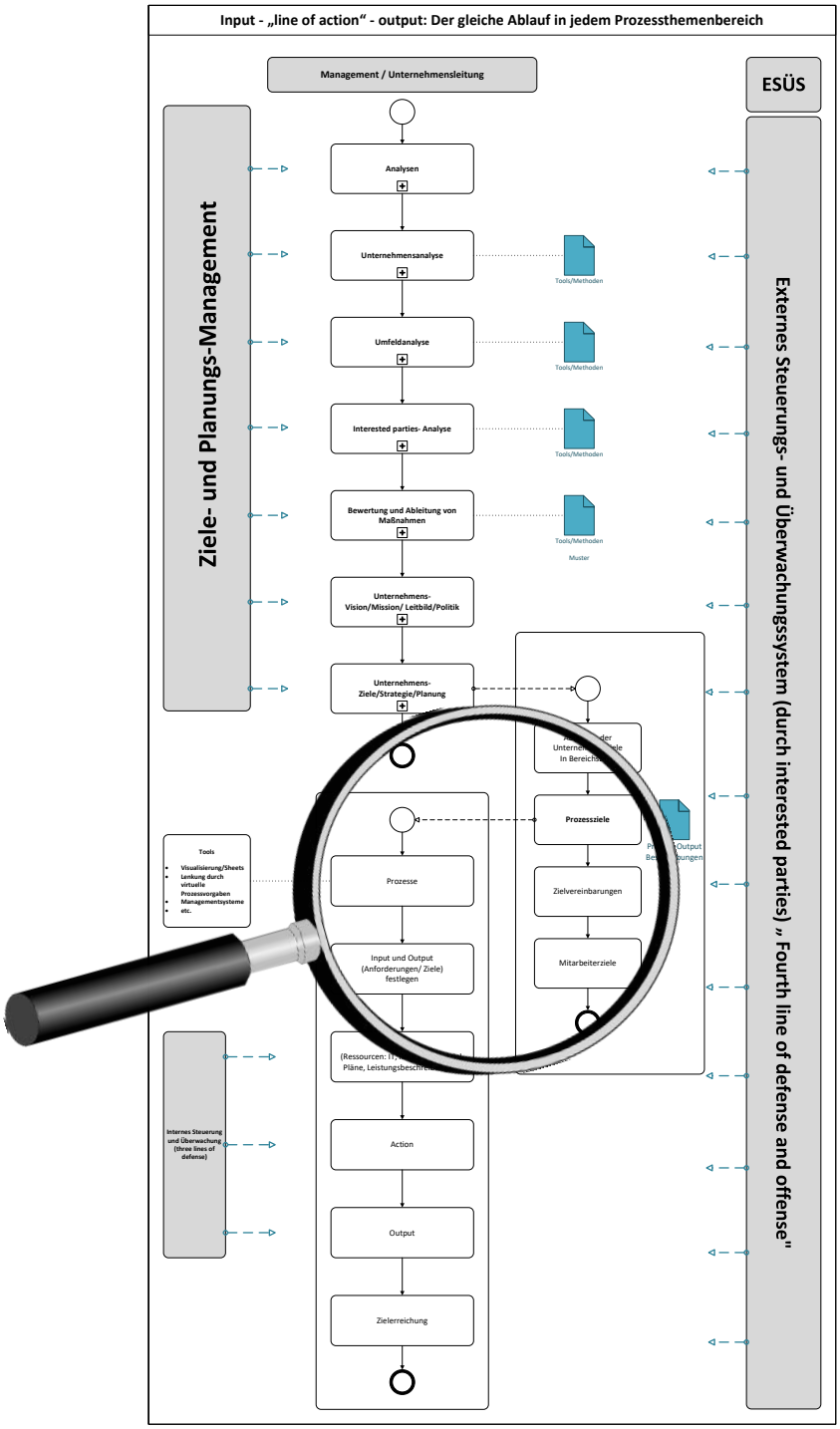


Abbildung 6: Input – „line of action“ – output: Der gleiche Ablauf in jedem Prozessthemenbereich.

Die HLS-Punkte 1 bis 5 (1. Anwendungsbereich, 2. Normative Verweisung, 3. Definitionen, 4. Kontext, 5. Führung und Verpflichtung) sind vor die Klammer gezogene, allgemeine Ausführungen und entsprechen den Blöcken 1-3 des Universal-Standards „Integriertes Managementsystem“ der „Deggendorfer Schule“.

Ab Punkt 6 ff. wird von der HLS eigentlich nur der gängige P/D/C/A-Zyklus oder ein typischer Prozessablauf nachempfunden, wenngleich dies m.E. nicht unbedingt sehr transparent und streng logisch dargestellt wird:

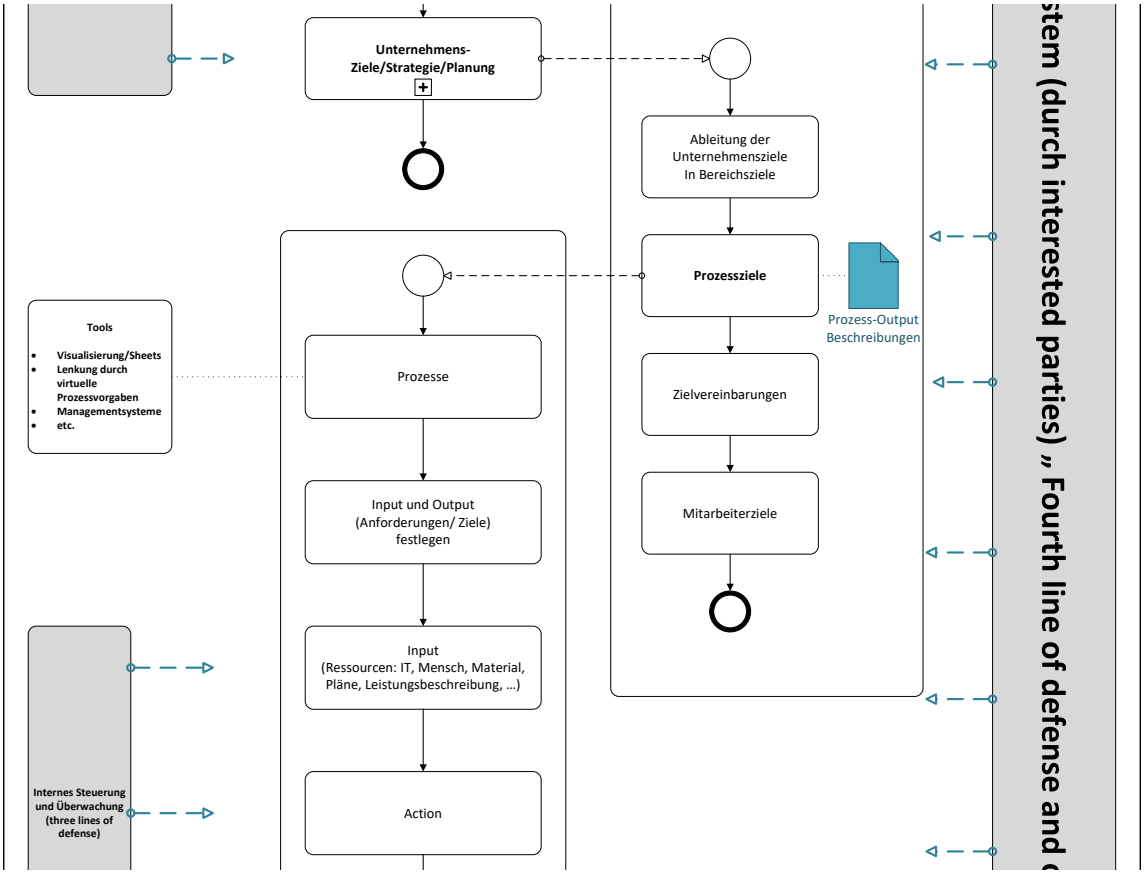


Abbildung 7: Plan / Do / Check / Act – Kreislauf in Prozessabläufen.

4.2.1 Ziele setzen und Anforderungen sowie Maßnahmen zur Erfüllung der Anforderungen zur Zielerreichung bestimmen

Dies entspricht
Block 4, Punkt 4.1 des Universal-Standards und
Punkt 6 „Planung“ der HLS und
der Phase „Plan“ im Deming-Kreislauf.

Zu diesem Punkt gehören aber in der Praxis bereits zwingend auch die Konzeptionierung eines Steuerungs- und Überwachungssystems („lines of defense“) und die Bestimmung von Risiken, die die Zielerreichung gefährden könnten sowie eines Prozesses zur Reaktion bei Abweichungen (vgl. Punkt 4.2 des Universal-Standards).

