Prof. Dr. Josef Scherer

Rechtsanwalt, Vorstand des Internationalen Instituts für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf. Mitglied diverser ISO/DIN-Normenausschüsse (Governance, Compliance, Personalmanagement) und von Austrian Standards International (Risiko-Managementsystem).

Giacomo Pasini

Bachelor Betriebswirtschaft, Consultant der Governance Solutions GmbH, Lehrbeauftragter an der Technischen Hochschule Deggendorf.

„Healthcare und Pflege 4.0" - Die digitale Transformation von Compliance, Risikomanagement und Standards im Gesundheitswesen – Teil 3

Integration von Standards in digitalisierte, vernetzte Managementsysteme

(Fortsetzung aus JMG 2/2019, S. 109–119)

Sofern Standards den geforderten Entwicklungsstand widerspiegeln oder „strenger" sind, ist es sinnvoll, sich angemessen an passenden Standards zu orientieren. Standards können „strafbarkeitskonstituierend" wirken.

Gerichte fordern mehr, als das bloße Einhalten von Standards. Sicherheit geht stets vor. Zertifizierte Sicherheit reicht unter Umständen noch nicht einmal.

Der Aufbau der vielen Standards differiert zum Teil sehr stark, die Inhalte dagegen glücklicherweise weniger.

Welche Struktur nun logischer/sinnvoller/besser für ein Integriertes System geeignet ist, sei dahingestellt, da all die existierenden Strukturen eine gemeinsame Schwachstelle aufweisen: Sie sind streng linear aufgesetzt – unser Gehirn selbst und eine Organisation jedoch arbeitet nicht linear, sondern vernetzt und iterativ.

Business Process Model and Notation (BPMN) ist ein Industriestandard, der weltweit zur grafischen Darstellung und Modellierung von Geschäftsprozessen eingesetzt wird.

Neuartige Technologien erlauben die Interpretation und Vernetzung der BPMN mit den 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.

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.

1. Rechtliche Einordnung von „Standards" und Rechtsfolgen bei Verstößen

1.1 Rechtsqualität von Standards

Unter Umständen mögen „*Standards*" **(Regeln und Regelwerke institutionalisierter Sachverständigengremien (ISO/DIN/ÖNORM/VDE/VDI/IDW/OECD/COSO/DIIR/…)** den *„Anerkannten Stand von Wissenschaft und Praxis*" widerspiegeln.

Dies gilt es jedoch, im Einzelfall zu prüfen.[1]

Es gibt in Deutschland nach geltender Verfassung nur **drei (!) Gewalten: Legislative, Judikative und Exekutive.**

Sachverständige gehören **nicht** dazu.

Da die nachfolgend als ***„Standards"*** bezeichneten Anforderungen, Regeln und Regelwerke (zB DIN/ISO 9001:2015 für Qualitätsmanagement als der verbreitetste und am häufigsten zertifizierte Standard, aber auch DIN/ISO 19600:2014/COSO I:2013/IDW PS 980:2011/ONR 192050:2013/etc für Compliancemanagement[2]) **von** nicht hoheitlich tätigen, sondern

1 Vgl *Birklbauer*, Die Bedeutung von (medizinischen) Leitlinien im Strafrecht, JMG 1/2019, 16-23.

2 Kontinuierlich befinden sich zahlreiche weitere Standards im Entstehen. ZB erarbeitet das ISO Technical Committee 260 (ISO TC 260) Personalmanagement-Standards (der erste mit „Definitionen" wurde 2016 verabschiedet) und das IDW verabschiedete 2017 die Prüfungs-Standards IDW PS 981, 982 und 983 für Risikomanagement, IKS und Revision.

privatrechtlich organisierten „Sachverständigengremien“ (DIN/ISO/VDI/VDE/IDW/OECD / …) **erlassen** werden, sind **Standards idR nicht durch eine der drei Gewalten legitimiert.**

Deshalb stellen sie auch **keine Rechtsnormen** dar. Auch als Auslegungsregeln für den Gesetzgeber oder die Rechtsprechung dürfen sie keine Anwendung finden, da keine Beeinflussung des Gesetzgebers oder der Judikative durch private Institutionen stattfinden darf.

Gerade deshalb fungieren sie auch **nicht** als „freiwillige Selbstbindung“ der **Gerichte**. Letztere **werden in keiner Weise *gebunden***, sich durch Vorgaben von Standards auf der Beurteilungsebene beeinflussen zu lassen.

