Interview

ISO 19600:2014

Zertifizierung von Compliance-Management-Systemen

Redaktion RiskNET 15.04.2015, 07:30

Compliance steht in allen Branchen und vielen Ländern rund um den Globus ganz oben auf der Agenda. Allgemein kann Compliance mit Regelkonformität übersetzt werden und umfasst die Einhaltung von Gesetzen und Richtlinien, aber auch von freiwilligen Kodizes, in Unternehmen. Im Kern handelt es sich um eine Binsenweisheit, das Unternehmen Gesetze und Regeln einhalten müssen.

Hierbei muss vor allem berücksichtigt werden, dass sich das Umfeld verändert hat, in dem Unternehmen heute agieren: Der Gesetzgeber hat neue Straftatbestände eingeführt, die Haftung erweitert und die Strafverfolgungsbehörden im Bereich der Wirtschaftskriminalität deutlich aufgerüstet. Aktuelle Entwicklungen in der Rechtsprechung zeigen recht deutlich. So hat beispielsweise das Landgericht München I den in der Zwischenzeit verstorbenen Ex-Siemens-Vorstand Heinz-Joachim Neubürger verurteilt, 15 Mio. Euro an seinen früheren Arbeitgeber als Schadensersatz dafür zu bezahlen, dass er nicht dafür gesorgte hatte, dass ein funktionierendes Compliance-Management-System eingerichtet wurde (LG München I, Urteil v. 10.12.2013 - 5 HKO 1387/10).

Der Siemens-Fall hat vor allem deutlich vor Augen geführt, dass sich international agierende Konzerne in unterschiedlichen Kulturen, Rechtsräumen und gesellschaftlichen Traditionen bewegen und hohe Compliance-Risiken eingehen, die im Risikomanagement erfasst und gesteuert werden müssen. Damit stellt sich die Frage, wie Unternehmen ein Compliance-Management-System aufbauen, damit es wirksam und erfolgreich ist. Bei der konkreten Umsetzung eines entsprechenden Systems gab es für Unternehmen bis vor wenigen Monaten keinen international akzeptierten Standard.

Dies soll sich mit dem im Dezember vergangenen Jahres veröffentlichten ISO Standards 19600:2014 ändern. Basierend auf dieser internationalen Guideline zum Thema Compliance-Management-System ("Compliance management systems — Guidelines") soll Unternehmen ein Orientierungsrahmen an die Hand gegeben werden, um entsprechende Systeme umzusetzen.

Das dem ISO-Standard zugrunde liegende Modell enthält im Wesentlichen zwei Phasen: Die erste Phase, welche in der Einführung des Compliance-Management-Systems besteht, und die zweite Phase, die im Betrieb des Systems besteht. In der ersten Phase müssen die Ziele und Anwendungsbereiche des Compliance-Management-Systems definiert werden. Auf dieser Basis wird die Compliance-Strategie bzw. -Politik definiert. Die Schnittstelle zur zweiten Phase wird durch einen risikobasierten Ansatz hergestellt. In dieser Phase werden die Compliance-Risiken und Anforderungen identifiziert und analysiert. In einem weiteren Schritt wird die Aufbauorganisation mit entsprechenden Verantwortlichkeiten definiert. Diese Elemente werden durch prozessuale Schritte begleitet: Entwicklung (development), Umsetzung (implementation), Evaluierung (evaluation) und Aufrechterhaltung (maintenance).

Wir sprachen mit Prof. Dr. Josef Scherer über aktuelle Entwicklungen im Bereich der Zertifizierung von Compliance-Management-Systemen.

Was bedeutet eigentlich Compliance? In der Praxis und Literatur findet man äußerst unterschiedliche Definitionen.

Josef Scherer: Es existiert diesbezüglich noch keine Legaldefinition: Unter Compliance versteht die herrschende Meinung, die sich aus Wissenschaft, Rechtsprechung und einschlägigen Standards zusammensetzen mag, die Einhaltung von verpflichtenden – externen und interne – Anforderungen. In diesem Kontext ist vor allem das Neubürger-Urteil wichtig. Das Landgerichts München hatte ein ehemaliges Vorstandsmitglied der Siemens AG zu einer Schadensersatzzahlung in Höhe von 15 Mio. EUR verpflichtet. Den Grund für die Schadensersatzpflicht des Ex-Vorstands sah das Gericht direkt in seinem

Organisationsverschulden. Er hätte es versäumt, ein funktionierendes Compliance-Management-System (CMS) für seinen Aufgabenbereich zu etablieren. Diese Definition stellt den *weiten* Compliance-Begriff dar.