Bereits an dieser Stelle – und nicht erst wie bei der HLS unter „8. Betrieb“ – ist auf die Inhalte eines N.N.-Managementsystems in Form von Soll-Komponenten und Prozessabläufen einzugehen:

Gerade diese Komponenten/Inhalte/Abläufe des behandelten Themas (QM, Risk, Compliance, Personal, IT, etc.) müssen ja bzgl. Ziele, Anforderungen, Maßnahmen etc. bekannt sein, um sie unter Punkt 6 (HLS) zu planen/projektieren, unter 7. (HLS) vorbereitend zu unterstützen, unter 8. Betrieb (HLS) umzusetzen, unter 9. Bewertung (HLS) zu bewerten und 10. Verbesserung (HLS) zu verbessern.
Zur Planung/Konzeptionierung gehört schließlich u.a. auch noch die entsprechende Managemententscheidung (mit Ressourcenfreigabe!) und die Projektierung.[29]
Damit wären die Anforderungen/Ziele transparent gemacht:

[29]Vgl. *Scherer/Fruth* (Hrsg.), Handbuch: Integriertes Managementsystem (IMS) „on demand“ mit Governance, Risk und Compliance (GRC), 2018, Punkt 1.3.

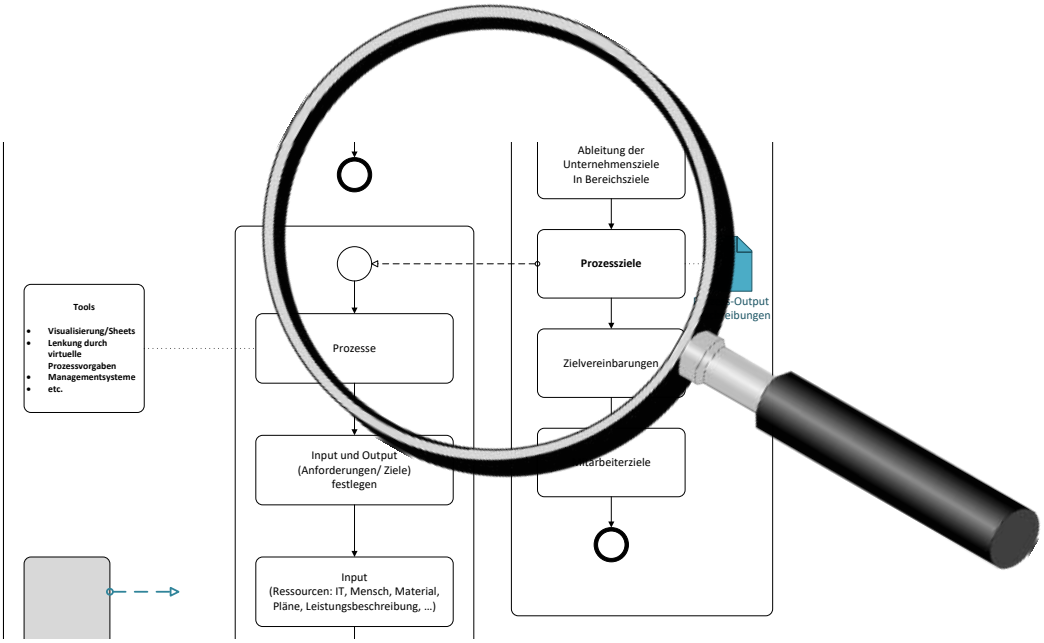


Abbildung 8: Gleiche Abläufe: Prozessziele definieren

4.2.2 Vor der eigentlichen „Action“ muss der „input“ bereitgestellt werden.

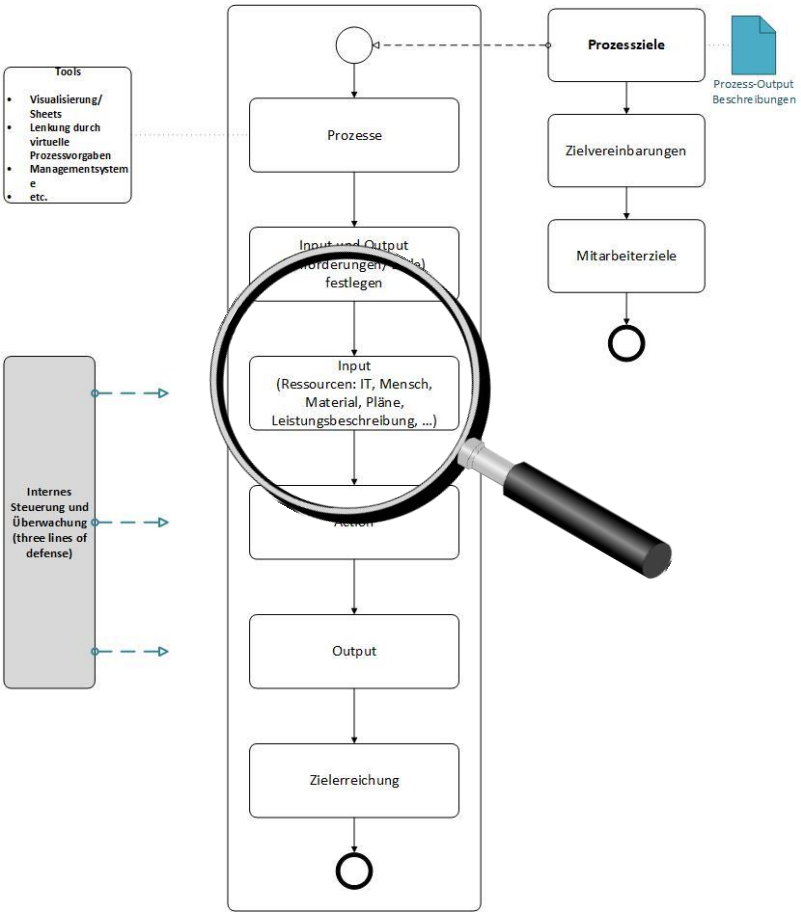


Abbildung 9: Gleiche Abläufe: Input.

Dies wird in der High Level Sturcture unter 7. mit „Unterstützung“ bezeichnet. Im Vierblock-Aufbau wird dies unter Block 2 und 3 dargestellt: Der Rahmen und die allgemeinen Anforderungen im Managementsystem, die vorhanden sein müssen, um über Aktionen (Prozessabläufe) diesen „input“ in „output“ zu verwandeln.
Diese Phase enthält auch die „Implementierung“ oder auch Do /Teil 1.
„Wirksam“ wird das Ganze erst mit der gelebten Umsetzung (Do /Teil 2) in den Prozessen (action!).

4.2.3 Über gelebte Prozessabläufe wird der input in output verwandelt.

Hier müsste in der HLS-Phase 8. „Betrieb“ bzgl. der Inhalte (was umfasst der „Betrieb“?) ein Verweis auf die bereits bei der Planungsphase unter 6. dargestellten Punkte genügen (Do/ Teil 2/ „action“).

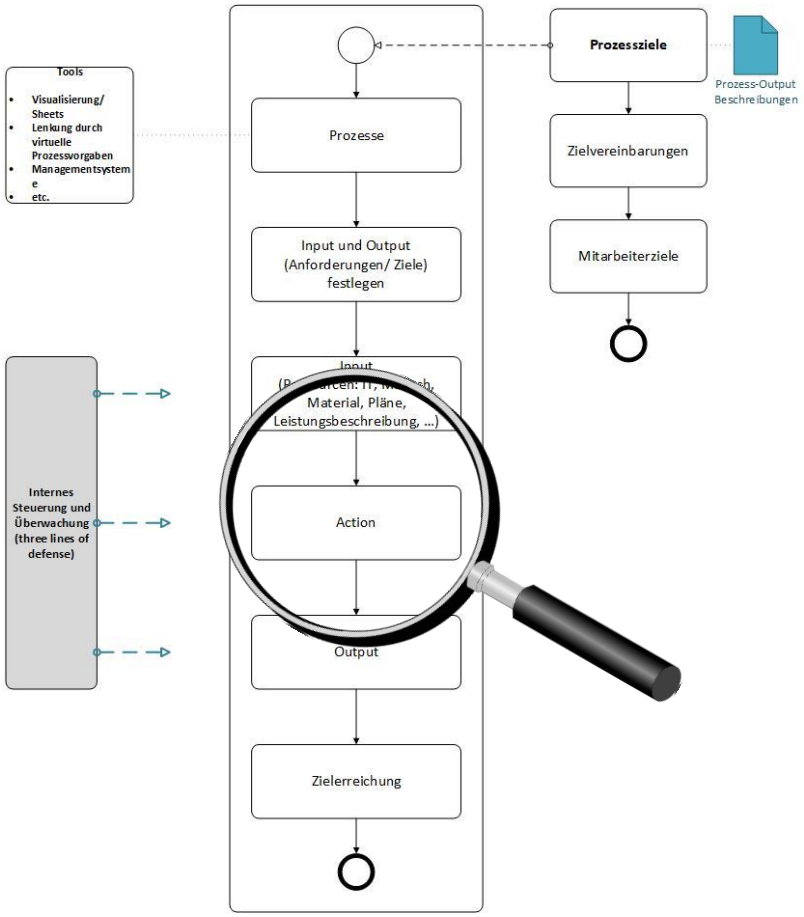


Abbildung 10: Gleiche Abläufe: Action.