Fall: „Luftschallschutz“
„(…) Liegt eine derartige Vereinbarung nicht vor, ist die Werkleistung im Allgemeinen mangelhaft, wenn sie nicht den zur Zeit der Abnahme anerkannten Regeln der Technik als vertraglichem Mindeststandard entspricht.
Die DIN-Normen sind keine Rechtsnormen, sondern private technische Regelungen mit Empfehlungscharakter. Sie können die anerkannten Regeln der Technik wiedergeben oder hinter diesen zurückbleiben.“[3]

Sachverständige fungieren lediglich als Hilfe, um Sachverstand von Legislative, Judikative und Exekutive anzureichern. Dabei können „*Standards*“ unter bestimmten Voraussetzungen als sogenannte „*antizipierte Sachverständigengutachten*“ anzusehen sein.

Jüngst wurde Standards vom Vorsitzenden Richter *Raum* des ersten Strafsenats des *BGH* eine „*unter Umständen strafbarkeitskonstituierende Wirkung*“ *zugesprochen.*[4]

Praxistipp:
Die **Nichteinhaltung von Standards kann** eine **Pflichtverletzung** bedeuten, wenn diese Standards aktuelle Gesetze, Rechtsprechung oder den Anerkannten Stand von Wissenschaft und Praxis widerspiegeln.
Es ist allemal sinnvoll, die **Vorgaben diverser aktueller Standards als *Mindest*voraussetzungen** für ein angemessenes Managementsystem zu behandeln, um sowohl strafrechtlich auf der Ebene der Pflichtwidrigkeit sowie Vorwerfbarkeit und des Verschuldens und zivilrechtlich bei der Frage der Pflichtverletzung und Fahrlässigkeit auf „Nummer sicher“ zu gehen.
Bei entsprechender Gefährdungslage trotz Einhaltung relevanter Standards sind weitere Steuerungsmaßnahmen erforderlich.

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:[5]

Beispiel: In Bankenkreisen war der „*Anerkannte Stand von Wissenschaft und Praxis*“ wohl schon wesentlich anspruchsvoller, als es die „*MaRisk*“ in der bis 2017 geltenden Fassung forderte.

1.2 Nichtbeachtung von Standards als Pflichtverletzung

Zahlreiche anschauliche **Beispielsfälle** aus der Rechtsprechung zeigen, dass **Nichteinhaltung von *Standards als Pflichtverletzung* Haftung und Strafbarkeit von Management und Mitarbeitern zur Folge haben können.**

Fall: „Standardwidrige Unternehmensberatung“[6]
Dieser Fall handelt von einer Unternehmensberatung und einem sich in wirtschaftlichen Schwierigkeiten befindenden Unternehmen im Streit um Honoraransprüche aus einer betrieblichen Beratung.
Ein Sachverständiger stellte fest, die Arbeiten des Unternehmensberaters seien praktisch unbrauchbar.
Weiter stellte das *Gericht* fest, die angewandten Geschäftsmethoden verstießen gegen das Gesetz und seien sittenwidrig. Hier läge ein Betrug vor und es

3 *BGH*, Urteil vom 14.05.1998, Az. VII ZR 184/97, Amtlicher Leitsatz, NJW 1998, 649 f.
4 *Raum* in *Hastenrath*, Compliance – Kommunikation, 2. Aufl., 2017, 31 f.
5 Vgl *Scherer*, Wieviel Standard braucht der Mensch? – Zum Anwendungsbereich von Standards, 2019 (www.scherer-grc.net).
6 Vgl. *Scherer/Fruth* (Hrsg), Anlagenband zu Governance-Management, Band 1, 2014, Anlage 5.

gelte § 826 BGB, weil es unwahrscheinlich sei, dass dem Berater sowohl die tatsächlichen Mängel seines Gutachtens, als auch der *Verstoß gegen die Bearbeitungsrichtlinien* nicht bekannt gewesen seien. Die „*Richtlinien des Bundeswirtschaftsministeriums zur Unternehmensberatung*“ seien vorsätzlich nicht beachtet worden und dies habe zur Ungeeignetheit der Arbeiten beigetragen.[7]