Die ISO 19600 scheint diesen Ansatz sogar noch zu erweitern, indem sie auch noch "principles of good governance and community and ethical standards" vom Compliancemanagement-System umfasst sieht, ohne auszuführen, was diese sehr interpretationsfähigen Begriffe umfassen sollen.

In der Praxis wird bisweilen auch ein *enger* Compliance-Begriff vertreten, dahingehend, dass Compliance-Management nur die Sicherstellung der Vermeidung von straf- und bußgeldbewährten Pflichtverletzungen zum Ziele hat. Teilweise wird dieser enge Begriff noch dahingehend ergänzt, dass auch besonders schwerwiegende Reputations- oder Vermögensschäden über Compliancemanagement zu verhindern seien.

Der enge Begriff überzeugt nicht, da die Legalitätspflicht sich nicht auf lediglich straf- und bußgeldbewährte Vorgaben beschränkt.

Der IDW PS 980:2011 (Compliance-Managementsysteme) definiert Compliance als die Einhaltung von Regeln (gesetzliche Bestimmungen und unternehmensinterne Richtlinien).

Was umfasst alles ein Compliance-Management-System in der Unternehmenspraxis?

Josef Scherer: Auch hier gibt es bisher noch keine Legaldefinition, so dass die Definitionsfreiheit viele Vorschläge ermöglicht: Compliance-Management-System könnte beschrieben werden als Aufbau- und Ablauforganisation einer Institution mit interagierenden Komponenten (beispielsweise Prozessabläufe und Zuständigkeiten) mit dem Ziel der Sicherstellung von Pflichtenkonformität im Hinblick auf externe und interne verbindliche Vorgaben.

Der IDW PS 980:2011 (Compliance-Managementsystem) definiert ein Compliance-Managementsystem folgendermaßen: "Unter einem Compliance-Managementsystem sind die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele, eingeführten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie gegebenenfalls von Dritten abzielen, d. h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen

Verstößen (Regelverstößen). Ein CMS im Sinne des IDW-Prüfungsstandards kann sich insbesondere auf Geschäftsbereiche, auf Unternehmensprozesse (z. B. Einkauf) und auf bestimmte Rechtsgebiete (z. B. Kartellrecht) beziehen (abgegrenzte Teilbereiche)."

Diese Ausführung suggeriert möglicherweise den Verantwortlichen in der Praxis, sie hätten Ermessen bei der Frage, worauf sich das Compliance-Managementsystem erstrecken soll beziehungsweise kann.

Hier fehlt meines Erachtens eine Bezugnahme auf Aufbau- und Ablauforganisation, die die wesentlichen Komponenten eines Managementsystems darstellen.

Das ist falsch und widerspricht der Rechtsprechung des Landgerichts München ("Neubürger-Urteil")! Aufgrund der Legalitätspflicht sind alle rechtlichen Pflichten einzuhalten. Auch in zunächst nicht primär im Fokus des Interesses stehenden Bereichen kann sich ein Compliance-Verstoß verheerend auswirken. Vergleiche hierzu die Insolvenz eines Lebensmittelherstellers in Freising auf Grund eines nicht abgestellten Hygienemangels.

Was ist denn dann der Kernbereich eines Compliance-Management-Systems?

Josef Scherer: Der Kernbereich eines Compliance-Management-Systems besteht in der Setzung von fakultativen Zielen, sowie der Planung und der Steuerung mit Überwachung von folgenden Komponenten: Identifikation und Bewertung der zwingenden und fakultativ gesetzten Ziele des Compliance-Management-Systems sowie die Ermittlung von Anforderungen und Handlungsbedarf für Maßnahmen zur Erreichung dieser Ziele.

Außerdem allgemeine Prophylaxe- und Reaktionsmaßnahmen, wie beispielsweise Erlass von fehlenden beziehungsweise ergänzenden Regelungen (unter Berücksichtigung von internen und Umfeld-Veränderungen), der Installation eines Compliance-Risikomanagement-Prozesses mit Eruierung und Analyse, Bewertung und Steuerung von Compliance-Risiken sowie der Installation eines wirksamen Complianceverstoß-Erkennungs- und -Sanktionsprozesses.

Gab es Umfeldveränderungen, die die Bedeutung von Compliance-Management-Systemen steigern? Ist die Entstehungsgefahr, Entdeckungsgefahr, Sanktionsgefahr beziehungsweise das Haftungsrisiko bei Compliance-Verstößen in den letzten Jahren gestiegen?

