Système de gestion de la conformité

Toute entreprise doit se conformer aux lois et règlements applicables, mais aussi aux principes éthiques et moraux. La conformité est comprise comme l'effort pour s'assurer que le comportement est conforme aux règles. Ainsi, un risque de conformité existe si une entreprise court le risque de violer les règles – qu'elles soient de nature juridique ou de directives internes.
Les risques varient d'une entreprise à l'autre et les conséquences potentielles peuvent être très différentes. Si l'un de ces risques se réalise, des sanctions, des demandes de dommages et intérêts, des amendes ou des peines d'emprisonnement sont envisageables, mais l'entreprise peut aussi subir des pertes massives de réputation.
Quelles sont les exigences pour un CMS?
Sur la base de la norme ISO 37301, les éléments de base d'un CMS sont divisés en sept catégories qui interagissent les unes avec les autres. Les transitions sont fluides.
Comme pour la gestion des risques, la direction de l'entreprise doit, dans un premier temps, définir la culture de conformité qui doit faire partie de la culture d'entreprise. C'est le seul moyen de garantir l'ancrage des aspects liés au contenu, à l'organisation et à la communication de la conformité. Pour que le système soit efficace, il doit être vécu par la direction et une tolérance zéro doit être appliquée aux violations de la conformité.

Compliance Management System

Ein Muss in der heutigen Zeit!

Die Pandemie hat die Wirtschaft, den Staat und die Gesellschaft in eine Krise geführt, welche kaum vorstellbar war. Gerade jetzt ist es wichtig, dass auf ein bestehendes Compliance Management System (CMS) zurückgegriffen werden kann. Die Unternehmen sind gefordert, die Umfeldveränderung, welche zu neuen Rechtsrisiken führen kann, zu analysieren und im CMS zu steuern. Aber wie behält man dabei den Überblick?

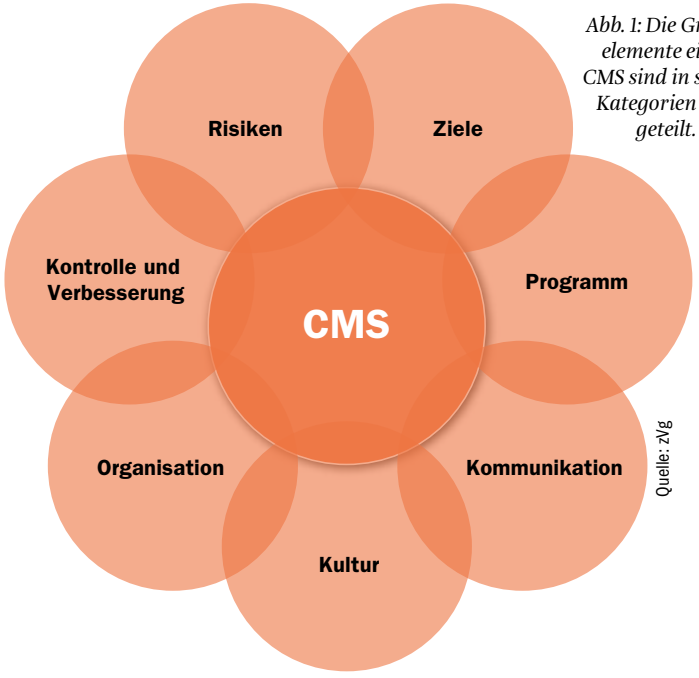

Abb. 1: Die Grundelemente eines CMS sind in sieben Kategorien eingeteilt.

Quelle: zVg

Nicole Heynen

Jedes Unternehmen muss geltende Gesetze und Regularien, aber auch die Einhaltung ethischer und moralischer Grundsätze befolgen. Unter Compliance wird die Bemühung verstanden, regelkonformes Verhalten sicherzustellen. Somit besteht ein Compliancerisiko, wenn eine Unternehmung Gefahr läuft, gegen die Regeln – seien diese gesetzlicher Natur oder interne Vorgaben – zu verstossen.