Fall: „Hygienestandard“
Das *OLG Hamm*[8] beurteilte den Fall, in dem ein Krankenhauspfleger eine Abszedierung an der Hand einer Patientin öffnete, dabei aber Handschuhe trug, mit denen er zuvor die Türklinke des Krankenzimmers berührt hatte, als Verstoß gegen den „*medizinischen Hygienestandard*“ und damit als Pflichtverstoß.[9]

1.3 Pflichtverletzung *trotz Einhaltung von Standards* aufgrund weiterbestehender Gefährdungslage

Gerichte fordern *mehr,* als das bloße Einhalten von Standards. Sicherheit geht stets vor. Zertifizierte Sicherheit reicht unter Umständen nicht:

Fall: „Zer-*malm*“-endes Wandregal
Das *Wandregal* eines schwedischen Möbelherstellers hatte vier Füße, sollte aber entsprechend den Standards für „Wandregale“ gemäß Gebrauchsanweisung fest an der Wand verankert werden.
In den USA wurden Kleinkinder von diesen Regalen erschlagen, weil sie nicht – wie vorgesehen – an der Wand befestigt, sondern lediglich – nicht standsicher – aufgestellt wurden.
Der Hersteller hatte den in den USA geltenden Sicherheitsstandard für *freistehende* Kommoden nicht eingehalten.
Reichlich spät wurden ca 36 Millionen Kommoden zurückgerufen.[10]
Nach ständiger Rechtsprechung und **Gesetz muss ein Hersteller bzw Verkehrssicherungspflichtiger bei der Produkt-Sicherheit auch mit *naheliegender Fehlanwendung* rechnen und konstruktive Sicherheit etwaigen Warnhinweisen vorziehen.**

Fall: „CE-Kennzeichnung“
Ein Ball, der an einem Gummiband befestigt war und eine **CE-Kennzeichnung** gemäß der EG-Spielzeugrichtlinie 88/378/EWG trug, **verletzte dennoch ein Kind am Auge**.
Das *Landgericht Osnabrück* verurteilte den Hersteller zu Schadensersatzansprüchen aus dem Produkthaftungsgesetz: Die **Einhaltung der produktsicherheitsrechtlichen Vorgaben bedeute keine produkthaftungsrechtliche Sicherheit**.[11]

Fall: „Eishockey-Puck und Sicherheitsstandards“[12]:
Ein Eishockey-Verein wurde von einer Zuschauerin, die durch einen Puck verletzt worden war, auf Schadenersatz verklagt, da abgesehen von den seitlich angebrachten Plexiglasbanden keine zusätzlichen Schutznetze angebracht worden waren.[13]
„*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*

7 Anmerkung: Unsere Kanzlei verklagte jüngst einen Sanierungsberater wegen eines fehlerhaften Sanierungsgutachtens auf Schadenersatz in Millionenhöhe, weil aufgrund des fehlerhaften Gutachtens zu spät Insolvenz angemeldet wurde.
8 Vgl *OLG Hamm*, Urteil vom 17.8.2015, 3 U 28/15.
9 Sofern ausgeführt wird „das OLG folge dem medizinischen Sachverständigen, dass ein Hygieneverstoß umso schwerer wiege und umso unverständlicher sei, je höher das Infektionsrisiko und je gravierender die Folgen einer möglichen Infektion sein könnten“ (es wurde aus klinischer Sicht eine Differenzierung in vier Risikogruppen vorgenommen), sind dies klassische Komponenten einer Risikobewertungsmethode.
10 Vgl *Die Welt* online unter https://www.welt.de/wirtschaft/article156658933/Ikea-ruft-in-USA-36-Millionen-Malm-Kommoden-zurueck.html vom 28.06.2016, Aufrufdatum: 17.09.2016.
11 Vgl *Scherer/Fruth* (Hrsg), Wer den Schaden hat…, Band 1, 2006, 136.
12 Hinweisbeschluss des *OLG Nürnberg* vom 6.7.2015, Az. 4 U 804/15.
13 Vgl o A, Fans müssen vor Pucks geschützt werden, abrufbar unter: www.lto.de/recht/nachrichten/n/lg-regensburg-3-o-1702-10-haftung-puck-zuschauer-eishockey vom 17.09.2015, Abrufdatum: 27.03.2019.

Veranstaltung die nicht nur geringe Wahrscheinlichkeit eines Unfalls mit der Gefahr nicht unerheblicher Verletzungen mit sich bringt."

