DICO
Deutsches Institut für Compliance

Standardisierung und Zertifizierung von Compliance-Management-Systemen

Bei der Einführung und Weiterentwicklung von Compliance-Management-Systemen (CMS) stehen Unternehmen weiterhin vor der Herausforderung, dass es keine klaren gesetzlichen Vorgaben gibt, die festlegen, wie solche Systeme auszusehen haben. Auf der anderen Seite fordern nationale Gesetzgeber verstärkt die Einführung von Compliance-Maßnahmen bzw. räumen Bußgeldmilderungen ein, falls Unternehmen CMS eingeführt haben, ohne diese näher zu konkretisieren. Wie können Unternehmen mit diesem Dilemma umgehen? Es gibt einzelne Standards (z.B. diverse ISO-Standards aus dem Bereich „Governance und Compliance Management“) die Orientierung geben. Auch bieten Wirtschaftsprüfer und einzelne Zertifizierungsstellen Compliance-Zertifizierungen an. Allerdings bleiben diese Standards zu vage und auch der Wert der Zertifizierungen ist unklar bzw. wird angezweifelt. Seit seiner Gründung befasst sich DICO mit dieser Herausforderung. Seit vielen Jahren erarbeiten die DICO-Arbeitskreise Leitlinien zu bestimmten Compliance-Maßnahmen oder Compliance-Risikofeldern. Diese konkreten Arbeitshilfen genießen bei den Anwendern große Beliebtheit, waren aber nie als Standards ausgelegt. Nunmehr möchte DICO in einem gemeinsamen Projekt mit dem Viadrina Compliance Center an der Europa-Universität Viadrina in Frankfurt(Oder) einen Schritt weiter gehen und konkrete DICO-Standards erarbeiten. Der folgende Beitrag beschreibt dieses Projekt und den Wert der DICO-Standards.

ISO-Standards

Die Internationale Organisation für Normung (ISO) und ihr deutsches Mitglied (DIN) waren in den letzten Jahren im Bereich der Compliance-Standardisierung sehr aktiv. So ist die bisherige nicht zertifizierbare Leitlinie ISO 19600 Compliance Management Systems zu einem zertifizierbaren Standard mit Anforderungen mit der neuen Hausnummer ISO 37301 überarbeitet worden. Hinzu getreten ist eine neue Leitlinie ISO 37002 Whistleblowing Management Systems, bei der es um die Ausgestaltung von Hinweisgebersystemen geht. Schließlich veröffentlichte ISO im August 2021 die übergeordnete Leitlinie ISO 37000 Governance of Organizations. Das Bild rundet der Standard mit Anforderungen für Korruptionsbekämpfung, ISO 37001 Anti-Bribery Management Systems, ab. Die Tatsache, dass sich ISO und DIN mit der Standardisierung befassen, zeigt wie bedeutsam das Thema Compliance in der Unternehmenspraxis geworden ist und dass es einen Bedarf für eine gewisse Vereinheitlichung gibt. Allerdings ist anhand dieser Standards, die insgesamt recht abstrakt gehalten sind, erkennbar wie schwer es ist, in einem internationalen Umfeld mit unterschiedlichen gesetzlichen Vorgaben und unterschiedlichen Unternehmenskulturen einheitliche Standards zu setzen. Gerade im Mittelstand, der sich bei technischen Themen gern von ISO und DIN leiten lässt, sind deren Compliance-Standards noch nicht wirklich angekommen.

DICO
Deutsches Institut für Compliance

DICO-Standards

Vor drei Jahren hat DICO gemeinsam mit dem Viadrina Compliance Center an der Europa-Universität Viadrina in Frankfurt (Oder) ein Projekt gestartet, ausgehend von den in den DICO Arbeitskreisen erarbeiteten DICO-Leitlinien neue DICO-Standards zu erarbeiten. DICO-Standards formulieren praxistaugliche und umsetzbare Anforderungen zu ausgewählten Compliance-Themen. Dargestellt wird die weithin anerkannte und (jedenfalls in Deutschland) überwiegend angewandte bzw. angestrebte Art und Weise, Compliance-Themen in der Unternehmenspraxis umzusetzen. Die DICO-Standards werden durch Compliance-Praktiker entwickelt und durch das Viadrina Compliance Center wissenschaftlich gegengeprüft. Compliance-Praktiker und Wissenschaft werden ausdrücklich aufgefordert fortlaufend an der Weiterentwicklung der DICO-Standards mitzuwirken.

