Kolumne: Spielräume erkennen

„Wie viele Lenkräder und Fahrersitze haben Sie in der Compliance", fragt unser Kolumnist Markus Jüttner in dieser Ausgabe und zeigt auf, dass auch der Weg vom Compliance-Management-System (CMS) zum integrierten CMS (iCMS) eindeutig nur mit einem Fahrer aufgenommen werden sollte, der Richtung und Geschwindigkeit bestimmt. Und dann rät er, erstmal „auf Sicht zu fahren", d.h. die Umsetzung neuer regulatorischer, komplexer Querschnittsthemen im Rahmen einer vorübergehenden Projektstruktur umzusetzen – auch so lassen sich Spielräume erkennen.

Das IMS hat auf den ersten Blick einen bestechenden Vorteil: Es fasst viele (Compliance-) Risiken unter ein Managementkonzept zusammen. Doch gerade in rechtlichen Kontexten steckt der Teufel im Detail.

Wie in der vorletzten Kolumne skizziert, müssen Organisationen bereits de lege lata eine Vielzahl von Gesetzen befolgen und halten daher für besonders risikoreiche Themen ein CMS vor. Ein solches Management-System unterscheidet sich aber von einem bloßen Haufen an Maßnahmen, wie ich in der vorherigen Kolumne aufgezeigt habe. Doch damit nicht genug, es kommen de lege ferenda etliche weitere juristische Risiko-Management-Systeme hinzu: Beispielsweise lassen EU-Entwaldungsverordnung, EU-AI-Act, NIS 2, Data Act, DORA, das LkSG bzw. die (noch national umzusetzende) CSDDD grüßen.

Wie sollen Organisationen all diese sogenannten 2nd-line-Management-Systeme mit begrenzten Ressourcen überhaupt operationalisieren, d.h. machbar implementieren und beherrschbar steuern. So kommen inzwischen auch große Unternehmen an ihre Grenzen, denn die vielen neuen Regularien erfordern nicht nur eine vertikale Operationalisierung in die „Tiefe" der Organisation bzw. des Konzerns, sondern auch in die „horizontale" Breite. Bei vielen neuen Themen werden daher in Unternehmen Komitees, Ausschüsse oder Arbeitsgruppen gebildet, in denen die verschiedenen betroffenen internen Stakeholder am Tisch sitzen. Das bislang vorherrschende Governance-Modell, einzelne Risiko-Themen durch einen einzelnen Fachbereich xyz zu managen, scheint damit ein Ende zu haben. Paralleles Silomanagement ist out – holistische, integrierte, ganzheitliche Governance-Systeme sind hingegen (wieder) in. Dies hat auch mit der zunehmenden Digitalisierung zu tun, denn damit geht eine Formalisierung und Standardisierung von Prozessen einher, die gezwungenermaßen zu einer Vereinheitlichung und Zentralisierung von Governance-Systemen führt.

Zeit also, Compliance größer und zentralistischer zu denken als bisher? Diese Fragestellung und das damit verbundene Phänomen sind außerhalb der Compliance keineswegs neu, wirft es doch grundsätzliche Fragen der Organisiertheit, der Suche nach der optimalen Organisationsform und Steuerbarkeit auf. Das Problem ist so alt wie es organisierte Arbeitsteilung gibt. Caius Petronius hat bereits 100 n. Chr. festgestellt: „Wir übten mit aller Macht. Aber immer, wenn wir begannen, zusammengeschweißt zu werden, wurden wir umorganisiert. Ich habe später gelernt, dass wir oft versuchen, neuen Verhältnissen durch Umorganisierung zu begegnen […]."