2. Schwachstelle bei Standards und Organisationsstrukturen: Ein streng linearer Aufbau

2.1 Managementsystem-Standards sollen helfen, die Organisationsstrukturen zu verbessern.

Der Aufbau der vielen Managementsystem-Standards differiert zum Teil sehr stark, die Inhalte dagegen glücklicherweise weniger.[14] 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[15]:

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

Anders strukturiert sind Standards anderer Institutionen, wie COSO, IDW, DIIR, diverse ÖNormen etc.

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 (1., 2., 3., 4. etc), so wie unsere bürokratische *Denkweise* und Organisationssysteme seit Tausenden von Jahren – unser *Gehirn* selbst jedoch arbeitet nicht linear, sondern vernetzt und iterativ.

2.2 Partielle, vollständige und vernetzte Schrift-, Informations- und Organisationssysteme im Wandel der Zeit

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 Bedeutung für organisatorische Zwecke zu (Assetmanagement: Verwaltung von Grundstücken, Vorräten etc). 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.[16]

Partielle und vollständige Schriftsysteme

Als „*Technik zur Speicherung und Verarbeitung von Information mittels physischer Zeichen*"[17] 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*"[18], 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.[19]

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[20] und trotz loser Verknüpfungen[21] in Sekundenschnelle abgerufen werden können, sind für ein funktionierendes Datenverarbei-

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

15 2018 erschien der sehr prominente **ISO-Standard für Risiko-Managementsysteme (ISO 31000:2018) und wies überraschenderweise keine High Level Structure (HLS) mehr auf.** Dies versucht nun die ÖNORM 4900 ff.: 2020 für Risiko-Managementsysteme zu kompensieren, die sich an der HLS orientiert und zertifizierbar ist.

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

17 *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 155 ff.

18 *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 156 ff.

19 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 158 ff.

20 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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."*

21 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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."*

tungssystem Kataloge und Ordner-/Suchsysteme sowie Verantwortliche, die sie zu bedienen wissen, vonnöten.[22] Insbesondere Letztere 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.[23]

Im Zuge der wachsenden Popularität von Datenverarbeitungssystemen ließ sich eine Tendenz weg vom natürlichen menschlichen, ganzheitlichen Denken[24] hin zu Bürokratie und Kästchendenken erkennen.[25]

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“[26]. Nahezu alle Staaten, Unternehmen uvm 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.[27]

2.4 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 einzelner Aktivitäten mit Information mittels physischer Zeichen, die die jeweils gesprochene Sprache nahezu lückenlos wiedergibt, ergänzt („partielles Schriftsystem“). 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 zur Erfüllung ihrer Tätigkeiten versorgen. Diese Daten bilden eine Basis für Workflowmanagement-Systeme.

Neuartige Technologien erlauben die Interpretation und Vernetzung von BPMN mit den 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.

Nutzung der mathematischen Schrift zu „gehirnähnlichen“ Methoden der Vernetzung von Informationen im digitalen Zeitalter

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 wer-

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

23 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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.“*

24 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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.“*

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

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

27 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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“.*

den, in eine bestimmte Aneinanderkettung dieser beiden Ziffern übersetzt.[28] Auf Basis dieses Systems wird im Forschungsgebiet der „Künstlichen Intelligenz" (KI) versucht, „eine neue Art der Intelligenz zu schaffen"[29].

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

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"[30] 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* (zB 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.[31]

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":

3. Von theoretischen, unflexiblen und ungelebten Managementsystem-Insellösungen in Richtung flexibles und vernetztes Integriertes Managementsystem

3.1 Redundante Komponenten diverser Managementsystem-Inseln

Die „*Deggendorfer Schule*"[32] geht davon aus, dass in allen existierenden (QM-, Risk-, Compliance-, Nachhaltigkeits-, Informationssicherheits-, etc.-) Managementsystem-Standards (auch außerhalb von ISO: zB bei COSO, IDW, DIIR, ÖNORM etc) eine Vielzahl ähnlicher Inhalte/Komponenten zu finden sind und versucht, den gemeinsamen Nenner darzustellen:[33]

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

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, findet sich nahezu in jedem Standard:

ISO 9001: 2015 (Qualitätsmanagementsystem)
„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien"
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"

28 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015,.166 ff.