4.2.4 Steuerung und Überwachung / Internes Kontroll-System

Das Steuerungs- und Überwachungssystem („Check“) würde *in einer vernetzten,* also nicht bürokratisch-linear ablaufenden *Organisation* die vorhergehenden Punkte 6 und 7 *parallel* mit Soll-Ist-Abgleich, Kennzahlenermittlung, Eskalationsprozess, Monitoring, Reporting, Dokumentation *begleiten* und nicht erst chronologisch nachfolgend ab Punkt 9 „Bewertung“ (HLS) zum Einsatz kommen, wenn „das Kind evtl. schon in den Brunnen gefallen“ ist.
Zu differenzieren ist auch deutlich zwischen Bewertung (Assessment) des Managementsystems und Bewertung der Abläufe und Komponenten eines Standards. Dies wird in ISO-Standards oft vermischt.[30]

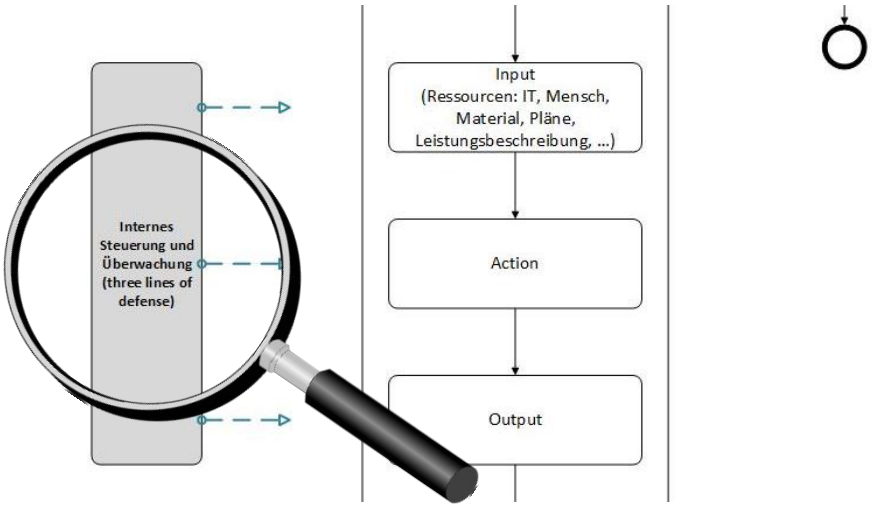


Abbildung 11: Gleiche Abläufe: Begleitende Steuerung und Überwachung.

4.2.5 Verbesserung und Anpassung an Veränderungen

Auch „Act“ (10. „Verbesserung“ (HLS)), also die Anpassung an interne / externe Veränderungen oder erkannte Schwachstellen, läuft *parallel im Steuerungs- und Überwachungssystem* mit.

[30]Vgl. *Scherer/Fruth* (Hrsg.), Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk und Compliance (GRC), 2016 und *Scherer/Fruth*, Danke ISO! Über die neue ISO 9001:2015 (Qualitätsmanagementsystem) zum integrierten, ganzheitlichen Managementsystem mit Governance, Risk und Compliance (GRC) – Buchbeitrag in: BCM – Berufsverband der Compliance Manager, COMPLIANCE 2015, Perspektiven einer Entwicklung, 2015, S. 83 – 107 (www.gmrc.de).

4.2.6 Zielerreichung als output

Wenn alles optimal läuft, würde der input in output, nämlich die Erfüllung der relevanten Anforderungen der interested parties und Zielerreichung umgewandelt.

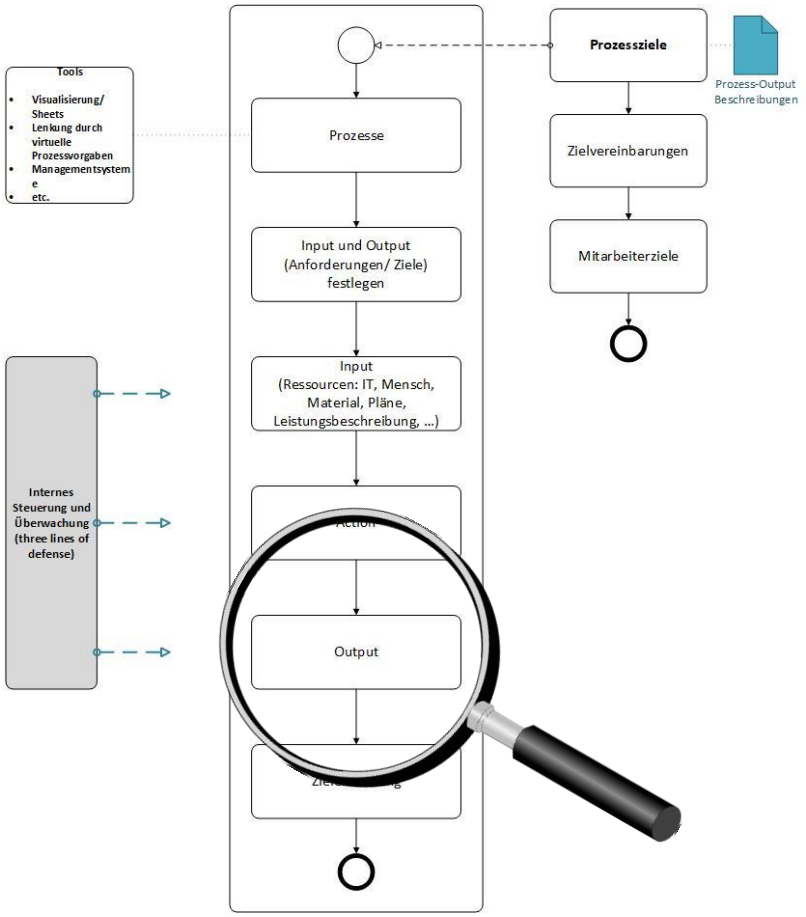


Abbildung 12: Gleiche Abläufe: Output.

5. „High Level Structure 4.0“: Die Vernetzung der Komponenten von Normen, Richtlinien und Standards in einem Integrierten Workflow-Managementsystem

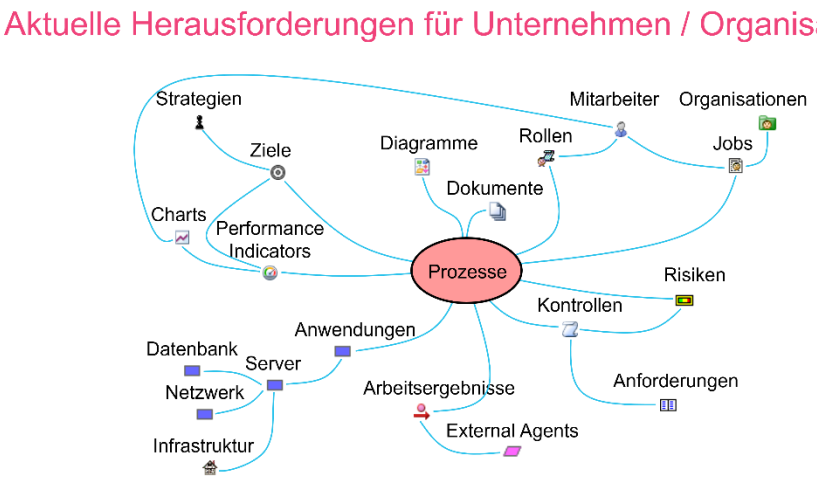


Abbildung 13: Vernetzung der Komponenten eines Managementsystems auf Basis von Prozessabläufen.

Die Prozesse stehen im Zentrum des Integrierten Managementsystems in einem Beziehungsgeflecht zu vielen Komponenten.

Sehr oft werden Prozesse in Unternehmen nicht ganzheitlich betrachtet. Mit einem Integrierten Human-Workflow-Managementsystem können die einzelnen Komponenten eines beliebigen N.N.-Managementsystems mit Fokus auf die Unternehmensprozesse in logische Beziehung gesetzt werden.

Dies bedeutet, dass in Human-Workflow-Managementsystemen jeder Prozess optimal mit den individuell benötigten Ressourcen (Ziele, Strategien, Anforderungen, Tools, Verantwortlichkeiten, etc.) angereichert wird. Dadurch wird ermöglicht, dass jeder Mitarbeiter *„das Richtige richtig tun“* kann.

These:

Ein analoges System, basierend auf denklogisch linear angeordneten Standards, verortet in Dokumenten, Handbüchern, Richtlinien, Excel-Tabellen oder E-Mail-Anhängen kann niemals den Sprung in die digitale Transformation schaffen:

Wenn „nicht gelebte analoge Dokumente“ digitalisiert werden, gibt es am Ende nur „nicht gelebte digitalisierte Dokumente“, aber keine gelebte Vernetzung, Automatisierung und digitale Transformation im Sinne von „4.0“!

Für eine „echte digitale Transformation“ sind Integrierte Human-Workflow-Managementsysteme notwendig. Um die „nicht-gelebten Dokumente“ wie Gesetze, interne Richtlinien, Standards, etc. via gelebte Prozessabläufe zum Leben zu erwecken, sind

sie *zunächst zu fragmentieren*, in relevante Anforderungen und Maßnahmen zur Erfüllung der Anforderungen *zu „übersetzen“* und die jeweiligen Abläufe den relevanten Prozessschritten zuzuordnen:

Beispiel Compliance:

Das Handelsgesetzbuch (*HGB)*: Ein „Rechtskataster“, das aufführt, dass in den Abteilungen Einkauf und Vertrieb „das *HGB*“ zur Anwendung komme, ist sinnlos (und kostet nur Geld).

