2017

Jahrbuch
Yearbook

FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

Die „Welt(en) der Überwacher“: Enormes Potenzial für Effektivität, Effizienz und Wertbeiträge bei Governance, Risk & Compliance (GRC)

Josef Scherer

Die Ausgestaltung diverser Überwachungs-Systeme als eigenständige Systeme ist möglich. Dieser Text stellt jedoch wahlweise einen neuen Ansatz eines integrierbaren („GRC“) Überwachungs-System dar. Dies erwies sich in Theorie und Praxis als schlüssig und geeignet, die vielen Unternehmensfunktionen, wie Governance, Qualitäts-, Risiko-, Compliancemanagement, Internes Steuerungs- und Überwachungssystem, Revision, etc., zu vernetzen, dadurch Redundanzen und Insellösungen zu vermeiden und erhebliche Synergien zu gewinnen.

Es wird mithilfe des „Universal“-Standards Überwachungs-Management (zum Download auf www.gmrc.de) versucht, aufzuzeigen, dass die meisten Standardwerke auf einem „gemeinsamen Nenner“ beruhen, wenngleich sie auch in Aufbau oder Formulierungen differieren mögen.

In der Unternehmenspraxis existiert eine Vielzahl interner und externer Prüfungs-/Überwachungs-/Audit-/Konformitätsbewertungs- Funktionen:

- 1st line of defense: Mitarbeiter und Kollegen, Vorgesetzte, Vorstand/Geschäftsführer.
- 2nd line of defense: Controlling, IKS, Risikomanagement, Compliance, Qualitätsmanagement sowie weitere Funktionen.
- 3rd line of defense: Revision, Assurance/Internal Investigation.
- 4th line of defense: Aufsichtsrat, Medien, Third parties (audits), Staatsanwälte, Behörden, Politik, Banken, Gerichte (Straf-, Zivil-, Verwaltungsgerichte) etc.

Diese „Überwacher“ gehen leider in der Praxis nicht konzertiert, sondern nebeneinander agierend vor, obwohl sie alle im Wesentlichen die gleichen Ziele verfolgen: Transparenz über die Anforderungen, um die Unternehmensziele zu erreichen sowie adäquate, auf diese Ziele abgestimmte Kennzahlen und gelebte Prozesse, die mit den diversen Muss- und Soll-Anforderungen angereichert sind, um den beabsichtigten Output zu gewährleisten. Flankiert wird dies durch ein angemessenes und wirksames Steuerungs- und Überwachungssystem.

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

Abgeleitet aus dem „Sarbanes Oxley Act“ (SOX) sowie COSO, agieren national und international Wirtschafts- und Abschlussprüfer mit eigenen Prüfstandards (beispielsweise IDW/IAS), die zum Teil zwischen Konzeptionierungs-, Angemessenheits- und Implementierungs- sowie Wirksamkeitsprüfung differenzieren. Für die „Wirtschaftsprüfungs-Welt“ ist beispielsweise IDW EPS 981:2017 (Risiko-Managementsysteme) oder IDW PS 341 (Risiko-Früherkennungssystem) relevant, genauso aber auch COSO II:2004 (Enterprise Risk Management) beziehungsweise künftig COSO II:2017 (Risk Aligned with Strategy and Performance).

Für Third-Party-Audits (beispielsweise Zertifizierungen für Kunden, weil gefordert, oder um damit zu werben) bietet die internationale ISO-Welt für Managementsysteme meist Wirksamkeitszertifizierungen / -audits an (wobei ISO 31000:2009 [neue Version soll 2017/2018 erscheinen] nicht zertifizierbar ist, weshalb für die Zertifizierung durch grundsätzliche ISO-Zertifizierer auch andere Standards [beispielsweise ONR 49000, die direkt auf die ISO 31000:2009 referenziert] herangezogen werden).

Nicht zu vergessen die „Welt der Revision“: beispielsweise in Deutschland die Standards des „Deutschen Instituts für Interne Revision“ (DIIR) oder global die Standards des „Institute of Internal Auditors“ (IIA). So existieren auch hier einschlägige Audit-Standards, beispielsweise DIIR Nr. 2:2014 (Prüfung des (Compliance-)Risikomanagements).

