Qualitäts-, Risiko-, Compliance- und Managementsysteme: ein Universal-Standard verbindet ISO, COSO und IDW-Standards

Weltweit richten sich Unternehmen bei der Implementierung beispielsweise eines Compliance-Managementsystems nach Standards wie ISO 19600:2014, COSO I:2013, IDW PS 980:2012. Das Internationale Institut für Governance, Management, Risk & Compliance der TH Deggendorf hat jetzt einen integrierten Ansatz entwickelt, der diese und viele weitere Standards berücksichtigt und zu einem integrierten GRC-Managementsystem zusammenführt.

Im Gespräch mit Professor Dr. jur. Scherer erfahren Sie Hintergründe und Zielsetzung des "Universal-Standards" in Bezug auf die Bedeutung und Implementierung von Qualitäts- Risiko- & Compliancesystemen.

3GRC: Herr Professor Scherer, was hat Sie und Ihre Kollegen dazu veranlasst, einen "Universal-Standard" für Compliancemanagement-Systeme zu entwickeln?

Die Kernmessage ist, dass sich im Zeitalter der Digitalisierung alles um Prozessabläufe dreht. Diese wiederum müssen die diversen Anforderungen von Qualitätsmanagement, Risk und Compliance erfüllen. Und zwar idealerweise so, wie von den vielfältigen Standards vorgegeben (oder besser).

Im digitalen Zeitalter wird auch in vielen Unternehmen überwiegend mit E-Mails und MS Office kommuniziert. Definierte Verfahrens- und Prozessabläufe werden in der Praxis häufig nicht genutzt. Dabei ist es umso wichtiger, dass die Prozesse aktuell und nachvollziehbar bleiben.

Für das unternehmensinterne Qualitätsmanagement ist die Überwachung der Einhaltung in der Schnelllebigkeit der Systeme und der steigenden Dynamik der Prozesse oft sehr schwierig. Unser „Universal-Standard" zeigt hier eine praktische Möglichkeit, wie Unternehmen und ihre Mitarbeiter in jedem Fachbereich ihre eigenen Prozesse verwalten und überwachen können. Dabei wird mit Checklisten, Musterformularen, IT-Tools, etc. gearbeitet, von denen jeder Mitarbeiter den Umgang kennt. Damit wird gewährleistet, dass das Qualitätsmanagement sichergestellt und Änderungen flexibel umgesetzt werden können.

3GRC: Welchen Stellenwert hat eigentlich eine Ombudsstelle oder ein Hinweisgebersystem innerhalb des Compliance-Managementsystems…

Ein Ombudsmannsystem bzw. der in diesem Rahmen berufene Ombudsmann steht Arbeitnehmern eines Unternehmens, sowie auch dessen Lieferanten, Auftragnehmern und sonstigen interessierten Parteien („Interested Parties") zur Verfügung. Sie können dem Ombudsmann einen Rechtsverstoß oder sonstige Straftaten sowie Verstöße gegen interne Regelungen und Verhaltenskodizes im Rahmen der Geschäftsbeziehungen zum Unternehmen mitteilen. Der Ombudsmann ist dabei ein objektiver Ansprechpartner, unterliegt keinen Weisungen durch das Unternehmen, sondern agiert selbstständig und unabhängig und gewährleistet (aufgrund berufsrechtlicher Verschwiegenheitsverpflichtungen als zugelassener Rechtsanwalt) gegenüber dem Unternehmen die Anonymität der Hinweisgeber.

Er ist aus diesem Grunde auch zur Verschwiegenheit gegenüber Dritten sowie an einschlägige, gesetzliche Bestimmungen zum Datenschutz gebunden.

Existiert ein Compliance-Team im Unternehmen, so arbeitet er mit diesem (unter Wahrung der Anonymität des Hinweisgebers) zusammen.

3GRC: … und welchen Mehrwert bringt es dem Unternehmen?

Der Ombudsmann unterstützt das Unternehmen dabei, seine Tätigkeiten auf der Basis rechtlich einwandfreier Grundsätze auszuführen. Außerdem berät er (auch anonym) in Fragen zum Umgang mit möglichen Verdachtsmomenten und Gefährdungssituationen. Dadurch leistet er einen wichtigen Beitrag zu einer rechtssicheren Organisation und Korruptionsbekämpfung.

Durch die Möglichkeit der Wahrung der Anonymität ist er als „Früherkennungsfunktion" meist wesentlich effektiver als Revision / Controlling / etc.

Ein Ombudsmannsystem kann zudem für die eigene Reputation bestens genutzt werden. Auch Kunden und Geschäftspartner schätzen es, wenn ein Vertragspartner sich offen dazu bekennt, transparent zu agieren und dabei die geltenden Gesetze einhalten zu wollen. Dies zeigt sich auch an der zunehmenden Verbreitung von „Know your Customer" oder „Know your Supplier"-Systemen.

3GRC: Gibt es Hilfsmittel, die bei der Implementierung eines solchen Systems unterstützen können?

Aus folgenden Standards kann entnommen werden, dass die Einrichtung eines Ombudsmann-Systems empfohlen / gefordert wird:

- ISO 19600:2014
- ISO 37001:2017
- UK Bribery Act 2010
- USA Foreign Corrupt Practices Act (FCPA) 1977

Entsprechend wird die Existenz eines solchen Ombudsmannes auch im Rahmen einer Auditierung der obigen Standards gewünscht / gefordert.