Josef Scherer: Eindeutig ja! Jüngst wies Tüscher (ZGG 2015, S. 34 ff.) auf diverse Aspekte hin: Die Gefahr, dass Compliance-Verstöße häufiger als früher entstehen, geht unter anderem mit der Globalisierung einher: Die meisten mittelständischen Unternehmen weisen mittlerweile auch Auslandsbezüge auf. Gerade in den neuen Märkten Asien und Osteuropa bestehen noch erhebliche Gefahren und Möglichkeiten, in Compliance-Problematiken verwickelt zu werden.

Eine weitere neue Erscheinung stellen die Forderungen und Anforderungen der Großunternehmen gegenüber ihren Kunden und Lieferanten dar: Sie verlangen mittlerweile verpflichtend von ihren Geschäftspartnern die Vorhaltung von entsprechenden Compliance-Einrichtungen und lassen sich dies unter anderem auch vertragsstrafenbewährt versichern.

Die Einhaltung entsprechender Anforderungen wird mittlerweile mittels ausführlichster Fragenkataloge oder sogar Audits vor Ort überprüft. Im Grunde werden die Anforderungen der Großunternehmen teilweise direkt in den Lieferketten von Unternehmen zu Unternehmen durch- und weitergereicht, so dass schließlich auch kleinere Unternehmen von diesem Trend betroffen sind. Als Sanktion für die Verweigerung entsprechender Anforderungen ist der Wegfall der Geschäftsbeziehung keine Ausnahme.

Das Entdeckungsrisiko ist ebenfalls gestiegen, wofür es diverse Gründe gibt: Die eingerichteten Hinweisgebersysteme wie Whistleblowing- oder Ombudsmannsysteme funktionieren laut diverser wissenschaftlicher Aufsätze und Erfahrungen in der Praxis besser als Revision und Controlling, um entsprechende Compliance-Vorfälle aufzudecken.

Kronzeugenregelungen im Strafrecht aber auch vor allem "Bonusregelungen" für den Erstmelder im Kartellrecht führen dazu, dass zum einen mehr Kartellverfahren eingeleitet werden, zum anderen aber die Informationen für die Behörden über den Hinweisgeber griffiger werden.

Eine weitere Erscheinung ist die verstärkte Professionalisierung der Staatsanwaltschaften und Wirtschaftsstrafkammern, die auf dem Gebiet des Compliancemanagements schon sehr eifrig arbeiten.

Auch die Möglichkeit der digitalen Datenanalyse im Zeitalter von Big Data kombiniert mit dem Einsatz von IT-Experten auf dem Gebiet der Forensik und entsprechender Spezialsoftware ermöglicht es, Verstöße aufzudecken, die mit herkömmlichen Methoden sehr häufig der Flut der Masseninformationen zum Opfer gefallen wäre.

Die Gefahr, bei Compliance-Verstößen verschärft sanktioniert zu werden, hat sich ebenfalls erhöht: Gewinnabschöpfungen, Geldbußen und Geldstrafen, entsprechende Nachforderungen von Sozialversicherungsbeiträgen und Steuern sowie Schadensersatzansprüche gegen unterschiedlichste Mitwirkende gehören zum Repertoire der Verfolger. Eine weitere, ganz erhebliche, existenzbedrohende Sanktion stellt der Wegfall von Geschäftsbeziehungen oder der Ausschluss von Märkten oder Auftragsvergaben dar. Auch bei einem finanziell weniger scharf sanktionierten Complianceverstoß kann das einhergehende sich verwirklichende Reputationsrisiko existenzbedrohende Züge annehmen.

Auch das Haftungsrisiko ist gestiegen, wenngleich nicht unbedingt neue Haftungstatbestände dazukamen. Lediglich die Pflichten wurden durch Literatur und Rechtsprechung ausgeweitet. Neu ist, dass sogar Mitglieder von Aufsichtsgremien auch tatsächlich regressiert werden. Im Übrigen gab es laut Bachmann (vgl. Gutachten zum 70. Deutschen Juristentag 2014, Seite 13) in den Jahren 1986 bis 1995 genauso viele Urteile zur Managerhaftung wie in den letzten 100 Jahren zuvor. In den nachfolgenden 10-Jahres-Zeiträumen habe sich diese Zahl nochmals verdoppelt. Auch in den Medien ist das Thema "Verantwortung von Managern und Aufsichtsräten" ein Dauerbrennerthema, so dass die Wahrnehmung aber auch die öffentliche Berichterstattung über die Betroffenen zugenommen hat.

Welchen Mehrwert bietet eine Compliance-Management-System einem Unternehmen? Was sind die Vorteile eines wirksamen Compliance-Management-Systems?