Das *HGB* muss also erst *fragmentiert und die relevanten Normen daraus übersetzt in Anforderungen und daraus resultierenden Maßnahmen den richtigen Prozessschritten zugeordnet werden:*

Beispiel:

Die Obligenheit zur unverzüglichen Untersuchung der Ware und Rüge gemäß § 377 HGB im Rahmen der Wareneingangslogistik[31]:

Diese fragmentierte / herausgelöste Anforderung (§ 377 HGB) aus dem gesamten Handelsgesetzbuch könnte zunächst in einen „Compliance-, Risiko-, IKS-, etc.-Steckbrief“ „übersetzt“ und dem relevanten Prozessschritt des Einkaufsprozesses zugeordnet werden.

[31] **§ 377 HGB:**
(1) Ist der Kauf für beide Teile ein Handelsgeschäft, so hat der Käufer die Ware unverzüglich nach der Ablieferung durch den Verkäufer, soweit dies nach ordnungsmäßigem Geschäftsgange tunlich ist, zu untersuchen und, wenn sich ein Mangel zeigt, dem Verkäufer unverzüglich Anzeige zu machen.
(2) Unterläßt der Käufer die Anzeige, so gilt die Ware als genehmigt, es sei denn, daß es sich um einen Mangel handelt, der bei der Untersuchung nicht erkennbar war.
(3) - (5) […]

Compliance-, Risiko-, IKS-, etc.-Steckbrief: Eine Maßnahme, die mit einer „Klappe mehrere Fliegen (Compliance-, Risiko-, IKS-, QM-, etc.-Anforderungen) erschlägt“.

Compliance-/ Risiko- / IKS-Anforderungen

Compliance-ID:
Ekauf 5 – LS1/Compliance

Abgleich der gelieferten Ware mit bestehenden Anforderungen.
Abstimmung mit Lieferschein und mit Bestellung und gegebenenfalls Qualitätssicherungsvereinbarung (§ 377 HGB)

(Compliance-)Risikoverantwortlicher:

1. Geschäftsleitung
2. Compliance-Beauftragter / -Officer
3. Leitung Einkauf

Instrumente / Tools / Methoden:

1. Checkliste Prüfung Wareneingang (§377 HGB)
2. Muster: Abgeschlossenen QSV
3. Muster: Lieferschein (mit zu prüfenden Punkten)
4. Liste mit Lieferanten, mit denen eine Qualitätssicherungsvereinbarung abgeschlossen wurde

Beschreibung des Compliance-Ziels:
(vom Unternehmen auszufüllen!)

„Ziel ist, die ordnungsgemäße Prüfung der Lieferscheine und die Beachtung der Anforderungen aus § 377 HGB bei Wareneingang. Zudem soll mit ausgewählten Lieferanten (vorrangig Lieferanten, die direkt auf die Baustelle liefern) eine Qualitätssicherungsvereinbarung geschlossen werden. Durch die QSV kann sichergestellt werden, dass auch ohne eine vollständige Prüfung nach § 377 HGB Ansprüche bei Mängel gegenüber dem Lieferanten bestehen bleiben.“

Darstellung der Maßnahmen zur Erreichung der Compliance-Ziele
(vom Unternehmen auszufüllen!)

1. Abschluss von Qualitätssicherungsvereinbarungen mit A-Lieferanten
2. Zuverlässige Kontrolle/Abgleich durch Einbau eines entsprechenden Prozessschrittes
3. Schulung der betroffenen Mitarbeiter

Beschreibung der Compliance-Anforderungen:
(vom Unternehmen auszufüllen!)

1. *Untersuchungs- und Rügepflicht des Kaufmanns bzgl. Mängel, richtiger Menge und Art der Ware nach **§ 377 HGB***
2. ***ISO 9001:2015: 8.2.3** Überprüfung von Anforderungen in Bezug auf Produkte und Dienstleistungen*
3. ***ISO 9001:2015: 8.4** Kontrolle von extern bereitgestellten Produkten und Dienstleistungen*
4. ***ISO 9001:2015: 8.7** Steuerung nichtkonformer Prozessergebnisse, Produkte und Dienstleistungen*
5. ***ISO 19600:2016: 8.3** Ausgegliederte Prozesse*
6. *Interne Richtlinien bei Wareneingangsprüfung*

Aussagen des Prüfers in Bezug auf Stichproben, Prüfungshandlung in Bezug auf die (Compliance-) Risikobehandlung, Bewertungsmaßnahmen, Ergebnisse der (Compliance-) Risikosteuerung und -überwachung:
(vom Prüfer/Compliance-Beauftragten auszufüllen!)

Beispiel:

1. *Prozessschritt ist implementiert.*
2. *QSV wurde mit relevante Lieferanten abgeschlossen*
3. *Kontrolle wird zu ca. 50% umgesetzt.*

Aussagen des Prüfers zur Reduzierung des (Compliance-)Risikos / Anmerkungen:
(vom Prüfer/Compliance-Beauftragten auszufüllen!)

Beispiel:

1. *Die betroffenen Mitarbeiter sind innerhalb des nächsten halben Jahres noch stärker zu sensibilisieren.*
2. *Die Liste der Lieferanten mit QSV ist jährlich zu aktualisieren.*

Abbildung 14: Compliance-, Risiko-, IKS-, etc.-Steckbrief: Eine Maßnahme, die mit einer „Klappe mehrere Fliegen (Compliance-, Risiko-, IKS-, QM-, etc.-Anforderungen) erschlägt“.

Weiteres Beispiel:

Ebenso ist mit Punkt 3 der HLS, „*Definitionen*“, zu verfahren:

Jede Definition gehört dahin, wo sie gebraucht wird. Dies entspricht auch den modernsten und zugleich sehr alten Lernformen: „Learning by doing“: im jeweiligen Prozessablauf.

Es empfiehlt sich also, nicht nur die Prozesse mit Risk-, IKS- und Compliance-Komponenten anzureichern, sondern auch für jeden Mitarbeiter verständliche **Definitionen** von Begriffen an den **jeweiligen Prozessschritten zu verorten**.

Somit wird nicht nur ein **digitales Glossar**, zum Beispiel im Intranet des Unternehmens, hinterlegt, sondern für den Mitarbeiter direkt an dem jeweiligen Prozess-Workflow der dafür notwendige Fachbegriff verständlich dargestellt.

Beispiel Wareneingangslogistik

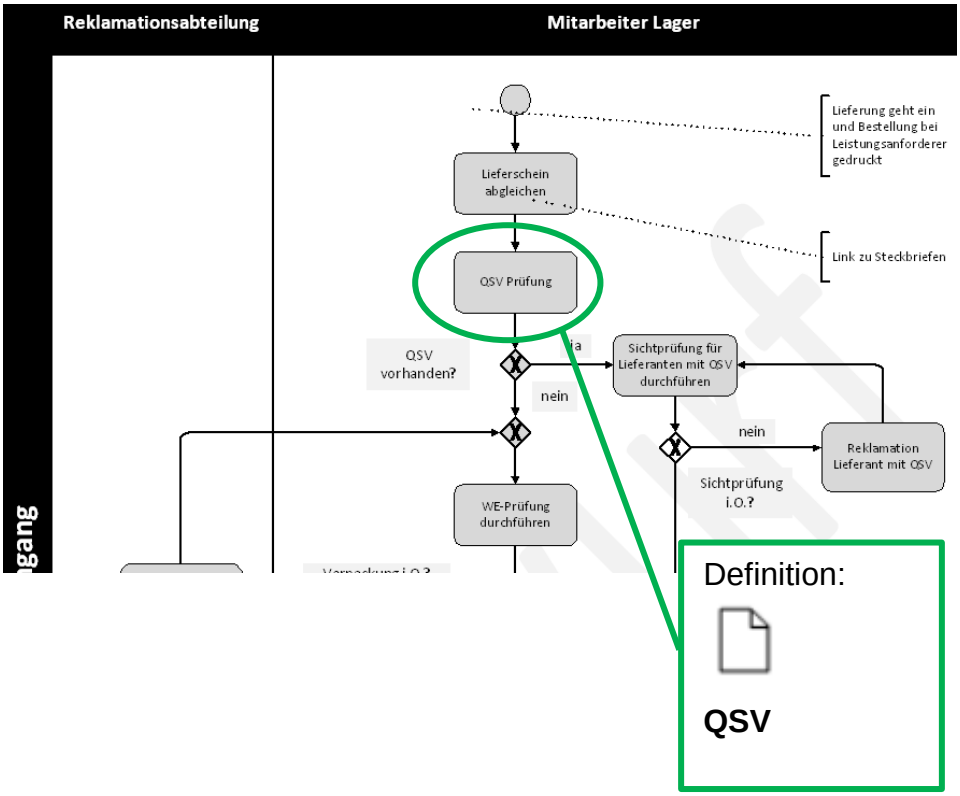


Abbildung 15: Prozessausschnitt: Wareneingangslogistik[32]

Im Einkaufsprozess „Wareneingangslogistik“ kann beim markierten Prozessschritt „QSV-Prüfung“ für den Workflow-Verantwortlichen die Definition der Qualitätssicherungsvereinbarung (QSV) verortet werden. Die Definition kann wie folgt lauten:

Qualitätssicherungsvereinbarung (QSV):

Eine QSV ist eine Vereinbarung mit wichtigen Lieferanten, damit unter anderem die Qualität, Liefertreue, etc. ihrer Produkte und Dienstleistungen gewährleistet wird.