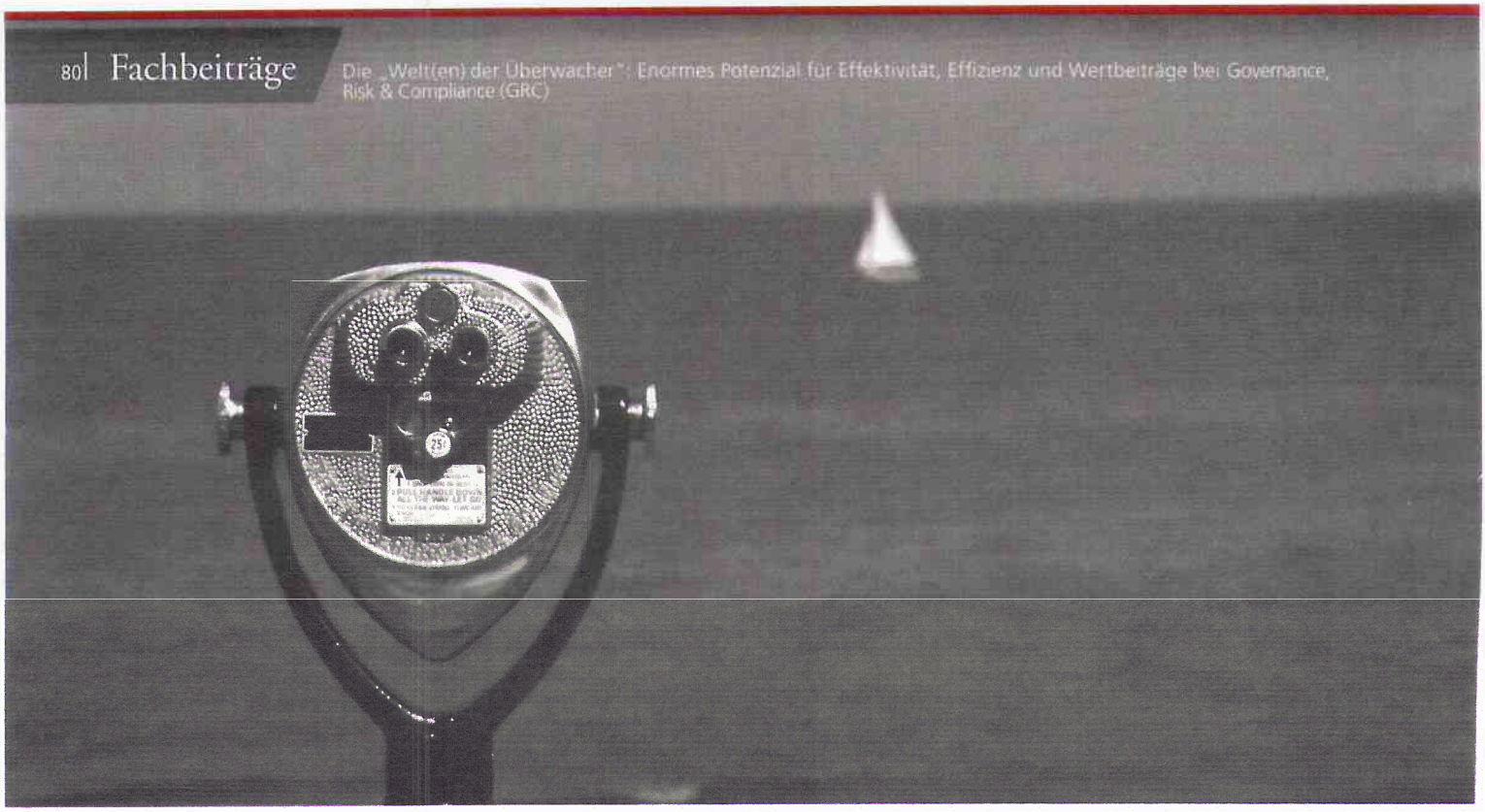
Die Welt der Revision (aber auch Aufsichtsbehörden oder die Staatsanwaltschaft) hinterfragen die Wirksamkeit, beruhend auf angemessenem Konzept und Implementierung.

Sinnvoll scheint hier eine Harmonisierung mit dem Ziel: „best of both/ three/four/... worlds“. Am Beispiel der Komponente „Anforderungen der interested parties“, die nahezu von jedem Standard gefordert wird, lässt sich die einfache Möglichkeit zur Auflösung von Redundanzen gut aufzeigen.

Aufgrund der veränderten technologischen Umwelt, die durch neue Möglichkeiten der Kommunikation erhöhte Präsenz und Transparenz gerade auch bei Ereignissen gewährleistet, die zu enormen Reputationsrisiken führen, verdient das Thema „interested parties“ in der Praxis eine wesentlich stärkere Beachtung. Dies spiegelt sich auch in den Anforderungen von „Industrie 4.0“ und den neueren Standards (ISO/IDW/G20/OECD Principles of Corporate Governance etc.) wider.

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

„4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien



*Aufgrund ihres Einflusses bzw. ihres potentiellen Einflusses auf die Fähigkeit der Organisation zur fortlaufenden Bereitstellung von Produkten und Dienstleistungen, die die Anforderungen der Kunden und die zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen, muss die Organisation: **a) die interessierten Parteien**, die für ihr Qualitätsmanagementsystem relevant sind, **b) die Anforderungen dieser interessierten Parteien**, die für ihr Qualitätsmanagementsystem relevant sind, **bestimmen**."*

Anmerkung: Es fehlt meines Erachtens als Anforderung, bestimmten Anforderungen zu bewerten (mit angemessenen Risikomanagementmethoden!) und daraus abgeleitete erforderliche Maßnahmen umzusetzen.