<u>Arbeitshilfen sind</u>:

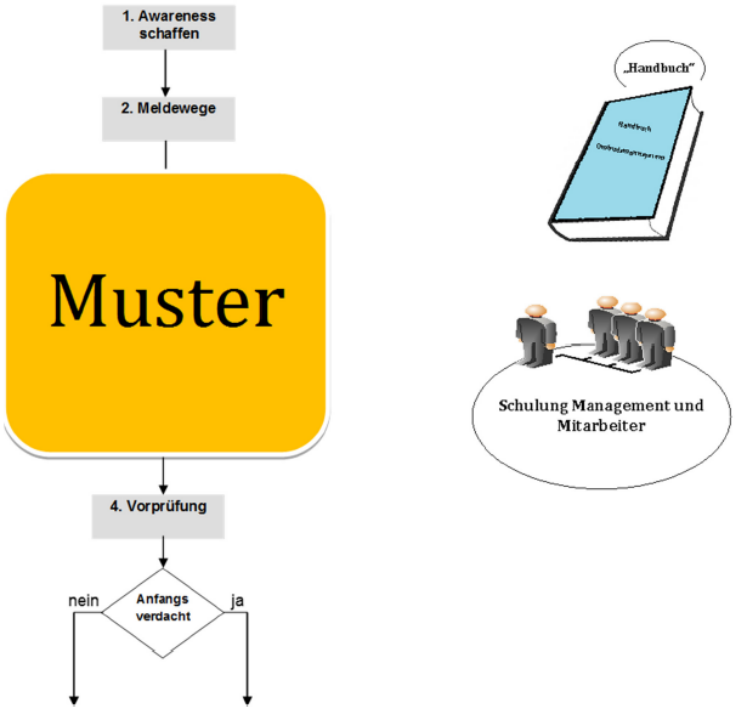
- Rahmenvertrag / Projektvertrag „Ombudsmannsystem"
- Beschluss über die Implementierung durch die Geschäftsleitung
- Prozessablauf für Hinweismitteilung und -bearbeitung
- Telekommunikative Einrichtungen
- FAQ (Frequently Asked Questions in Bezug auf das Ombudsmannsystem)
- "Handbuch" Ombudsmannsystem
- Einführungsschulung (Präsentation/Vorstellung) für Management und Mitarbeiter

3GRC: Können Sie uns kurz den Prozess zur Implementierung eines Hinweisgebersystems erläutern?

Für das Unternehmen ist lediglich folgendes erforderlich:

- Abschluss eines Rahmen- /Projektvertrages
- Beschluss (der Geschäftsführung) über die Ernennung des Ombudsmannes
- Bekanntgabe der Kontaktdaten an die angesprochenen Personenkreise
- Einführungsschulung

Die erstmalige Einrichtung eines Ombudsmann-Systems kostet ab 3.500,00 € netto zuzüglich Umsatzsteuer.



3GRC: In den USA gibt es bereits verbindliche gesetzliche Regelungen für die Einrichtung von Hinweisgebersystemen. Wie sieht die rechtliche Situation in Deutschland aus?

Eine allgemeine rechtlich verbindliche Pflicht zur Einrichtung eines Ombudsmann-Systems besteht in den meisten Fällen – zumindest im deutschen Recht – noch nicht ausdrücklich (z.B. explizit, im Gesetz allgemein geregelt).

Es wird von Jahr zu Jahr vermehrt die Ansicht geteilt, dass es bereits zum anerkannten Stand von Wissenschaft und Praxis gehöre, ein Hinweisgebersystem vorzuhalten. Damit gehöre dies auch zu den Pflichten eines gewissenhaften Unternehmers (§§ 43 GmbHG, 93 AktG, 347 HGB) und der Ermessenspielraum, ob so ein System vorzuhalten ist, reduziere sich stark.

Außerdem existiert bereits in § 25a Abs. 1 Satz 6 Nr. 3 KWG (Kreditwesengesetz) eine solche gesetzliche Verpflichtung für Finanzinstitute und seit 30.06.2016 in § 23 Abs. 6 VAG (Versicherungsaufsichtsgesetz) auch für Versicherungsunternehmen.

3GRC: Mit welchen Ansätzen wird sich die Forschung im Bereich Compliance-Management in Zukunft beschäftigen?

Das Thema Risiko- und Compliancemanagement ist gerade in Zeiten der Digitalisierung und Datenschutz aktueller denn je. Besonders wichtig sind daher zum einen digitalisierte, human Workflowmanagement ausgestaltete Prozesse in allen Unternehmensbereichen, die mit den relevanten Compliance-Komponenten angereichert sind.

Damit stehen integrierte GRC-Managementsysteme in engem Zusammenhang; Qualitätsmanagement, Risk und Compliance, CMS und Revision, etc. sind also eng miteinander verknüpft.

Deshalb werden nicht nur die Anforderungen an die zu erarbeitenden technischen Lösungen steigen, auch die Unternehmen und Mitarbeiter müssen ihre (fachlichen) Kompetenzen erweitern, um die künftigen Anforderungen im digitalen Zeitalter zu erfüllen.