29 Vgl *Harari*, Eine kurze Geschichte der Menschheit, 25. Auflage, 2015, 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. […]"*

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

31 *Scherer*, Managerenthaftung und digitale Transformation versus Unvernunft im Lichte aktueller Rechtsprechung des Bundesgerichtshofs, FIRM Jahrbuch, 2018, 74 ff. (www.scherer-grc.net) und *Scherer/Fruth* (Hrsg), Handbuch: Integriertes Managementsystem (IMS) „on demand" mit Governance, Risk und Compliance (GRC), 2018.

32 Als *„Deggendorfer Schule"* bezeichnet das Netzwerk um das *Internationale Institut für Governance, Management, Risk und Compliance* diverse neue Ansätze zur Geschäftsprozess-Digitalisierung und von Integrierten Human Workflow-Managementsystemen (www.gmrc.de).

33 Vgl hierzu auch die ÖNORM Leitfaden 4901-1 „Einbettung von Risiko-Management ins Managementsystem.

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

PAS 99: 2012 (Integriertes Management System)

„4.2 Understanding the needs and expectations of interested parties"

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.": „Ziel (…) ist es, ein zutreffendes Bild (…) von den mit dieser Entwicklung einhergehenden Chancen und Risiken zu machen."

„37.": „(…) g) externen Einflussfaktoren für das Geschäft."

„59.": „(…) sind die gesamtwirtschaftlichen und branchenbezogenen Rahmenbedingungen (…) darzustellen und zu erläutern."

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. (…) Fokuspunkt 35: Beurteilt Veränderungen in externer Umwelt."

etc.

Diese Komponente „*Interested parties-Analyse*" ist also nur ein einziges Mal durchzuführen und erfüllt zugleich die Anforderungen zahlreicher Managementsystem-Inseln: Über einen Datenraum mit Zugriffsberechtigungen für relevante Adressaten werden diese Informationen zentral zur Verfügung gestellt: Effektivität und Effizienz zugleich!

3.2 Die Vernetzung der Komponenten von Normen, Richtlinien und Standards in einem Integrierten Workflow-Managementsystem

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

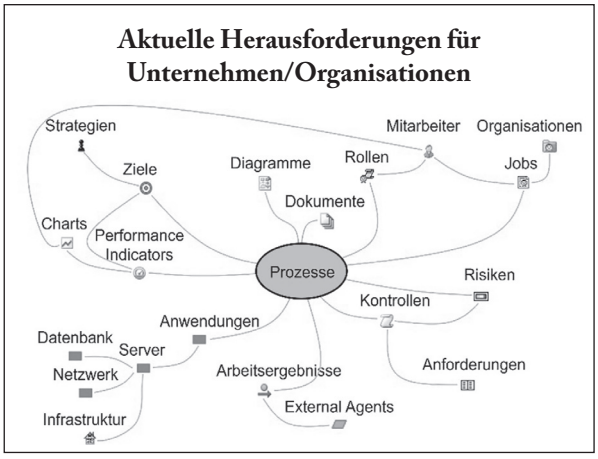

Abbildung 1: Vernetzung der Komponenten eines Managementsystems auf Basis von Prozessabläufen.

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

Mit einem Integrierten Human-Workflow-Managementsystem werden die einzelnen Komponenten eines beliebigen N.N.-Managementsystems mit Fokus auf die Unternehmensprozesse in logische Beziehung gesetzt.

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 streng 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 „überset-*

zen " und die jeweiligen Abläufe den relevanten Prozessschritten zuzuordnen:

Beispiel: „Lieferantenmanagement und „Supplier screening"
Zurück zum „Skandal im Medizinprodukte-Bereich" (vgl Teil 1, Punkt 1.1): Ein wesentliches Element zur Vermeidung von Problemen ist ua die Sicherung der Qualität/Sicherheit von fremdbezogenen Leistungen/ Produkten via Lieferantenmanagement und „Supplier screening".

