01.15

10. Jahrgang
Februar 2015
Seiten 1 – 48

10 Jahre ZRFC

ZRFC

Risk, Fraud & Compliance

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

ESV ERICH SCHMIDT VERLAG

64683

Keywords: *CMS*
ISO 19600
Standard
Leitfaden

ISO-Compliance

Ein internationaler Leitfaden für das Unternehmens-CMS

RA Dr. Christian Schefold*

Es ist ein erster Leseeindruck vom neuen ISO-Standard 19600 „Compliance management systems – Guidelines", der in seiner Erstauflage offiziell von der International Organization for Standardization (ISO) in Genf am 15. Dezember 2014 veröffentlicht wurde. Dieser Beitrag will eine zusammenfassende Darstellung, erste Analyse wie auch Einschätzung über seine möglichen Auswirkungen vermitteln. Wie der ISO-Standard – der offiziell nur einen Leitfaden- bzw. Empfehlungscharakter hat – in der Wirtschaft weltweit übernommen wird, bleibt noch abzuwarten. Die ZFRC wird die Entwicklung aufmerksam beobachten und über erste Anwendungsfälle und ihre Ergebnisse berichten.

1. Einleitung: Compliance – ein Handelshemmnis?

Im Vorwort des Standards stellen seine Autoren – das Projektkomitee ISO/PC271 – sogleich einen Bezug zu den völkerrechtlichen Zielen der ISO her: Die ISO dient als internationale Nichtregierungsorganisation unter anderem durch den Abbau von Handelshemmnissen primär der Förderung des internationalen Handels und steht daher nicht nur örtlich der Welthandelsorganisation [World Trade Organization, (WTO)] in Genf nahe. Ob der Hinweis zum Abbau technischer Handelshemmnisse [Technical Barriers to Trade, (TBT)] und damit zu dem entsprechenden GATT-Übereinkommen der Uruguay Runde 1994 – einem der Gründungsdokumente und Grundpfeiler der WTO – hier in Zusammenhang mit Compliance ein richtiger ist, sei einmal dahingestellt. Es ist jedoch der erste Eindruck: Wir bewegen uns hier auf dem Feld des internationalen Freihandels; Compliance hat die Sphären der Welthandelsorganisation erreicht. Die Compliance-Bewegung hat globale Auswirkungen und es besteht ein Bedarf an weltweit einheitlichen Lösungen.

Der neue Compliance-Standard – auch wenn es nach den Autoren bloß ein Leitfaden ist – soll weltweit für eine gewisse Vereinheitlichung sorgen. Compliance ist aber kein technisches Handelshemmnis. Compliance im Sinne der Rechtstreue von Unternehmen ist auch kein Qualitätsmerkmal von Produkten oder Dienstleistungen. Compliance geht eine Dimension weiter und spricht den Integritätshintergrund von Produkten und Dienstleistungen an. Maßstab für Integrität und Legalität sind aber gesellschaftliche Kriterien wie nationale Rechtsnormen, nationale oder auch regionale Kulturauffassungen. Wenn Unternehmen sich mit Compliance an nationale Kriterien halten (und sich nicht wie manche multinationale Einheiten einfach darüber hinwegsetzen), kann dies eine Einschränkung des Weltwirtschaftsverkehrs bedeuten. Diese Beschränkung ist aber durch die jeweiligen Staaten und Staatenverbände (etwa der EU) und nicht durch Unternehmen verursacht. Traditionell hat ISO dann weltweit einheitliche Standards entwickelt. Es könnte nun ein Freihandelsansatz sein, Empfehlungen zum Verhalten in unterschiedlichen Rechts- oder Kulturkreisen zu geben und Maßstäbe für eine „internationale Compliance" zu setzen. Diese Ansätze verfolgt ISO 19600 aber erkennbar nicht.

Dr. Christian Schefold

Das Ziel der ISO-Norm ist die allgemeine Geltung von Grundsätzen für ein Compliance-Management-System (CMS). Das Vorwort stellt den Bezug zu rechtlichen (und keinesfalls technischen) Anforderungen klar: Nachdem nun in einigen Rechtsordnungen Gerichte bei der Zumessung von Sanktionen gegen Rechtsverstöße den Status der jeweiligen unternehmensinternen CMS berücksichtigt haben, spricht ISO 19600 ausdrücklich Legislative und Exekutive der Staaten an: Sie sollen von diesem neuen Standard als Benchmark profitieren. Damit verlässt die ISO den Boden ihrer eigentlichen Aufgabe, durch (technische) Standardisierung Freihandel zu ermöglichen. Werden ISO-Standards in Zukunft Grundlage von Strafzumessungsentscheidungen sein?