Josef Scherer: Nach Tüscher (ZCG 2015, S. 36) liegen die Vorteile eines wirksamen (gelebten) Compliance-Managementsystems nicht nur in der Einsparung von Bußgeldern und Schadensersatzzahlungen. Vielmehr soll es die Identifikation der Mitarbeiter mit dem Unternehmen stärken und hohe Fluktuationsraten vermeiden. Bezüglich der Akquise von Fachkräften könne ein Compliance-Managementsystem ein Differenzierungsmerkmal darstellen. Auch bei Kreditratings und Versicherungen im Hinblick auf Risikobewertung und Prämienfestsetzung werden Vorteile festgestellt. Es lassen sich aber noch viele weitere Vorteile finden, wie beispielsweise die Erfüllung von zwingenden Kundenanforderungen oder das Überwinden von Markteintrittsbarrieren. Ebenso die Vermeidung persönlicher zivil- und strafrechtlicher Sanktionen mit der Folge des persönlichen und beruflichen Existenzverlustes.

Was sind die Vorteile eines zertifizierten Compliance-Management-Systems?

Josef Scherer: Laut Tüscher (ZCG 2015, S. 36) bestünden zwar vielfältige Möglichkeiten, durch unabhängige Sachverständige den Reifegrad eines Compliance-Managementsystems prüfen zu lassen. Dabei gäbe es "die relativ umfassenden und fundierten Prüfungen durch Wirtschaftsprüfer auf der Grundlage des IDW PS 980 bis zu auf allgemeinen Checklisten basierenden Prüfungen diverser Anbieter."

Nach erfolgreicher Prüfung erhält in der Regel das Unternehmen ein Zertifikat, welches gegenüber den "Interested Parties / Stakeholdern" eine Beurteilung des Compliance-Managementsystems ermöglichen soll.

Der Nutzen einer entsprechenden Dokumentation dürfte nach Tüscher in einem unabhängigen und objektivierten Nachweis liegen, dass die Compliance-Strukturen angemessen und möglicherweise auch wirksam sind. Dieser Nachweis lasse sich dann im positiven Sinn gegenüber Kunden, Versicherungen, Banken, Aufsichtsbehörden und Mitarbeitern und bei öffentlichen Ausschreibungen verwenden.

Intern könne so eine Prüfung auch als Stresstest für das Unternehmen zu verstehen sein, um den Verantwortlichen Schwächen im System aufzuzeigen und im eigenen Interesse die Möglichkeit zur Verbesserung zu geben. Dies mag häufig einen sogenannten "heilsamen Druck" erzeugen.

Unter Umständen könne eine erfolgreiche Wirksamkeitsprüfung auch eine haftungsmindernde Wirkung entfalten: Die Gerichte und Staatsanwaltschaften betonen in Fachvorträgen jedoch kontinuierlich, dass die Exculpation nicht lediglich in Dokumenten zu sehen, sondern vielmehr die Vorbildfunktion der Geschäftsleitung ("Tone form the top") und das "Leben" der Vorgaben durch alle Mitarbeit ausschlaggebend sei.

Was kann "geprüft" bzw. "zertifiziert" werden?

Josef Scherer: Im Grunde lässt sich alles prüfen beziehungsweise zertifizieren, also Personen, Produkte, aber natürlich auch Systeme. Weitere Infos hierzu finden sich im Akkreditierungsstellen-Gesetz.

Welche Arten von Prüfungen sieht der IDW PS 980 vor?

Josef Scherer: Der Prüfungsstandard für Wirtschaftsprüfer zur Prüfung von Compliance-Management-Systemen IDW PS 980 sieht zunächst eine Konzeptionsprüfung vor. Dabei wird geprüft, ob die Konzeption des CMS in wesentlichen Belangen zutreffend dargestellt ist und eine Beschreibung sämtliche Grundelemente eines CMS umfasst.

Des weiteren ist eine Angemessenheitsprüfung vorgesehen. Dabei wird geprüft, ob die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sowie angemessen sind. Darüber hinaus, ob die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt auch (in Aufbau- und Ablauforganisation) implementiert sind.

Als "letzte Stufe" ist eine Wirksamkeitsprüfung vorgesehen. Bei der Wirksamkeitsprüfung wird festgestellt, ob Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt und angemessen sind sowie zu einem Zeitpunkt implementiert und in einem bestimmten Zeitraum wirksam sind.

Nach Tüscher haben diese vorgegebenen Prüfungstypen bestimmte Vor- und Nachteile: Eine haftungsmindernde Wirkung könne nur bei einer bestandenen Wirksamkeitsprüfung erzielt werden. Die Beurteilung der Wirksamkeit durch den Wirtschaftsprüfer erfolge jedoch auf dem Niveau einer hinreichenden Sicherheit (was nicht absolute Sicherheit bedeutet). Zum Erreichen dieser hinreichenden Sicherheit müssten jedoch umfangreiche Funktionstests durchgeführt werden, welche einen hohen Aufwand für die Beteiligten darstellten.