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

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

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

Gegenüberstellung (Synopse) mit anderen Standard-Texten, die das Gleiche (nicht das Selbe) fordern:
ISO 19600: 2014 (Compliance-Management):
„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 (...)"

Ähnlich IDW PS 981: 2017 (Risiko-Managementsystem):
„7.3.1 Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichen und wirtschaftlichen Umfeld".

ONR 192050: 2013 (Compliance-Management-Systeme):
Hier ist keine entsprechende Anforderung ersichtlich.
COSO I: 2013 (Internal Control):
Hier ist keine entsprechende ausdrückliche Forderung ersichtlich. Jedoch existieren Anforderungen, die zumindest mittelbar auch die „interessierten Gruppen" betreffen:

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

PAS 99: 2012 (Integriertes Management System)
„4.2 Understanding the needs and expectations of interested parties"

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

Auch der **DRS Nr. 20:2013 (Lageberichterstattung)** und die **ISO 37001:2016 (Antikorruption)** verlangen die Berücksichtigung der **„interested parties"**.

Ebenso läuft es mit allen anderen Komponenten der diversen Standards: Auch die Forderung nach Durchführung einer Unternehmensanalyse (organization's internal context) findet sich in nahezu jedem Standard. Diese als einzelne Komponenten darstellbaren redundanten Anforderungen sind jeweils nur ein einziges Mal (!) abzuarbeiten.

Weiteres Beispiel: Jede Überwachungsfunktion (Controlling / Risikomanagement / Compliance / Audits / Revision etc.) verlangt dokumentierte Prozessabläufe, die diverse Anforderungen (effektiv, qualitativ, rechtssicher, technisch sicher, effizient etc.) erfüllen: Ein einziges Prozess-Audit kann den erforderlichen Soll-/Ist-Abgleich durchführen.

Bei der Vielzahl der aufgeführten Überwachungsmaßnahmen – hier beispielsweise bezüglich der Existenz einer „interested parties", Unternehmensanalyse oder korrekte Prozesse – gibt es eine riesige Überschneidung und damit enormes Einsparungspotenzial, wenn beispielsweise durch eine zentrale Funktion – abgestimmt mit den übrigen Themengebieten – die immer wieder gleichen Checks (Dokumenten-,/ Prozess-,/ workflow-Prüfungen / Interviews etc.) durchgeführt und die Erkenntnisse verteilt werden.

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

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

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

Die vielen redundanten und analogen Anforderungen / Komponenten lassen sich auch wunderbar einem aus den diversen sehr ähnlichen gängigen Standards der diversen „Überwacher-Welten" komprimierten **„Universal-Kombi-Standard („on demand")** zuordnen (und mit einem **„Kombi-Zertifikat"** testieren). Der Standard *Universal-Standard Compliance-Managementsystem* mit synoptischer Darstellung der analogen Anforderungen bei ISO, COSO und IDW findet sich zum kostenlosen Download auf www.gmrc.de:

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

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

Wertbeitrag und Wert eines Integrierten Managementsystems

„Wenn in den diversen einzelnen Unternehmensfunktionen/ Prozessfeldern/ Themenbereichen, oder bei (Corporate) Governance generell („GRC als Klammer") ein ***hoher Reifegrad*** *erreicht wird, resultiert daraus* ***automatisch*** *ein* ***hoher Nachhaltigkeitsgrad, Wertbeitrag und Pflichterfüllungsgrad.*** *Damit werden die Ziele von Unternehmen, Management und Mitarbeitern mit hoher Wahrscheinlichkeit erreicht und es entsteht* ***somit auch ein hoher Zielerreichungsgrad.*** *" [Scherer/Fruth 2016].*

Auch *Achleitner* ist der Ansicht, dass „Corporate Governance ein wichtiger Werttreiber" wird/ist [Achleitner 2015, S. 28]:

„Die operative Wertschöpfung wird die größte Herausforderung für die Unternehmen (...) in Zukunft sein. (...) In den vergangenen Jahren stand Corporate Governance in den notierten und öffentlichen Unternehmen oft unter dem Überwachungsaspekt. Der wertschöpfende Aspekt fehlte dagegen. Es geht um bessere unternehmerische Entscheidungen durch funktionierende und gelebte Governance im besten unternehmerischen Sinne. (...)Eine gute Corporate-Governance-Praxis wird ein entscheidender Wettbewerbsfaktor in der Zukunft (...) aus der Beteiligungspraxis hören sie, dass es Fälle gibt, in denen die Corporate Governance zwei Drittel der Wertsteigerung der Firmen beisteuert. (...)"

Literatur

Achleitner, P. [2015]: Corporate Governance als Werttreiber, in: Handelsblatt, 30.06.2015, S. 28.

Scherer J./ J./Fruth, K. (Hrsg.) [2016]: Governance-Management Band II (Standard und Audit), 2016.

Autor

Prof. Dr. jur. Josef Scherer

Internationales Institut für Governance, Management, Risk- und Compliance Management der Technischen Hochschule Deggendorf sowie Mitglied des FIRM-Beirats