In diesen Vereinbarungen kann auch geregelt werden, dass der Lieferant neben einem Qualitäts-Managementsystem auch ein Risiko-, Compliance- und Nachhaltigkeits-System vorhalten muss.

Idealerweise wird an diesem Prozessschritt nicht nur die jeweilige Definition der QSV verlinkt, **sondern auch eine Muster-QSV verortet**.

Ergänzend könnte sogar noch ein **Kurz-Lehrfilm** („KISS“) zum jeweiligen Handlungsablauf an dieser Stelle verlinkt sein.

[32] Aus: *Scherer/Fruth* (Hrsg.), Handbuch: Einführung in ein Integriertes Einkaufs-Managementsystem mit Governance, Risk und Compliance (GRC), 2018.

Nach wie vor haben wir lediglich eine (durchaus gute) Dokumentation / ein Wissensmanagement. Aber: Der Prozess lebt noch nicht!

Dafür sorgt nun eine Vernetzung aller Aktivitäten zur Erfüllung der in den Komponenten von Normen, Standards, Richtlinien enthaltenen Anforderungen:

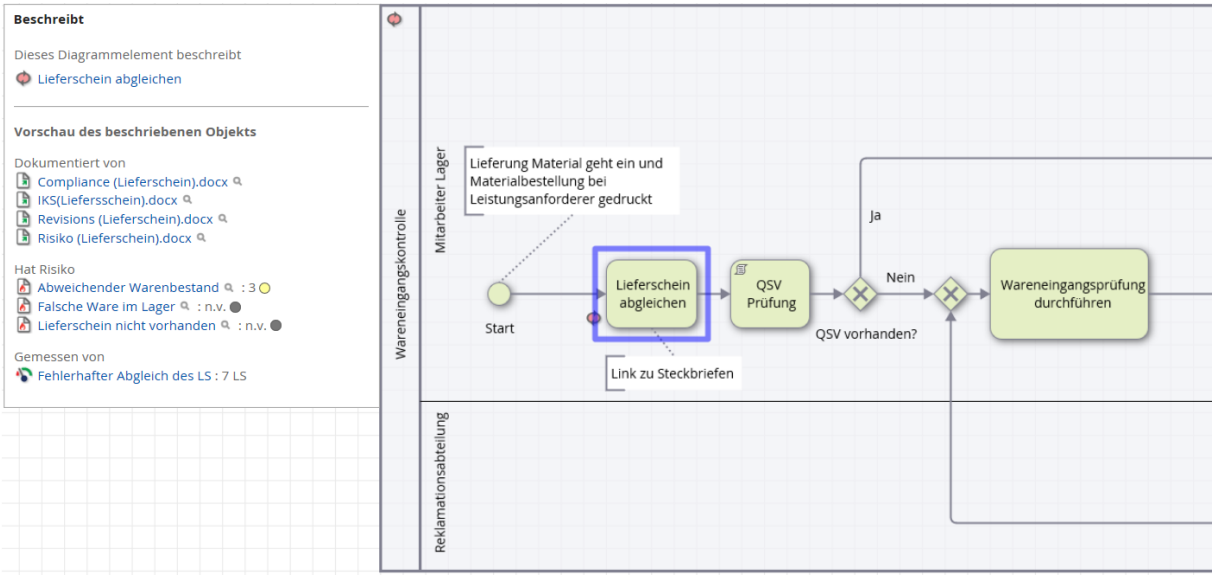


Abbildung 16: Wareneingangskontrolle in GRC-PS - I.

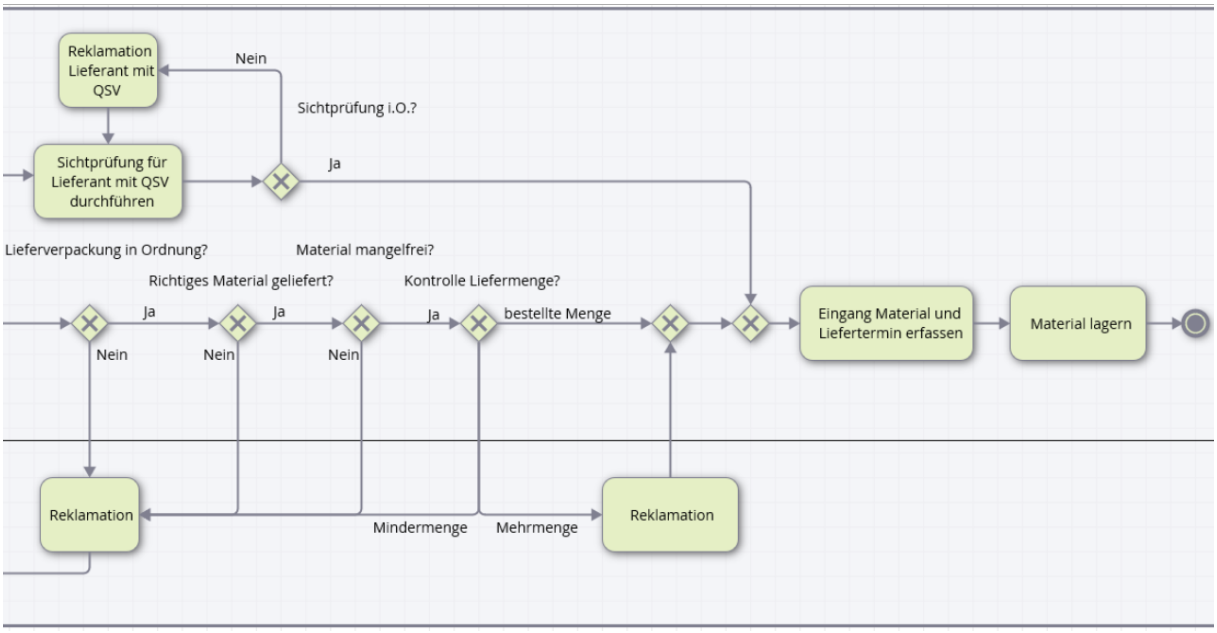


Abbildung 17: Wareneingangskontrolle in GRC-PS - II.

Weiteres Beispiel: (Aufbau-) Organisation: **Rollen und Verantwortlichkeiten**:

Auch der *Risiko- (oder Compliance-)beauftragte* mit seiner Stellenbeschreibung sollte nicht nur Bestandteil eines Standards (Punkt 7 der HLS), der Rechtsprechung oder eines Handbuches sein, sondern bekommt eine „Rolle“, vernetzt im Rollen- und Berechtigungssystem der IT-basierten Prozessabläufe:

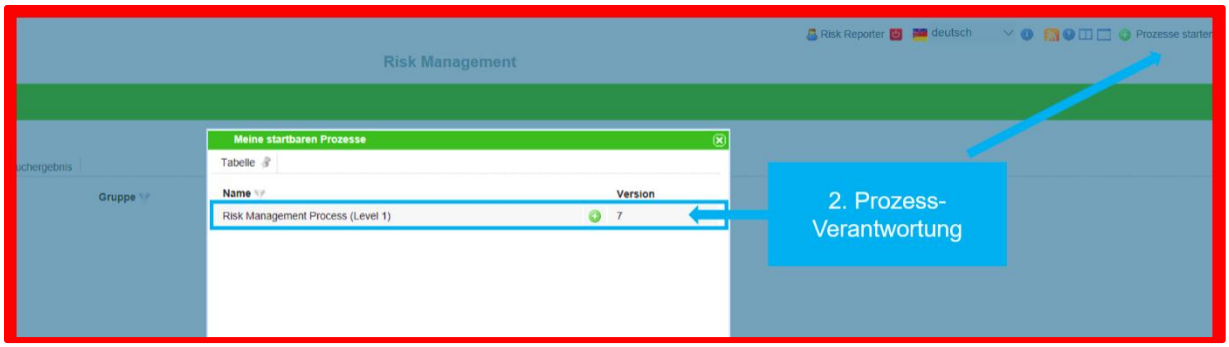


Abbildung 18: Risk-Management-Prozess: Risiko-Prozess starten.

In einem digital transformierten Workflow-Managementsystem sind also Bestandteile der Ablauforganisation oder auch von Normen / Richtlinien / Standards / etc. nun Bestandteil *gelebter Abläufe:*

Der Risikobeauftragte ist z. B. Adressat der Mitteilungen aufmerksamer Mitarbeiter bzgl. Gefahren und Chancen.