Alleine schon eine ausreichende Systembeschreibung stelle einen erheblichen Aufwand dar, da die Prüfung darauf abstelle, ob das Compliance-Management-System alle sieben Grundelemente nach IDW PS 980 berücksichtige. In der Praxis fehle es häufig auch an einer systematischen Bestimmung von Compliance-Risiken.

Tüscher sieht als Kompromisslösung die Möglichkeiten eines prüferischen "Reviews" oder auch eine Prüfung mit zuvor vereinbarten Untersuchungshandlungen ("Agreed-Upon-Procedures"). Er stellt auch die Frage, ob nicht eine eingeschränkte Wirksamkeitsprüfung auf dem Niveau einer "Limited-Assurance" für ein mittelständisches Unternehmen ausreiche. Dabei bringe der Wirtschaftsprüfer im Falle fehlender (auch positiver) Feststellungen zum Ausdruck, dass er bei seiner Prüfung keine Hinweise erhalten habe, die die Wirksamkeit der Compliance-Strukturen in Frage stellen.

Tüscher stellt fest, dass damit zwar keine haftungsmindernde Wirkung mehr zu erreichen sei, jedoch die internen Vorbereitungs- und Prüfungskosten deutlich reduziert werden könnten.

Er geht davon aus, dass eine derartige Bescheinigung eines unabhängigen und complianceerfahrenen Wirtschaftsprüfers bei Kunden, Versicherungen, Banken, Aufsichtsbehörden und Mitarbeitern auf eine ähnliche Akzeptanz stoße, wie eine

uneingeschränkte Prüfung nach IDW PS 980. Dies ist allerdings aus meiner Sicht kritisch zu hinterfragen.

Worauf ist bei der Vertrags-, Testats- und Urkundengestaltung zu achten?

Josef Scherer: Hierbei sind vielfältige Überlegungen anzustellen: Über den entsprechenden Auftrag, aber auch das erteilte Testat oder eine ausgestellte Urkunde werden Informationen unter Umständen auch für Dritte mit einem vereinbarten oder sich aufgrund einer Prüfung ergebenden Inhalt erstellt und kommuniziert. Dies kann, sofern Aussagen nicht zutreffend sind, unter Umständen sogar zu Haftungsansprüchen bei den Beteiligten führen. Es ist deshalb im Vorfeld genau zu überlegen, welche Leistungen erbracht werden sollen ("Lasten- und Pflichtenheft") und welche Ergebnisse erzielbar sind und wie diese letztendlich kommuniziert werden sollen/dürfen.

Kann ein Zertifikat oder Testat sogar haftungserhöhende Wirkung entfalten?

Josef Scherer: Ja, dies kann passieren. Aufgrund entsprechender vertraglicher Vorgaben werden bereits jetzt schon zwischen Unternehmer und Kunden oder sonstigen Akteuren im Hinblick auf Compliancemanagement verbindliche Vereinbarungen getroffen, die oft sogar vertragsstrafenbewährt sind oder bei Pflichtverstößen Schadensersatzzahlungen auslösen könnten. Wird durch das Testat Unzutreffendes bestätigt, hat dies unter Umständen Einfluss auf entsprechende Sanktionsmöglichkeiten und kann zu Regressen führen.

Darüber hinaus kann auch das Werben mit einem Zertifikat, das den tatsächlichen Zustand nicht realistisch widerspiegelt, zur erhöhten Verantwortung führen. Dies wurde von mir bereits 2007 im Hinblick auf die Zertifizierung von Qualitätsmanagement- und Risikomanagementsysteme dargestellt (Scherer / Friedrich, Risikoerhöhung durch Qualitäts- und Risikomanagementsysteme, ZfAW 2007, S. 2 ff.) und gilt entsprechen auch für die Zertifizierung von Compliance-Management-Systemen. Entscheidend ist, dass das über Urkunden / Testate / Zertifikate Versprochene auch zutrifft!

Wie wird in der Praxis auditiert?

Josef Scherer: Ein Audit erfolgt üblicherweise – nicht abschließend – über Dokumentenprüfung, Interviews, Prozessprüfungen, digitale Datenanalyse und eigene Beobachtungen des Auditors.

Ist die ISO 19600:2014 (Compliance-Managementsystem) zertifizierbar?