Die Risiken sind von Unternehmen zu Unternehmen unterschiedlich und die potenziellen Folgen können sehr verschieden sein. Sollte eines der Risiken eintreten, sind Sanktionen, Schadenersatzforderungen, Geldstrafen oder

Haftstrafen denkbar, aber auch massive Reputationsverluste können dem Unternehmen drohen.

Welches sind die Anforderungen an ein CMS?

Orientiert an der ISO-Norm 37301 sind die Grundelemente eines CMS in sieben Kategorien eingeteilt, welche miteinander in Wechselwirkungen stehen. Die Übergänge sind fliessend (vgl. Abb. 1).

Wie beim Risikomanagement ist die Unternehmensleitung gefordert, in einem ersten Schritt die Compliancekultur zu definieren, welche ein Teil der Unternehmenskultur sein muss. Nur dadurch ist gewährleistet, dass die inhaltlichen, organisatorischen und kommunikativen Aspekte der Compliance verankert werden. Damit das System greift, muss es von der Geschäftsleitung gelebt und eine Nulltoleranz sollte bei Complianceverstössen angewendet werden. Regelmässige Compliancerundschreiben, Unterstützung der Compliancefunktionen im Unternehmen, Intranetauftritte zum Thema Compliance oder ein Code of Conduct helfen unter anderem bei der Einführung eines CMS.

Die Complianceziele halten fest, was die Grundlagen für die Beurteilung von Risiken sind, während die Complianceorganisation die Rollen und Verantwortlichkeiten klärt und die notwendigen Ressourcen zur Verfügung stellt. Die Kommunikation sorgt dafür, dass die jeweils betroffenen Mitarbeitenden und allenfalls Dritte über das Complianceprogramm sowie die festgelegten Rollen und Verantwortlichkeiten informiert werden, damit sie ihre Aufgaben im CMS ausreichend verstehen und sachgerecht erfüllen können.

Die Risikoanalyse – das Fundament des CMS

Die Basis des CMS bildet die Risikoanalyse, welche für eine nachhaltige Umsetzung sorgt. Die Risikoidentifikation besteht darin, frühzeitig mögliche Verstösse oder Fehlverhalten zu erkennen, welche zu Haftungsansprüchen und damit verbundenen Reputationsverlusten führen können. Neben den klassischen Themen wie namentlich Korruption, Arbeitsrecht, Datenschutzverletzungen sowie Verstoss gegen das Kartellrecht sind auch betriebliche Anforderungen nicht zu vergessen. Um eine verlässliche, nicht dem Zufall überlassene Identifikation sicherzustellen, braucht es einen systematischen, periodisch durchgeführten Prozess. Dieser Prozess sollte Top-down wie auch Bottom-up durchgeführt werden. Nur so kann gewährleistet werden, dass keine Lücken zwischen dem Management, welches auf strategischer Ebene tätig ist, und den Mitarbeitenden entstehen.

Eine erste Übersicht kann durch die Risikoanalyse mit Hilfe von Gesetzen und Verordnungen sowie mit internen Dokumenten wie Geschäftsreglementen oder Prüfberichten erstellt werden. Diese Dokumentenanalyse bildet die Grundlage für die anschliessenden Interviews und Workshops, welche im Management durchgeführt und mit den operativ tätigen Einheiten validiert und ergänzt werden sollten. Durch die Bewertung der Eintrittswahrscheinlichkeit und der Schadenhöhe können Priorisierungen vorgenommen werden. Das Kernstück des Systems sind dann die Massnahmen, welche zur Steuerung von Risiken implementiert werden. Diese Complianceprogramme können beinhalten, dass unter anderem neue Richtlinien, Schulungen oder Prozesse wie Personalrotationen umgesetzt werden. Die Massnahmen müssen dokumentiert und nachvollziehbar sein. Nur so ist gewährleistet, dass sich ein Unternehmen bei Untersuchungen im Kontext von Verstössen in eine bessere Position bringen kann.

Die Complianceüberwachung und Verbesserung ist wichtig und beurteilt die Angemessenheit und Wirksamkeit des CMS anhand der Dokumentation. Werden im Rahmen der Überwachung Schwachstellen im CMS beziehungsweise Regelverstösse festgestellt, werden diese an die Geschäftsleitung bzw. die hierfür bestimmte Stelle im Unternehmen berichtet. Dieses Gremium muss im Sinne einer kontinuierlichen Verbesserung des CMS die Mängel beseitigen und das System verbessern.