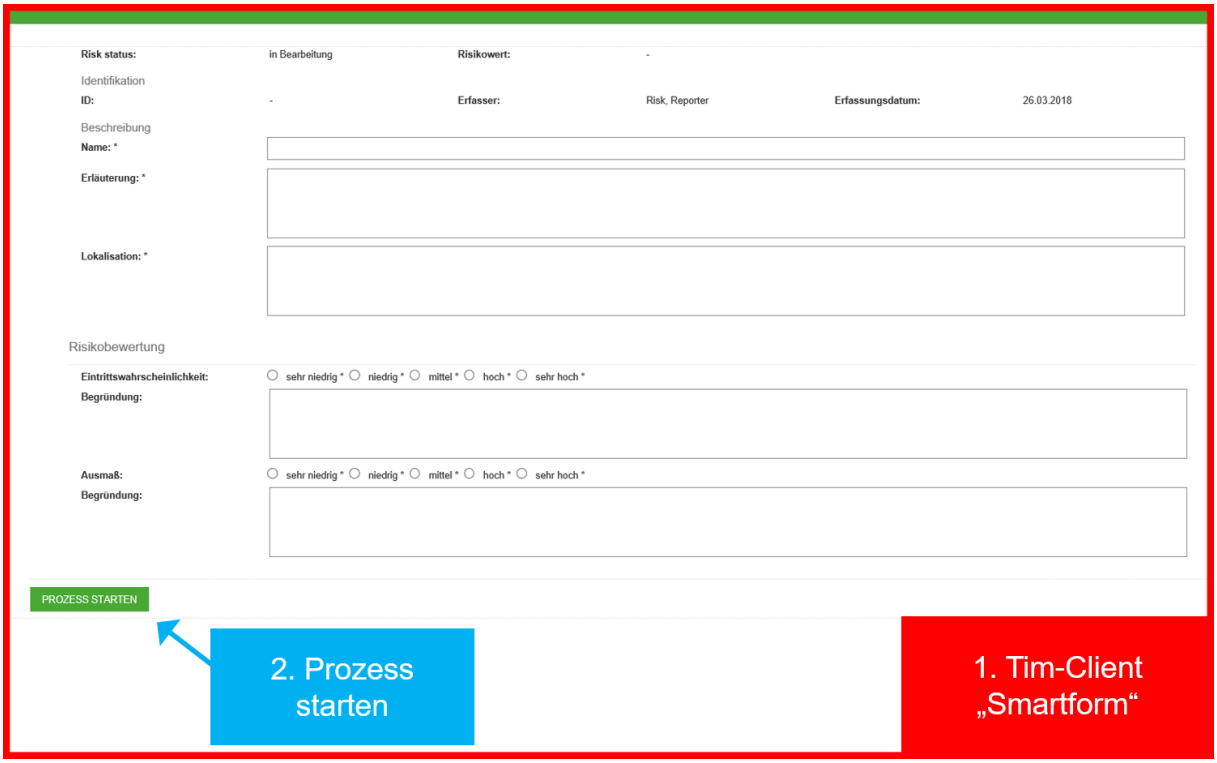


Abbildung 19: Risk-Management-Prozess: Smartform zum Prozessstart.

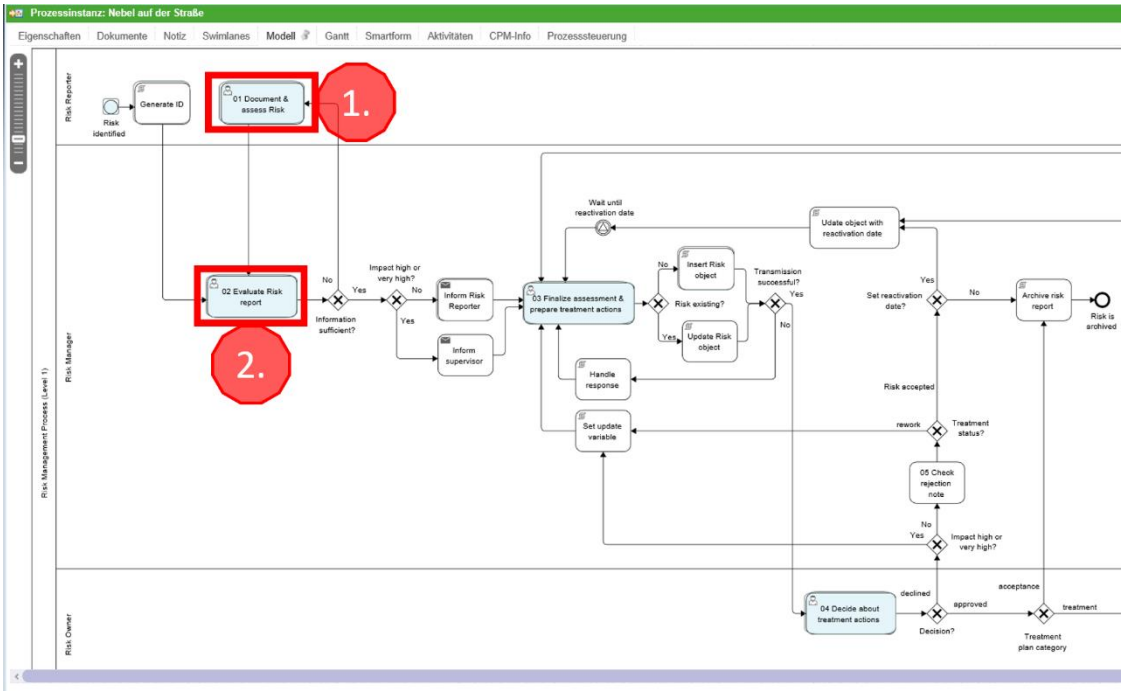


Abbildung 20: Risk-Management-Prozess: Prozessmodell (Teil 1).

Die Erfüllung der Anforderungen und entsprechende Maßnahmen werden über gesteuerte und kontrollierte Aufgabenverteilung sichergestellt.

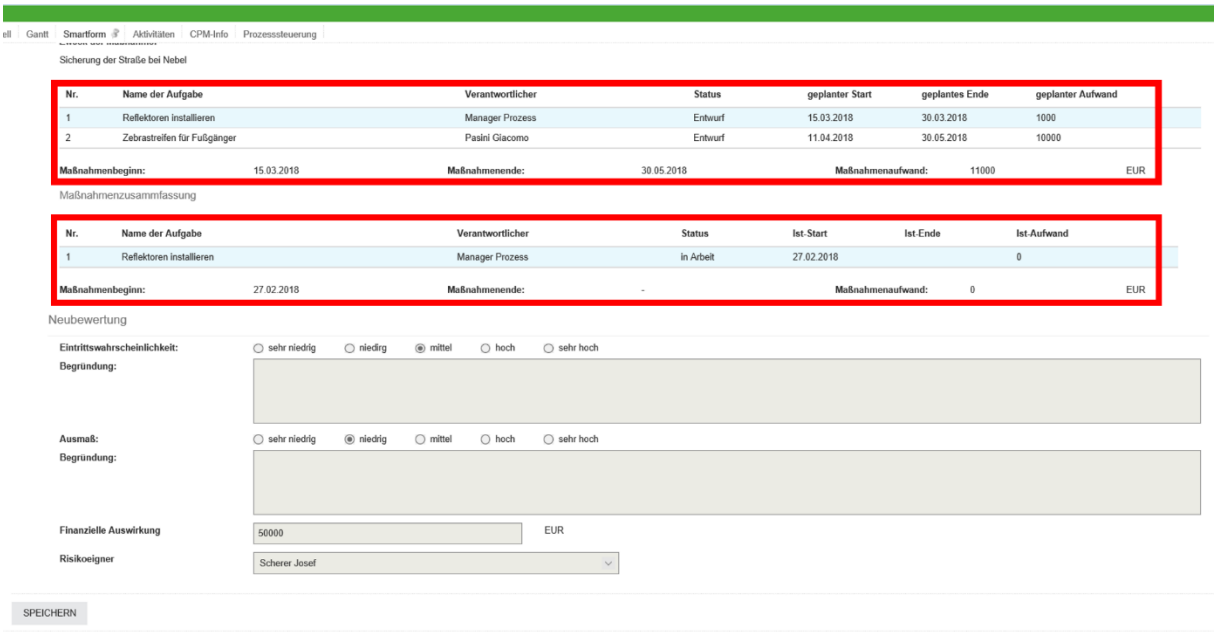


Abbildung 21: Risk-Management-Prozess: Aufgaben zur Maßnahmenerfüllung.

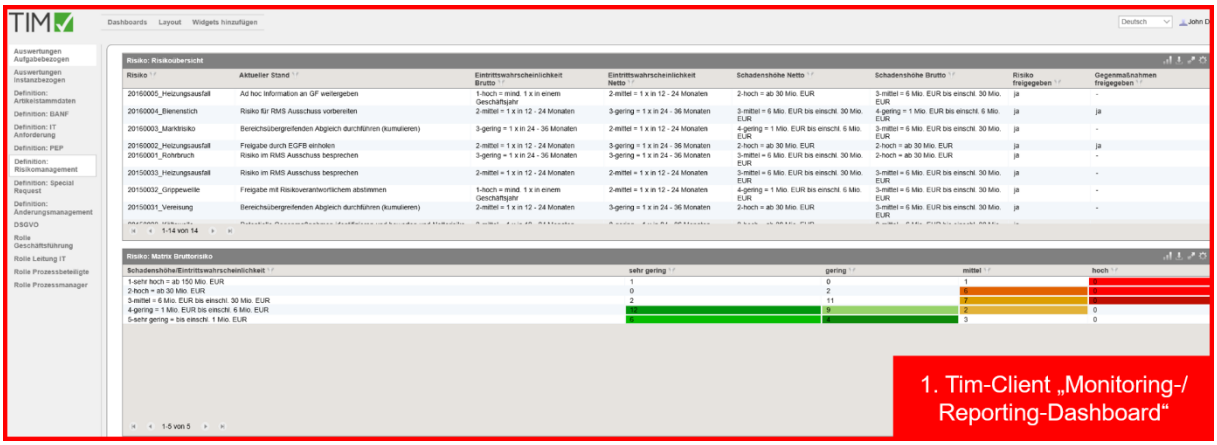


Abbildung 22: Risk-Management-Prozess: Risiko-Cockpit.