Josef Scherer: Nein, die ISO 19600 weist keine Mussvorschriften auf und ist nicht auf Zertifizierbarkeit angelegt. Nachdenklich stimmt, dass eine weitere Arbeitsgruppe ISO an einer – zertifizierbaren – ISO 37001 ("Anti-bribery management systems") arbeitet und eventuell bereits im Jahr 2015 noch einen ersten Entwurf und 2016 die finale Fassung veröffentlichen will. Ob dann "anti-bribery" nur Korruptionsbekämpfung im Focus hat oder entsprechend der weiteren Bedeutung von "bribery" auch Geldwäsche etc., wird sich zeigen. Jedenfalls ist der Bereich von "Compliance" wesentlich weiter.

Gerade im Bericht von Korruption bis zur umfassenden Compliance zuzüglich ethischer Grundsätze gibt es bald eine unüberschaubare Zahl von "Angeboten" an Standards und Gesetzen: Den UK-Bribery Act, die US Federal Sentencing Guidelines, in Deutschland einen Leitfaden des Bundesinnenministeriums, weitere nationale Standards in Österreich (ONR) und Australien und supranational die OECD "Good practice Guidance on Internal Controls, Ethics an Compliance" sowie die "ICC Rules on Combating Corrupion", u.v.m.. Das mag bisweilen verwirren.

Wie kann im Hinblick auf ISO 19600:2014 (Compliance-Managementsystem) zertifiziert werden?

Josef Scherer: Gegebenenfalls ist eine Zertifizierung in Anlehnung an die in der ISO 19600 enthaltenen Bestimmungen möglich. Diesbezüglich wurde bereits vor Jahren im Hinblick auf Risikomanagement nach entsprechender Vorbereitung durch unsere Kanzlei vom TÜV das erste Unternehmen in Deutschland in Anlehnung an die ISO 31000 unter Heranziehung der ONR 49000 zertifiziert. Auch für die ISO 19600:2014 wäre ein ergänzender, sich an Legislative und Judikative orientierender Kriterienkatalog mit "Muss-" und "Kann-" bzw. "Soll-" Vorgaben möglich und hilfreich.

Besteht bei einer Zertifizierung von Compliance-Managementsystemen die Voraussetzung der Akkreditierung des Zertifizierers?

Josef Scherer: Soweit bisher bekannt ist, setzt die Zertifizierung von Risiko- oder Compliance-Managementsystemen noch keine Akkreditierung des Zertifizierers voraus. Da die Zertifizierung kein Hoheitsakt ist, würde auch eine Akkreditierung lediglich ein mögliches Qualitätsmerkmal im Hinblick auf Objektivität und Sachkunde des Zertifizierers darstellen.

Ob eine existierende Akkreditierung für andere Themen (beispielsweise Qualitätsmanagement, Umweltmanagement) unter Beachtung der Vorgaben des Akkreditierungsstellen-Gesetzes die entsprechende Sachkunde auch für Compliancemanagement verifizieren kann, ist zu diskutieren. Objektivität und

Sachkunde sollte zumindest nachvollziehbar und transparent sein. Dies sollte jedoch nicht nur für die jeweilige Organisation, sondern auch für die handelnden Personen gelten.

Welche rechtliche Qualität hat ein Zertifikat einer privatrechtlichen Organisation?

Josef Scherer: Ein Zertifikat eines privaten Zertifizierers stellt eine Bekundung aufgrund einer privatrechtlichen Vereinbarung dar. Keinesfalls stellt ein entsprechendes Zertifikat eine hoheitliche Maßnahme dar, die entsprechenden Vertrauensschutz genießt.

Ist bei den herkömmlichen Zertifizierungsgesellschaften bzw. Auditoren bereits die entsprechende Sachkunde bezüglich Compliancemanagement vorhanden?

Josef Scherer: Das kann nicht hinreichend beurteilt werden. In der Praxis gibt es hierzu noch wenige Informationen über entsprechende Referenzen. Klar ist, dass es bisher kaum klassische und wenige berufsbegleitende Hochschulprogramme gibt, die sich interdisziplinär mit Governance, Risk und Compliance beschäftigen. Das berufsbegleitende und akkreditierte Masterprogramm Risiko- und Compliancemanagement der Technischen Hochschule Deggendorf (THD), das gemeinsam mit dem Kompetenzportal RiskNET und dem TÜV Süd konzipiert wurde, stellt hier noch immer eine Ausnahme dar.

Welche Rolle spielt ein Testat nach IDW PS 980 im Ausland?

Josef Scherer: Da IDW PS 980 auf Deutschland bezogen ist, mag unter Umständen im internationalen Geschäftsverkehr ein entsprechendes Testat nicht die erwünschte Anerkennung, beziehungsweise Wirkung erzielen.