Beispiel: „Compliance"
Das *Handelsgesetzbuch* (*HGB) (D) oder Unternehmensgesetzbuch (UGB) (A)*: Ein „Rechtskataster", das aufführt, dass in den Abteilungen Einkauf und Vertrieb „das *HGB/UGB*" zur Anwendung komme, ist sinnlos (und kostet nur Geld).
Das *HGB/UGB* muss also erst *fragmentiert und die relevanten Normen daraus übersetzt in Anforderungen und daraus resultierenden Maßnahmen den richtigen Prozessschritten zugeordnet werden:*

Beispiel: „Wareneingangsprüfung"
Die Obliegenheit zur unverzüglichen Untersuchung der Ware und Rüge gemäß § 377 HGB/UGB im Rahmen der Wareneingangslogistik[34]:

Diese **fragmentierte / herausgelöste Anforderung** (§ 377 HGB / UGB) aus dem gesamten Handels-

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 2: Compliance-, Risiko-, IKS-, etc-Steckbrief in Anlehnung an IDW PS 951

34 **§ 377 HGB/UGB:**
(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) […]

gesetzbuch könnte zunächst in **einen „Compliance-, Risiko-, IKS-, etc-Steckbrief“ „übersetzt“** und dem relevanten Prozessschritt des Einkaufsprozesses zugeordnet werden.

Sehr häufig sind die Texte von Gesetzen, Richtlinien oder Standards für die betroffenen Mitarbeiter, die die daraus resultierenden Anforderungen zu erfüllen haben, völlig unverständlich.[35]

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

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 mit den Prozessen:

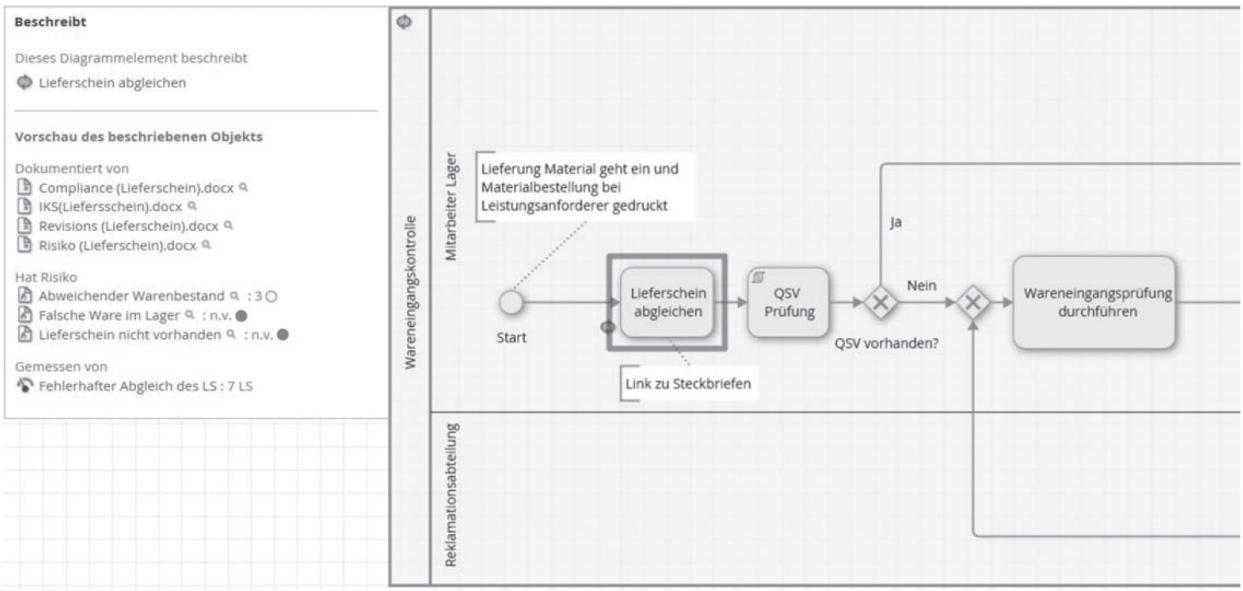

Abbildung 3: Wareneingangskontrolle in GRC-PS - I.