Jederzeit kann in Echtzeit überwacht oder auch über den Soll-Ist-Zustand berichtet werden:

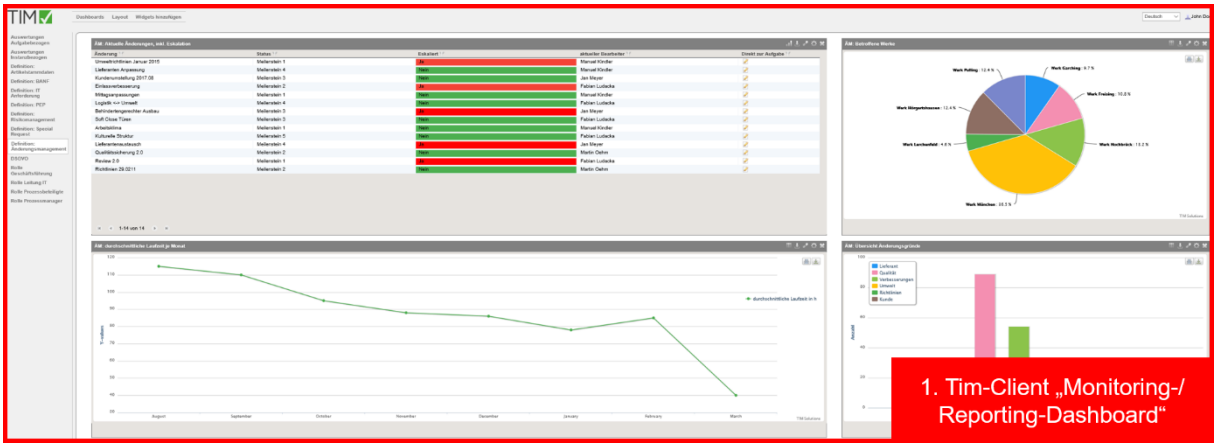


Abbildung 23: Risk-Management-Prozess: Reporting-Dashboard.

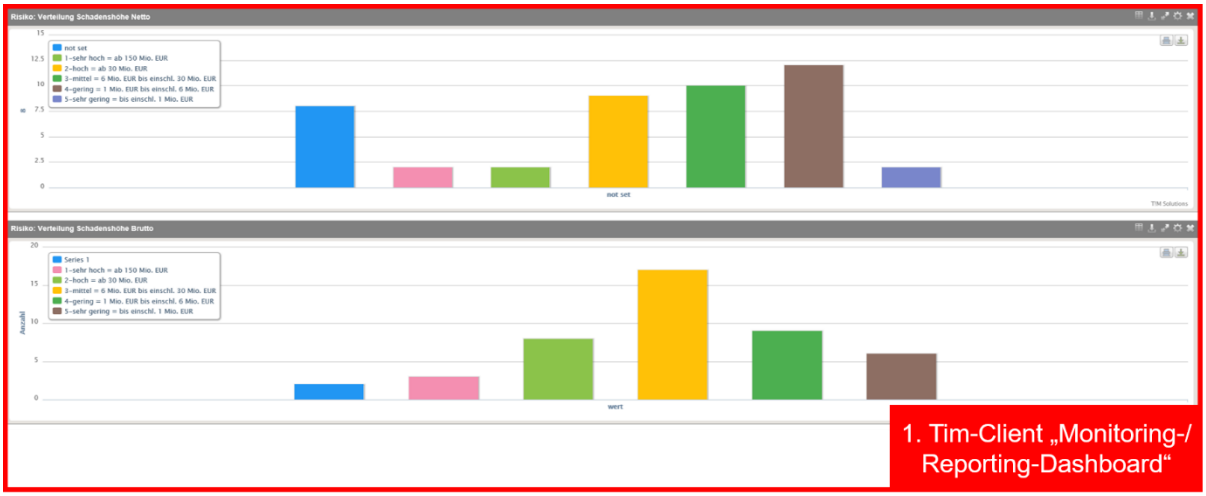


Abbildung 24: Risk-Management-Prozess: Reporting-Dashboard.

Exkurs: Die erste „Kognitive Revolution“

Nach *Harari* konkurrierte der *Homo sapiens*, bevor vor circa 70.000 Jahren mit der kognitiven Revolution[33] seine enorme Entwicklung und Ausbreitung von Ostafrika bis nach Europa und Ostasien begann, zunächst u. a. mit den Neandertalern.

Trotz Hürden wie dem offenen Meer gelang dem *Homo sapiens* schließlich auch die Besiedelung Australiens.[34]

Die gängigste Erklärungs-Theorie dieser Entwicklung geht von zufälligen Genmutationen aus, wodurch es dem Sapiens ermöglicht wurde, zu denken, zu lernen und in Form von Sprache zu kommunizieren. Dank der Anpassungsfähigkeit von Gehirn und Sprache können immense Mengen an Informationen zu verschiedenen Zwecken aufgenommen, gespeichert und weitergegeben werden.

Nach einer zweiten Erklärungs-Theorie dient die Sprache dem Zweck des Austauschs von Informationen über die Umwelt,[35] da damit das sich verändernde Beziehungsgeflecht in einer Personengruppe transparent gemacht werden kann. Dadurch können Gruppenerweiterungen und auch komplexe Formen der Zusammenarbeit entstehen bzw. entwickelt werden.[36]

Mithilfe unserer Sprache können wir auch nichtexistierende Dinge erörtern, spekulieren und Geschichten erfinden, weshalb sie auch als „fiktive Sprache“ bezeichnet wird.[37]

Ende Exkurs

---

[33] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 34: *„Die Entstehung neuer Denk- und Kommunikationsformen in dem Zeitraum, der vor rund 70 000 Jahren begann und vor etwa 30 000 Jahren endete, wird als kognitive Revolution bezeichnet.*

[34] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 33: *„Die meisten Forscher sehen in diesen beispiellosen Leistungen einen Hinweis darauf, dass die kognitiven Fähigkeiten des Homo sapiens einen Quantensprung gemacht haben.“*

[35] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 35: *„Es ist viel wichtiger zu wissen, wer in der Gruppe wen nicht leiden kann, wer mit wem schläft, wer ehrlich ist und wer andere beklaut.“*

[36] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 36: *„Sie glauben doch nicht etwa, dass sich Geschichtswissenschaftler beim Mittagessen nur über historische Ereignisse austauschen, oder dass Physiker ihre Kaffeepause mit der Erörterung von Quarks zubringen? Natürlich nicht. Sie unterhalten sich über die Professorin, die ihren Mann mit einer andren erwischt hat, über den Streit zwischen dem Fachbereichsleiter und der Dekanin oder über das Gerücht, dass sich ein Kollege von den Forschungsgeldern der Studienstiftung einen Mercedes gekauft hat.“*

[37] Vgl. *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S. 38: *„Sapiens sind dagegen ausgesprochen flexibel und können mit einer großen Zahl von wildfremden Menschen kooperieren. Und genau deshalb beherrschen die Sapiens die Welt, während Ameisen unsere Essensreste verzehren und Schimpansen in unseren Zoos und Forschungslabors herumhocken.“*

Fazit

Über vernetzte *Human Workflow-Managementsysteme*, künstliche Intelligenz, Quanten-Chip-Technik und viele weitere aktuelle Themen in Forschung und Praxis, hat der Mensch es möglicherweise nach tausenden von Jahren gerade geschafft, seine „Schrift-“ und Managementsysteme vom bürokratischen, analogen „Beamten-Organisations-Denken“ (vgl. oben Punkt 2) der realen vernetzten Welt in Unternehmen und Organisationen, aber auch der Funktionsweise des Gehirns anzupassen.

Eventuell sind automatisierte Prozessabläufe in nicht allzu ferner Zeit sogar in der Lage, sich - selbst lernend – kontinuierlich zu verbessern („KVP 4.0“)?

Nach der ersten „*kognitiven Revolution*“, die den Siegeszug des homo sapiens über den homo neanderthalensis ermöglichte[38], stellt dies möglicherweise die nächste „kognitive Revolution“ dar.

Unter Umständen konkurrieren aber bei der aktuellen „*zweiten kognitiven Revolution*“ dieses Mal homo sapiens und künstliche Intelligenz?[39]

Zunächst jedenfalls ist es angesagt, Normen, Richtlinien und Standards zeitgemäß mit Leben (Wirksamkeit) zu füllen und tatsächlich *digital zu transformieren*.

Da es im Unternehmen nicht nur *einen* Prozess, der optimal für alle Mitarbeiter gestaltet werden muss, sondern womöglich Hunderte gibt, ist es anspruchsvoll, aber auch umso wichtiger, diese Komplexität „im Griff zu haben“.

[38] Vgl. Summary von *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, S.10, 32 ff.
[39] Vgl. dazu *Harari*, Homo deus: Eine Geschichte von Morgen, 14. Auflage, 2018.