Sieht die ISO 19600 ähnlich wie der IDW-Standard Bereichsausnahmen vor?

Josef Scherer: Die ISO nennt entsprechende Bereichsausnahmen nicht so explizit wie der IDW-Standard. Entsprechende Bereichsausnahmen müssten auf alle Fälle vertraglich sowie im Testat und auch in der entsprechenden Zertifikatsurkunde explizit hervorgehoben werden. Im Übrigen mögen Bereichsausnahmen der Legalitätspflicht widersprechen.

Spielt die zertifizierbare ISO 9001:2015 (Qualitätsmanagementsysteme) möglicherweise im Hinblick auf den Bedarf eines Compliance-Managementsystems nach ISO 19600 eine Rolle?

Josef Scherer: Die ISO 9001:2015 (Qualitätsmanagementsysteme) sieht als primäres Ziel die Kundenzufriedenheit vor. Gleichwohl ist in diesem Standard, wenn auch nicht explizit, so doch an zahlreichen Stellen eingeflochten, die Forderung erkennbar, dass gesetzliche und behördliche Anforderungen zu erfüllen sind.

Dass zur Erfüllung der gesetzlichen und behördlichen Anforderungen (was den weiten Compliancebegriff noch nicht vollständig abdeckt) jedoch auch unter Umständen ein systematisches Vorgehen im Sinne von Compliancemanagement erforderlich ist, nennt die ISO 9001 nicht.

Ebenso erwähnt diese Norm neuerdings den "verstärkten" prozessorientierten und "neuen" risikobasierten Ansatz an zahlreichen Stellen, konstatiert jedoch gleichwohl, dass ein Risikomanagementsystem, insbesondere auch nach ISO 31000, nicht erforderlich sei, um die Kundenanforderungen zu erfüllen. Dies mag den sachkundigen Leser irritieren. Außerdem muss ein "risikobasierter Ansatz" zwingend auch Compliance-Risiken umfassen, da angemessenes Risikomanagement nicht ein ganz erhebliche Risikogruppe (Compliance-Risiken) einfach ausklammern darf.

Somit verlangt auch die ISO 9001:2015 nach Compliance- und Risikomanagement im Unternehmen. Diese "Systeme" sollten angemessen und wirksam sein, müssen sich jedoch nicht zwingend nach den einschlägigen ISO-Normen richten.

Belastend für die Praxis ist jedoch der sogar wachsende Trend der Standard-Ersteller, immer mehr zusätzliche Management-System-Inseln zu schaffen, statt – was ohne weiteres möglich wäre – der Praxis einen Standard zur Verfügung zu stellen, der diverse Anforderungen integriert. Cui bono? Wem nützt das? Ein positives Beispiel stellt dagegen der PAS 99 (2012) zum integrierten Managementsystem dar.

Wird die ISO 19600:2014 (Compliance-Managementsystem) im Ausland Anerkennung finden?

Josef Scherer: ISO-Standards sind im Ausland durchaus bereits sehr verbreitet und anerkannt. Gleichwohl gibt es auch Regionen, die auf COSO-Standards aufbauen. COSO ist beispielsweise im anglo-amerikanischen Rechtsraum noch stärker verbreitet als ISO. COSO I (2014) (International Control) erweiterte in der neuen Version gerade seinen Anwendungsbereich in Richtung "social responsibility", wozu bei entsprechender Interpretation auch Compliance zählen mag und COSO II (2004) beschäftigt sich mit Risikomanagement: Es läuft wieder auf Governance, Risk und Compliance (GRC) hinaus.

Welche rechtliche Bedeutung haben Standards?

Josef Scherer: Standards können unter Umständen einen bestimmten technischen Stand, wie beispielsweise den "Stand der Technik" oder die "Anerkannten Regeln der Technik" (den "Anerkannten Stand von Wissenschaft und Praxis") widerspiegeln. Nach Rechtsprechung von Bundesgerichtshof oder Bundesverwaltungsgericht besteht bei idealtypisch zu Stande gekommenen Standards eine entsprechende Vermutungswirkung, dass der Standard die "Anerkannten Regeln der Technik" widerspiegelt.

Es muss aber bezweifelt werden, dass bei dem derzeit inflationär produzierten Standards immer von einem "idealtypischen" Zustandekommen in Transparenz, Fach- und Sachkunde bezüglich der maßgeblichen Disziplinen und Beteiligung der Öffentlichkeit auszugehen ist.