Einbezug von Standards und Normen

Der Aufbau und die Sicherstellung der Compliance ist eine komplexe Aufgabe. Deshalb ist es empfehlenswert, sich an Standards und Normen anzulehnen. Bereits 2014 wurde mit der ISO-Norm 19600 eine Leitlinie und Hilfestellung konzipiert, welche als Standard und Best Practices zu verstehen war. Bewusst wurde dabei auf eine Zertifizierungsmöglichkeit verzichtet. Schnell setzte sich aber die Meinung durch, dass gerade eine Zertifizierung die Möglichkeit bot, die Effektivität des CMS unter Beweis zu stellen.

Diese Lücke schliesst nun die ISO 37301, die klare und überprüfbare Anforderungen an das System stellt. Als Grundlage wird eine Risikoanalyse für das Managementsystem gefordert. Darüber hinaus schreibt die Norm vor, dass die Compliancerisiken regelmässig und unter bestimmten Umständen gänzlich neu bewertet werden. Die Aufgabe des Com-

Autorin

Nicole Heynen (MAS Risk Management und eidg. dipl. Versicherungsfachfrau) ist Leiterin der Abteilung «Risikomanagement und Versicherungspolitik» bei der Eidgenössischen Finanzverwaltung EFV. Sie war von 2015 bis 2021 Präsidentin des Netzwerks Risikomanagement.

> *www.netzwerk-risikomanagement.ch*

pliancemanagers ist eine multidisziplinäre Herausforderung und erfordert hohes Mass an fachlicher und sozialer Kompetenz und Durchsetzungsvermögen. Damit das gelingt, muss die Unterstützung und das Commitment der Geschäftsleitung zwingend vorliegen. Wie die Complianceorganisation aufgestellt ist, muss der Organisation entsprechen. Kurze Berichts- und Entscheidungswege müssen aber gewährleistet sein. Es ist in der Verantwortung der Geschäftsleitung dafür zu sorgen, dass die Mitarbeitenden die Gesetzte einhalten. Die Beaufsichtigung der Unternehmensleitung im Hinblick auf die Befolgung der Gesetze ist eine gesetzliche Kernaufgabe des Verwaltungsrates. Die erwähnten Aufgaben müssen die Verwaltungsräte und Unternehmensleitungen mit aller Sorgfalt erfüllen. Wenn sie diese erhöhte Sorgfaltspflicht absichtlich oder fahrlässig verletzen, haben sie für den Schaden die Verantwortung zu tragen.

Schlussfolgerung

Rechtsrisiken zählen zu den grössten Risiken. Ein wirksames CMS hilft, diese zu bewältigen. Diese Aufgabe ist eine nicht delegierbare Chefsache, welche zentral für den Unternehmenserfolg ist.

Eine grosse Anzahl an Unternehmen in der Schweiz halten nach wie vor am «Three Lines of Defense Modell» des US-amerikanischen Institute of Internal Auditors fest. Dabei wird nicht beachtet, dass dieses Modell keinen Standard regelt und inhaltlich weder dem Risiko- noch dem Compliance Management gerecht wird. Verwaltungsräte, die sich darauf abstützen, tragen im Schadenfall faktisch die Beweislast. Es ist fraglich, ob bei einem Vorfall der Beweis erbracht werden kann, dass dieses Modell die Substanz und Qualität anerkannter internationaler Standards bietet.

Es ist empfehlenswert, dass die Unternehmensleitung das bestehende Compliancesystem durch externe Revisoren überprüfen lässt. Dadurch wird ersichtlich, ob die bestehende Reife und Wirksamkeit den Anforderungen eines modernen Compliance Managementsystems genügt. Ist das nicht der Fall, ist es Aufgabe des Verwaltungsrates, ein angepasstes System zu implementieren. Durch die Digitalisierung werden die rechtlichen Herausforderung auch künftig gross sein. Der langfristige Erfolg jedes einzelnen Unternehmens hängt von einem gelebten CMS ab. ■