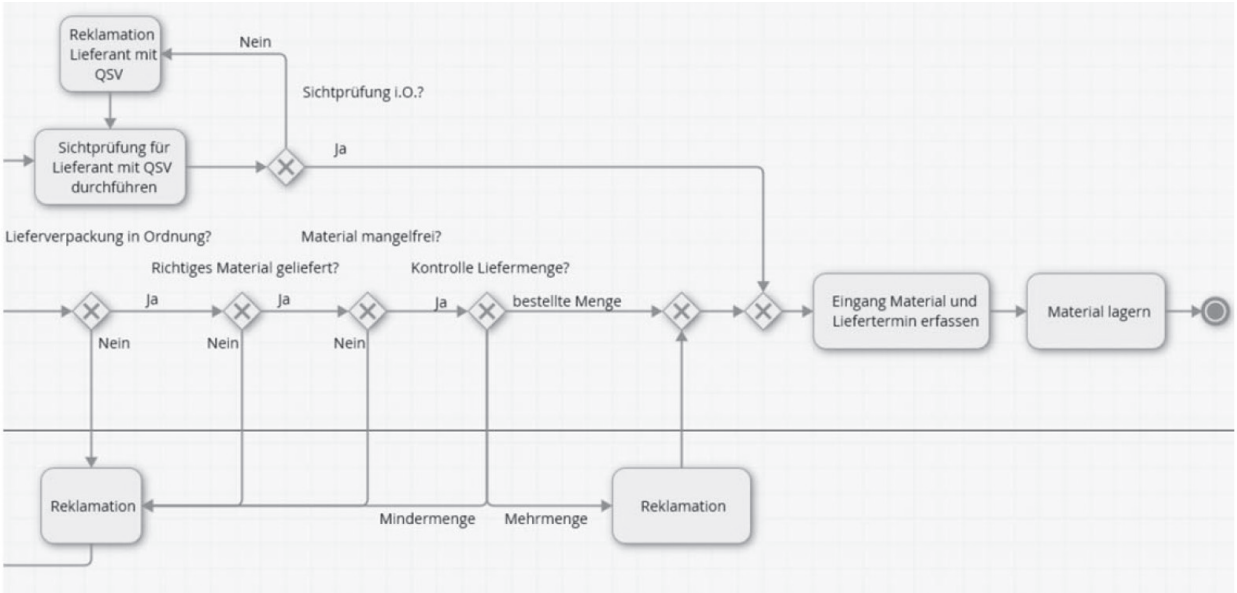

Abbildung 4: Wareneingangskontrolle in GRC-PS - II.

35 Beispiel: § 164 BGB: „*Tritt der Wille, in fremdem Namen zu handeln, nicht erkennbar hervor, so kommt der Mangel des Willens, im eigenen Namen zu handeln, nicht in Betracht.*“

Es empfiehlt sich außerdem, 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

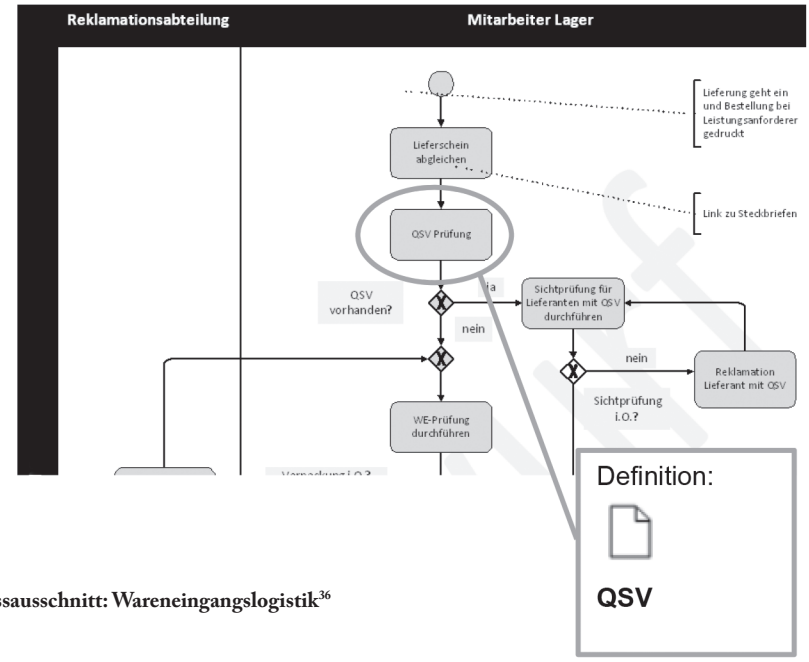

Abbildung 5: Prozessausschnitt: Wareneingangslogistik[36]

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 könnten in den Prozessabläufen sogar noch **Kurz-Lehrfilme** zu sensiblen Handlungsabläufen an relevanten Stellen verlinkt sein.

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

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

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

Der *Risiko-Beauftragte* ist zB Adressat der Mitteilungen aufmerksamer Mitarbeiter bzgl Gefahren und Chancen.