Die Basis der Reihe von DICO-Standards bildet der übergreifende DICO-Standard zu Compliance-Management-Systemen, der in knapper Form allgemeine Empfehlungen zur Ausgestaltung eines CMS enthält. Er ist auf alle Unternehmensarten anwendbar, unabhängig von ihrer Größe, Struktur und Komplexität. Dieser übergreifende Standard wird durch DICO-Spezialstandards ergänzt, die ausführliche Empfehlungen zur Gestaltung ausgewählter CMS-Elemente enthalten. Dabei handelt es sich zum Teil um überarbeitete und aktualisierte DICO-Leitlinien. Es wurden aber auch bereits Standards zu neuen Themenfeldern erarbeitet, zu denen es bisher noch keine DICO-Leitlinien gab. Ziel des Projektes ist es, eine Reihe von DICO-Standards aufzulegen, die alle wesentlichen CMS-Elemente abdeckt.

Im Vergleich zu den ISO-Standards sind die DICO-Standards konkreter gefasst. Sie berücksichtigen die grundlegenden Vorgaben der ISO-Standards und auch anderer Standards (z.B.: IDW PSW 980), gehen dann aber themenspezifisch auf die (insbesondere in deutschen Unternehmen) vorherrschende Praxis ein und berücksichtigen auch die relevanten rechtlichen Vorgaben und Erkenntnisse aus der Fachliteratur. Insofern gewährleistet in der Regel die Umsetzung eines DICO-Standards eine gute Vorbereitung auf die Implementierung einer ISO-Norm mit anschließender Zertifizierung. Da die DICO-Standards von Praktikern entwickelt worden sind, haben sie eine hohe Praxistauglichkeit. Durch die wissenschaftliche Gegenprüfung ist aber auch eine Objektivität gewährleistet, so dass die DICO-Standards nicht nur von Unternehmensinteressen geleitet sind. In einem Zielbild sollen möglichst alle CMS-Elemente durch DICO-Standards abgedeckt sein.

Prüfungsstandards und Zertifizierung

Bewusst entschied sich DICO dafür, seine Standards als Leitfäden zu gestalten und nicht für eine Zertifizierung freizugeben. Als generische Standards sind sie aber durchaus geeignet, einen Referenzrahmen, die sog. Soll-Vorschrift, für eine Prüfung durch Wirtschaftsprüfer nach IDW PS 980 vorzugeben oder sich auf eine anschließende Zertifizierung durch Zertifizierungsstellen etwa nach der ISO 37301 Compliance Management Systems vorzubereiten.

Fazit

DICO möchte mit den DICO-Standards Unternehmen helfen, dem oben beschriebenen Dilemma zu begegnen, steigenden gesetzlichen Anforderungen für CMS-Maßnahmen ausgesetzt zu sein, ohne dass diese hinreichend durch den Gesetzgeber konkretisiert werden. Die DICO-Standards können die

Grundlage bilden für mögliche Zertifizierungen anhand anderer Standards. Die DICO-Standards können aber ggf. auch in Zukunft in behördlichen oder gerichtlichen Verfahren für die Prüfung der Angemessenheit von CMS-Maßnahmen herangezogen werden.

Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt (Oder), Sprecher des wiss. Beirats

Dr. Philip Matthey, Head of Governance, Risk and Compliance / Chief Compliance Officer der Traton Group (vormals Volkswagen Truck & Bus AG) und der MAN SE und Sprecher des DICO Vorstandes

Dipl.-Kfm. Meinhard Remberg ist Generalbevollmächtigter der SMS GmbH und Sprecher des DICO Vorstandes