ISO 37301: klare Strukturen für das CMS

Im April 2021 wurde von der International Organization for Standardization (ISO) eine neue Norm für Compliance-Management-Systeme (CMS) veröffentlicht. Diese Norm ermöglicht es Unternehmen erstmalig, die Angemessenheit des gesamten CMS durch ein international anerkanntes Zertifikat bestätigen zu lassen und bietet hierbei gleichzeitig einen Leitfaden für die Implementierung.

ISO 37301 betrachtet das Unternehmen ganzheitlich im Sinne eines Plan-Do-Check-Act-Ansatzes.

Die regulatorischen Anforderungen an Unternehmen steigen – sowohl auf nationaler als auch internationaler Ebene. Zeitgleich fehlte es bisher jedoch an einem weltweiten Standardwerk, das sowohl die Implementierung von CMS als auch die Zertifizierung ihrer angemessenen Ausgestaltung und Wirksamkeit ermöglicht. Der neu veröffentlichte ISO 37301 kann hier nun die Lösung sein, denn er schafft klare Vorgaben, die für ein angemessenes CMS umgesetzt werden müssen.

Dabei grenzt der Standard den Bereich der Anwender bewusst nicht ein, sodass dieser grundsätzlich auf jeden Unternehmenstypus – unabhängig von Branche und Größe – anwendbar ist. Wie auch andere aktuelle ISO-Standards zur Prüfung von Managementsystemen basiert der ISO 37301 auf der so genannten High-Level-Struktur und betrachtet durch die Verzahnung der Normbereiche im Sinne eines Plan-Do-Check-Act-Ansatzes das Unternehmen immer ganzheitlich. Die Basis dafür ist eine umfassende Compliance-Risikoanalyse über alle Compliance-Bereiche hinweg zur Bestimmung der Haupt-Compliance-Risiken. Dies hat zunächst auf einer übergeordneten Ebene als Gesamtschau der relevanten Rechts- und Regulatorikbereiche zu erfolgen und wird dann auf die konkreten Einzelrisiken des Geschäftsmodells, der Prozesse, der Geschäftspartner- und Mitarbeiterstrukturen sowie hinsichtlich der regionalen Ausprägung konkretisiert. Die fehlende Eingrenzung auf einzelne Rechtsbereiche (wie z.B. noch beim ISO 37001 – Antikorruptions-Managementsysteme) und die starke Risikoorientierung erlauben eine individuelle Skalierung des CMS.

Dies ermöglicht es auch, die Ausgestaltung des CMS im Hinblick auf die Anforderungen des ISO 37301 an bereits etablierte Unternehmensprozesse anzupassen und dabei individuell auf organisationsspezifische Besonderheiten einzugehen. Daher ist die Berücksichtigung des ISO 37301 auch für Unternehmen interessant, die bereits ein CMS gemäß IDW PS 980 implementiert haben. Sie können auf den bestehenden Strukturen aufbauen und die vorhandenen Prozesse weiter optimieren. Die Verbesserung des eingerichteten CMS ist ein zentrales Element der Normanforderungen und führt dazu, dass Unternehmen strukturiert auf externe und interne Änderungen reagieren und sich so ständig weiterentwickeln können und müssen.

Neben der Schaffung eingespielter Strukturen, die es ermöglichen flexibel auf geänderte Anforderungen zu reagieren, liegt der große Vorteil dieses Standards jedoch vor allem in der Möglichkeit, ein international anerkanntes Zertifikat über die angemessene Ausgestaltung und Wirksamkeit des CMS zu erlangen. Ziel ist es, hierdurch Sicherheit zu schaffen – innerhalb der eigenen Organisation, für die Geschäftsleitung, für Aufsichtsorgane und gegenüber Dritten.

Mit dem Blick auf externe Stakeholder dient das Zertifikat hierbei als eine Art Bestätigung, die die internen Bemühungen auch nach außen sichtbar werden lassen. Dies bietet vor allem gegenüber Geschäftspartnern und Kunden einen großen Vorteil, da das Vertrauen in das zertifizierte Unternehmen und im Hinblick auf seine Compliance-Haltung gesteigert wird. Dies wird gerade auch durch die nach ISO 37301 verpflichtende, aktive und regelmäßige Beurteilung der Wirksamkeit des CMS auf Basis verschiedener Informationen, wie einem Internen Audit nach ISO 37301 oder bekannt gewordener Hinweise auf Compliance-Verstöße durch die Geschäftsführung und die Aufsichtsorgane, noch verstärkt.

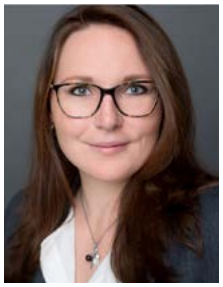
Neben der ausstrahlenden Wirkung eines solchen Zertifikats im geschäftlichen Verkehr darf nicht außer Acht gelassen werden, dass eine erfolgreich durchlaufende Zertifizierung auch hinsichtlich der Erfüllung der Sorgfaltspflicht förderlich sein wird. Für international agierende Konzerne ist außerdem zu beachten, dass auch internationale Tochtergesellschaften leicht in den Geltungsbereich des Zertifikats eingeschlossen werden können – sowohl bei der Ausgestaltung eines CMS als auch in der Zertifizierung.

Zusammenfassend lässt sich festhalten, dass der neue ISO Standard 37301 viele Vorteile für Unternehmen im Hinblick auf die Ausgestaltung und Prüfung des CMS liefert. Dessen Anwendung kann langfristig die Anfälligkeit von Unternehmen für Compliance-Verstöße reduzieren.

Dr. Jan-Hendrik Gnändiger, Claudia Dietrich und Katharina Bremer

KPMG AG

Dr. Jan-Hendrik Gnändiger, Dr. rer. oec., Steuerberater und Wirtschaftsprüfer, ist Partner und Head of Risk & Compliance Services bei der KPMG AG, ansässig in Köln. Sein Spezialgebiet ist die Beratung und Prüfung von Corporate Governance.



KPMG AG

Claudia Dietrich ist Senior Managerin bei der KPMG AG und Prokuristin der KPMG Cert GmbH Umweltgutachterorganisation, ansässig in Köln. In dieser Position verantwortet sie die KPMG-Methodik zu ISO Managementsystem-Zertifizierungen nach ISO 37001 und ISO 37301.

KPMG AG

Katharina Bremer ist bei der KPMG AG im Bereich Risk & Compliance Services am Standort München tätig. Sie ist maßgeblich am Auf- und Ausbau des europäischen KPMG-Compliance-Expertennetzwerks beteiligt.