Anlage 1: Muster einer Risk- und Compliance-Managementbewertung (Management Review)

Managementbewertung (Management Review) in Bezug auf das Risiko- und Compliance-Managementsystem von N. N. (Name der Organisation)

(Vgl. ISO 19600 Punkt 9.3, ISO 31000, IDW PS 980, IDW PS 981, COSO II, DIIR, ÖNORM D 4900)

1. Ist-Zustand zum (Datum)

1.1. Wie ist der Status der aufgrund der vorherigen Managementbewertungen veranlassten Maßnahmen in Bezug auf das Risiko- und Compliance-Managementsystem?

1.1.1 Früher beschlossene Maßnahmen		**1.1.2 Status**	**1.1.3 Weitere Maßnahmen, falls veranlasst**
1.1.1.1 (Beispiel:) Thema Prozesse *„In den Bereichen Einkauf und Business Continuity Management müssen bis (Datum) angemessene Prozesse implementiert und wirksam sein.“*		1.1.2.1 (Beispiel:) Thema Prozesse *„Die Prozesse sind implementiert, werden aber noch nicht gelebt.“*	1.1.3.1 *„Schulungen / Workshops / internes Wirksamkeits-Audit“*
1.1.1.2 Thema: Kompetenzen der Mitarbeiter		1.1.2.2 … *„Die Mitarbeiter sind zu 60 % angemessen kompetent in Compliance und Risk“*	*1.1.3.2 „Schulung der restlichen 40 % der Mitarbeiter“*

1.2. Ist die Risiko- und Compliance-Politik (noch) geeignet, die Risiko- und Compliance-Managementsystem-Zielerreichung angemessen zu unterstützen?

…

1.3. Wie ist der Grad der Erreichung der Risiko- und Compliance-Ziele?

1.3.1 Ziele	1.3.2 Zielerreichungsgrad (qualitativ / quantitativ)
1.3.1.1 (Beispiel:) …	1.3.2.1 (Beispiel:) …
1.3.1.2 …	1.3.2.2 …

1.4. Sind die (finanziellen / logistisch (IT / Infrastruktur) / personellen) freigegebenen Ressourcen (Budget) für die nächsten 2 Jahre angemessen?

…

1.5. Veränderungen bei externen und internen Themen, die das Risiko- und Compliance-Managementsystem betreffen:

Zusammenfassung und Handlungsempfehlungen aus Unternehmens-, Umfeld-, interested parties-Analyse:

…

1.6. Informationen über die Risiko- und Compliance-Managementsystem-Leistung, einschließlich Entwicklungen bei:

1.6.1 Nichtkonformitäten, Korrekturmaßnahmen und Zeitplänen für deren Beheben

…

1.6.2 Ergebnissen von Überwachungen und Messungen:

…

1.6.3 Kommunikation mit interessierten Parteien, einschließlich Beschwerden:

…

1.6.4 Auditergebnissen:

…

1.7. Möglichkeiten zur fortlaufenden Verbesserung:

…

2. Empfehlungen:

2.1. Besteht eine Notwendigkeit von Änderungen der Risiko- und Compliance-Politik, deren zugehörigen Zielen, Systemen, Strukturen und Personal?

…

2.2. Besteht ein Bedarf für Änderungen von Risiko- und Compliance-Prozessen, um eine wirksame Integration in betriebliche Abläufe und Systeme sicherzustellen?

…

Falls ja, welche Maßnahmen sind erforderlich?

…

2.3. Gibt es Bereiche, die hinsichtlich möglicher künftiger Non-Compliance oder (neuer) wichtiger Risiken zu überwachen sind?

…

2.4. Korrekturmaßnahmen bei Non-Compliance oder Abweichungen im Risikomanagement:

…

2.5. Lücken oder Mängel im gegenwärtigen Risiko- oder Compliance-Managementsystem und längerfristige Initiativen zur fortlaufenden Verbesserung:

…

Entscheidungen des Managements:

(Die Ergebnisse der Managementbewertung sollten Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung sowie zu jeglichem Änderungsbedarf am Risiko- und Compliance-Managementsystem enthalten.)

1. …

2. …

3. …

Anlage 2: Herausgeberprofile

Prof. Dr. jur. Josef Scherer

Rechtsanwalt

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

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliancemanagement (GRC) spezialisierten Kanzlei Prof. Dr. Scherer, Dr. Rieger & Mittag Partnerschaft mbB, erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren.

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

Prof. Dr. Scherer fungiert in diversen Unternehmen / Körperschaften als Compliance-Ombudsmann sowie externer Compliancebeauftragter und ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der virtuellen Hochschule Bayern (VHB).

In Kooperation mit TÜV konzipierte er als Studiengangsleiter und Referent den seit 10 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm).

Ebenso seit 2016 Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19 AA) zur Erarbeitung von ISO/DIN-

Standards im Personalmanagement und seit

2017 Mitglied der Delegation ISO TC 309 Governance of organizations (Arbeitsausschuss Governance und Compliance NA 175-00-01-AA zur Erarbeitung von ISO/DIN-Standards im Bereich Unternehmensführung und -überwachung (Corporate Governance), Compliance und whistle blowing).

Seit 2016 fungiert er als fachlicher Leiter der „User Group Compliance“ der Energieforen Leipzig.

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Manager*ent*haftung, Governance-, Risiko- und Compliancemanagement, Integrierte Human Workflow Managementsysteme und Digitalisierung sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht, Arbeitsrecht und Personalmanagement.

Prof. Dr. Scherer ist auf dem Gebiet angewandte Forschung und Lösungen / Tools im Bereich GRC, Digitalisierung und integrierte Workflow-Managementsysteme Gesellschafter-Geschäftsführer der GRC-Process Solutions GmbH und der Governance-Solutions GmbH.

Die Veröffentlichungen (auch zum kostenlosen Download) finden Sie unter www.gmrc.de

Kontakt:

josef.scherer@th-deg.de

www.gmrc.de

Richter am Amtsgericht Klaus Fruth

Vorsitzender Richter des Schöffengerichts

Leiter der Sparte „Lehre“ am Internationalen Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf

Klaus Fruth studierte Jura an der Universität Passau.

Nach dem Staatsexamen arbeitete er in der Insolvenzverwaltung Professor Dr. Scherer. Anschließend war er mehrere Jahre Staatsanwalt bei den Staatsanwaltschaften in Deggendorf und Passau. Seit 2007 ist er Richter am Amtsgericht. Derzeit ist er beim Amtsgericht Freyung hauptsächlich als Strafrichter eingesetzt und dort als Vorsitzender des Schöffengerichtes in vielfältigen Compliance-Fällen entscheidend.

Seine Interessenschwerpunkte liegen im Bereich von Technik und Governance, Compliance, des Managerstrafrechts und des Wirtschaftsstrafrechts.

Er ist seit über 10 Jahren Lehrbeauftragter an der Technischen Hochschule Deggendorf (THD) u.a. für Governance und Compliance, Produkthaftungsrecht, Unternehmensrecht und Geschäftsführer- Compliance.

Zugleich verantwortet er an der THD im Studiengang BWL Bachelor die Durchgängigkeit eines geschlossenen Curriculums für Governance und Compliance.

Außerdem ist er Dozent u.a. für die TÜV-SÜD Akademie, sowie für die Hans-Lindner-Stiftung und im Rahmen von Inhouse-Schulungen sowie Modulverantwortlicher und Referent im berufsbegleitenden Masterstudiengang Risiko- und Compliancemanagement an der THD.

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

Er ist Leiter der Funktion „Praxis“ am Internationalen Institut für Governance, Management, Risk & Compliance.

Zusammen mit Prof. Dr. Scherer und dem Weiterbildungsinstitut der THD konzipierte er den weiterbildenden Zertifikatslehrgang „Governance, Risk und Compliance“.

Anlage 3: Bücher aus der gmrc-Reihe

www.gmrc-verlag.de

Bestellungen bitte an info@gmrc-verlag.de

- □ Scherer/Fruth (Hrsg.), Governance-Management – Band I, Grundsätze ordnungsgemäßer Unternehmensführung (GoU) und -überwachung (GoÜ): Grundsätze ordnungsgemäßer (Corporate) Governance (GoGov) (2014)
  – ISBN 978-3-00-048186-4 – Preis: 19,90 EUR

- □ Scherer/Fruth (Hrsg.), Governance-Management Band II (Standard & Audit) (2015)
  – ISBN 978-3-00-051342-8 – Preis: 19,90 EUR

- □ Scherer/Fruth (Hrsg.), Anlagenband zu Governance-Management Band II (Standard & Audit) (2016)
  – ISBN 978-3-00-053425-6 – Preis: 19,90 EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes Managementsystem „on demand“ mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-09-6 – Preis: 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes Personal-Managementsystem mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-05-8 – Preis: 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes (Compliance-) Risiko-Managementsystem mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-11-9 – Preis: 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes Compliance-Managementsystem mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-04 – Preis: 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes Qualitäts-Managementsystem mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-04-1 – Preis: 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Product Compliance, Vertragsmanagement und Qualitätsmanagement - Anlagenband zu Integriertes Qualitätsmanagement und Leistungserbringungsmanagement mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)
  – ISBN 978-3-947301-06-5 – Preis 15.- EUR

- □ Scherer/Fruth (Hrsg.), Handbuch: Einführung in ein Integriertes Einkaufs-Managementsystem mit Governance, Risk und Compliance (GRC) (mit e-Book) (2018)