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

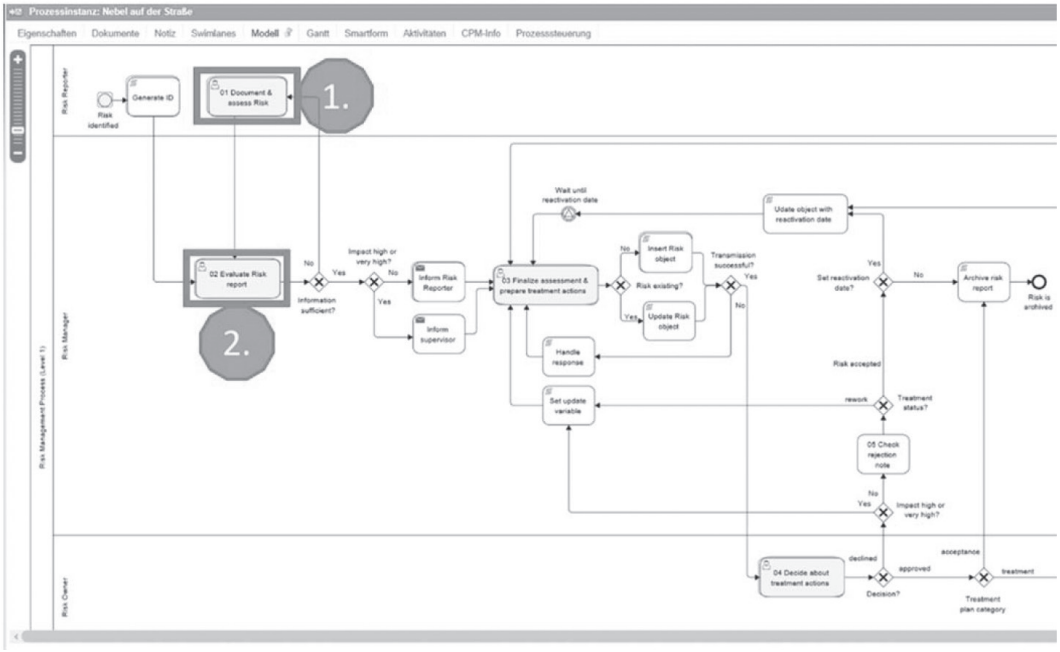

Abbildung 6: Risk-Management-Prozess: Prozessmodell (Teil 1).

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

Das Steuerungs- und Überwachungssystem („Check und Act“) würde *in einer vernetzten,* also nicht bürokratisch-linear ablaufenden *Organisation* die Punkte „Plan“ und „Do“ des Deming-Kreislaufs *parallel* mit Soll-Ist-Abgleich, Kennzahlenermittlung, Eskalationsprozess, Monitoring, Reporting, Dokumentation *begleiten* und *nicht erst* chronologisch *nachfolgend* zum Einsatz kommen, wenn „das Kind evtl schon in den Brunnen gefallen“ ist.

Jederzeit kann – logischerweise – bei (automatisierten) Workflow-Prozessen in Echtzeit überwacht, eskaliert oder auch über den Soll-Ist-Zustand „per Knopfdruck“ berichtet werden:

Das Zeitalter des aufwändigen Erstellens von Berichten, die aus Hochglanz-Powerpoint-Folien und

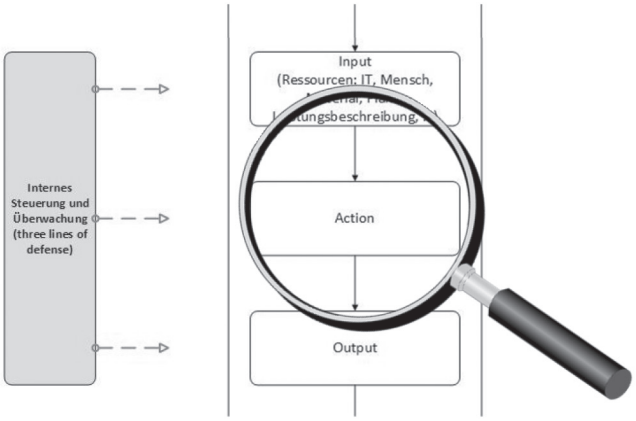

Abbildung 7: Begleitende Steuerung und Überwachung.

Excel-Friedhöfen mit bereits bei Präsentation abgelaufener Halbwertszeit bestehen, dürfte damit ein Ende finden … ***Fortsetzung folgt!***

Abbildung 8: Risk-Management-Prozess: Reporting-Dashboard.