Übersetzt auf Compliance hieße dies aktuell, sich mit der Frage auseinanderzusetzen, ob man etwa Bereiche bzw. Themen zusammenfassen und zentralisieren soll oder eher das Heil in der Spezialisierung und Dezentralisierung sucht. So hat etwa ein integriertes Compliance-Management-System („iCMS" oder „IMS") zumindest auf den ersten Blick im Vergleich zu isoliert nebeneinanderstehenden Compliance-Management-Systemen („CMS") einen bestechenden Vorteil: Man kann alle oder zumindest viele (Compliance-) Risiken unter ein Managementkonzept zusammenfassen und hat im Best-Case auch eine Verantwortlichkeit, einen Datenpool und ein einheitliches Reporting. Allerdings sollte man nicht organisationsnaiv sein, sondern stets im Hinterkopf behalten, dass jede Problemlösung Lösungsprobleme in Organisationen mit sich bringt.

So kann ein IMS sicherlich Effizienzen heben, aber es ist nicht notwendigerweise damit auch effektiv, denn gerade in rechtlichen Kontexten steckt der Teufel im Detail. Dies wird einem relativ schnell klar, wenn man bedenkt, dass sich für ein einheitliches IMS nur dann ein gemeinsamer Management-Nenner der verschiedenen Compliance-Risiken bzw. Rechtsthemen finden lässt, wenn man einen relativ hohen Abstraktionslevel wählt. Unter einem Managementdach des „prevent – detect – respond", eines „plan – do – check – act" oder den sieben Elementen des IDW PS 980 Standards lässt sich durchaus ein gesamthaftes House of Governance oder House of Compliance fassen. Aber bereits eine Ebene tiefer, beispielsweise bei der Durchführung einer Compliance-Risikoanalyse kommt es auf die Spezifika der jeweils einzuhaltenen Regularien an: Datenschutzrechtsfolgenabschätzungen sind anders durchzuführen als eine LkSG-Risikoanalyse; diese wiederum sieht anders aus als eine nach dem Geldwäschegesetz – von einer Compliance-Risikoanalyse, die nach blinden Flecken und Indikatoren von Unternehmenskriminalität oder Fraud-Risiken sucht, ganz zu schweigen.

Wie geht man also mit diesem Dilemma um? Die Lösung bzgl. des „Ob" ist relativ eindeutig: Am besten wäre es, wenn es nur ein Lenkrad und einen Fahrer gibt, der Richtung und Geschwindigkeit bestimmt. In Bezug auf das „Wie" lautet die Empfehlung: „So viel Integration wie nötig, so viel Arbeitsteilung wie möglich." Wie dies konkret aussieht, muss jede Organisation für sich entscheiden. Da die meisten Zuständigkeiten und Strukturen historisch gewachsen sind, wird es keine einfache Aufgabe sein, sich mit dem Thema der (Um-) Organisation im Unternehmen auseinanderzusetzen. Konflikte, Machtfragen, Befindlichkeiten werden offen oder versteckt auftreten, mit der Gefahr, dass Sachfragen zur Effizienz und Effektivität in den Hintergrund treten können. Aus meiner Praxiserfahrung wäre es daher ratsam, erstmal „auf Sicht zu fahren", d.h. die Umsetzung neuer regulatorischer, komplexer Querschnittsthemen im Rahmen einer vorübergehenden Projektstruktur umzusetzen. Der Vorteil ist, dass eine Projektstruktur die Zuständigkeit in der sich daran später anschließenden Regelorganisation nicht zwingend vorwegnimmt und die ersten Implementierungserfahrungen aus dem Projekt bei der Suchfrage nach der permanenten Verortung des Themas einfließen können. Dies setzt aber eine Kompetenz voraus, die nicht naturgemäß mit der Legal-, Compliance- und Governancefunktion verbunden wird: Das Projektmanagement.

Markus Jüttner


© Privat

Markus Jüttner ist Rechtsanwalt und Partner des Fachbereichs Forensic & Integrity Services, Ernst & Young GmbH. Er berät Unternehmen in Fragen der Compliance, der Kultur und der Integrität.
markus.juettner@de.ey.com