Wie ist das Thema "pflichtgemäßes Verhalten von Geschäftsführung, Vorstand, Aufsichtsrat" in Hinblick auf §§ 43 GmbHG, 93, 107 Aktiengesetz, 130 OWiG etc. und auf den "Anerkannten Stand von Wissenschaft und Praxis" und bezüglich des Standards ISO 19600 abzugrenzen?

Josef Scherer: Die Pflichten zur gewissenhaften Geschäftsführung ergeben sich primär aus dem Gesetz und richten sich nach dem aktuellen Stand von Gesetzgebung und Rechtsprechung.

Dabei wird häufig auf den "Anerkannten Stand von Wissenschaft und Praxis" als Messlatte für den einzuhaltenden Pflichtmaßstab Bezug genommen.

Entsprechende Standards wie ISO 19600 spiegeln diesen "Stand von Wissenschaft und Praxis" im Sinne einer Vermutungswirkung nur dann wider, wenn sie idealtypisch zustande gekommen sind. Dies wäre zu verifizieren. Ebenso kann auch eine Vermutung natürlich widerlegt werden.

Besteht eine Vermutung, dass ISO- oder IDW-Standards generell idealtypisch zustande kommen?

Josef Scherer: Dies müsste im Detail überprüft werden, da hierzu oft die nötige Transparenz fehlt. Bisweilen wird argumentiert, dass in diesen Institutionen durch zahlreiche einzugehende Kompromisse, aber auch sogar durch Lobbyismus und der bisweilen fehlenden Darstellung vertieften des maßgeblichen Kernbereichs Standards nicht optimiert gefasst seien.

Dennoch können die positiven Elemente des Standards Hinweise auf vernünftiges und pflichtgemäßes Verhalten geben und sind zumindest diesbezüglich begrüßenswert.

Enthält der Kernbereich eines Compliance-Management-Systems auch Risikomanagement-Komponenten wie beispielsweise die Erkennung, Analyse, Bewertung und Steuerung von Compliance-Risiken?

Josef Scherer: Dies ist zu bejahen und wird auch in der Literatur immer wieder angeführt. Im Kern geht es bei einer Compliance-Risikoanalyse um nichts anderes als die Analyse einer spezifischen Risikoart, eben Compliance-Risiken. Die Methoden, die sich im Risikomanagement als "Stand von Wissenschaft und Praxis" entwickelt haben, können auch bei Compliance-Risiken angewendet werden. Zudem bestehen aus einer unternehmensweiten Sicht auf die Risikolandkarte vielfältige Abhängigkeiten zwischen Compliance-Risiken und anderen Risikoarten, etwa Reputationsrisiken oder Finanzrisiken.

Sind aufgrund der in einem CMS vorhandenen Risikomanagementkomponenten Kompetenzen von Standarderstellern und Auditoren nicht nur im Bereich Compliancemanagement, sondern auch im Bereich Risikomanagement gefragt?

Josef Scherer: Auch dies ist eindeutig zu bejahen. Sowohl Standardersteller als auch Auditoren oder Zertifizierer müssen Kenntnis bezüglich der nach "Anerkanntem Stand von Wissenschaft und Praxis" anzuwendenden Methoden des Risikomanagements, aber auch des Prozessmanagements und der Anforderungen aus Zielsetzung und Planung mit Kennzahlen sowie Steuerung und Überwachung haben und die entsprechenden Tools und Methoden zum sachlich richtigen Einsatz bringen.

[Die Fragen stellte Frank Romeike, Chefredakteur RiskNET sowie Mitglied des Vorstands beim Institut für Risikomanagement und Regulierung (FIRM)]

Prof. Dr. jur. Josef Scherer ist seit 1996 Professor für

Unternehmensrecht (Compliance), insbesondere Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf sowie Gründer und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliance Management der Technischen Hochschule Deggendorf THD. Zuvor arbeitete er als Staatsanwalt und Richter in einer Zivilkammer an verschiedenen Landgerichten.

Neben seiner Tätigkeit als Seniorpartner der auf Governance, Risk & Compliance (GRC) spezialisierten Wirtschaftsrechtskanzlei Prof. Dr. Scherer, Dr. Rieger & Partner erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren. Von 2001 bis 2014 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.
In Kooperation mit TÜV und RiskNET konzipierte er als Studiengangsleiter und Referent den akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliance Management an der Technischen Hochschule Deggendorf.

Seine Forschungs- und Tätigkeitsschwerpunkte mit zahlreichen Publikationen liegen auf den Gebieten der Managerhaftung, Governance, Compliance- und Risikomanagement sowie des Vertragsmanagements, Produkthaftungsrechts, Krisen-, Sanierungs- und Insolvenzrechts.

[Bildquelle: © Marco2811 - Fotolia.com]