2. Der Compliance-Begriff der ISO-Welt

Wie ist Compliance im Sinne dieses neuen Leitfadens ISO 19600 zu verstehen? In der Einführung zum Text des Standards wird sogleich eine Definition des Begriffs geboten. Frei ins Deutsche übersetzt wird Compliance ISO-mäßig wie folgt interpretiert: Compliance (i) entsteht, wenn eine Organisation – d. h. im Regelfall ein Wirtschaftsunternehmen – ihren Verpflichtungen nachkommt und (ii) wird dadurch nachhaltig, indem es in die Kultur des Unternehmens sowie dem Auftreten und der persönlichen Einstellung der für das Unternehmen tätigen Menschen verinnerlicht wird.

- zu i): Verpflichtungen ergeben sich dabei nicht nur aus den jeweils anzuwendenden Rechtsnormen, sondern auch aus Industriestandards sowie allgemeinen Anforderungen an Organisation, gute Unternehmensführung, Best Practices, ethische Anforderungen und – sehr weitgehend – der Erwartungshaltung der jeweiligen Gesellschaft.
- zu ii): Die Verinnerlichung (bzw. Integration oder Einbettung) von Compliance als Grundlage der Nachhaltigkeit erfolgt vor allem als Konsequenz des Führungsverhaltens aller Managementebenen bei der Anwendung eindeutiger Werte, allge-

* Dr. Christian Schefold ist Rechtsanwalt im Berliner Büro der globalen Wirtschaftskanzlei Dentons.

ISO 19600 ist ein Compliance-Leidfaden, der auf funktionalen Bereichen aufbaut.

mein anerkannter Führungsgrundsätze, ethischer und gesellschaftlicher Regeln sowie der Umsetzung und Wertschätzung von Maßnahmen zur Förderung Compliance-gerechten Verhaltens.

In der Einführung wird zugleich Organisatorisches unmittelbar angesprochen: Selbst wenn eine Compliance-Funktion (im Sinne einer Compliance-Organisation oder ein Compliance-Management) unabhängig bleiben soll, muss eine Integration mit den, für Finanzen, Risikomanagement, Qualitätsmanagement, Produktsicherheit, Umwelt- und Gesundheitsschutz sowie für operative Anforderungen und Verfahren zuständigen Unternehmensbereichen stattfinden. Damit werden zwei Grundsätze einer Compliance-Organisation vorweggenommen: Unabhängigkeit – sowie Integration und Zusammenarbeit mit anderen Unternehmensfunktionen.

Ferner gibt es eine weitere, aufschlussreiche Aussage in der Einführung: Ein wirksames, das gesamte Unternehmen umfassendes CMS ermöglicht es dem Unternehmen, sein Bekenntnis zu Compliance nachzuweisen. Es schließt sich der Kreis zum Vorwort: Der Standard soll als Benchmark für richterliche bzw. behördliche Entscheidungen dienen. Dann scheint es nur allzu konsequent, ein Compliance-System allein auf die entsprechende Nachweisbarkeit hin auszurichten.

3. Struktur des ISO-Leitfadens

Diese ISO-Norm definiert jedoch keine Anforderungen, sondern soll nur Anleitung und Empfehlung (guidance) für ein Unternehmens-CMS und die Compliance-Praxis in Unternehmen darstellen. Der Standard ist Orientierung für den Aufbau, die Entwicklung und Umsetzung, die Bewertung, die Pflege und die Verbesserung eines wirksamen und reaktionsfähigen CMS.

Die Autoren des Standards legen so mehrfach Wert auf die Erwähnung, dass der Standard flexibel handhabbar sein und je nach Größe, Ausgereiftheit des CMS und Situation des Unternehmens sowie Natur und Komplexität der Unternehmenstätigkeit (einschließlich des Compliance-Konzepts und der jeweiligen Compliance-Ziele eines Unternehmens) angepasst werden kann. Gerade aber Detailhinweise und Beispiele differenzieren nicht nach Unternehmensgrößen, sodass der Eindruck entsteht, es müsse das gesamte Werk implementiert werden. Wenn im Rahmen des sonst im Standard zuweilen vorherrschenden Detaillierungsgrad keine gleichermaßen detaillierten Hinweise auf mögliche Anforderungsreduktionen gegeben werden, wird im Zweifel immer auf eine vollständige Umsetzung hingewirkt werden – gerade aus Risikogesichtspunkten. Wirklich mittelstandsfreundlich ist der Standard damit nicht.

Der ISO 19600 Standard setzt auf sieben, eher funktionale Bereiche eines CMS auf:

- 1. Unternehmenssituation (context of the organization)
- 2. Führung (leadership)
- 3. Strategie (planning)
- 4. Hilfestellung (support)
- 5. Betrieb (operation)
- 6. Leistungsbewertung (performance evaluation)
- 7. Verbesserung (improvement)

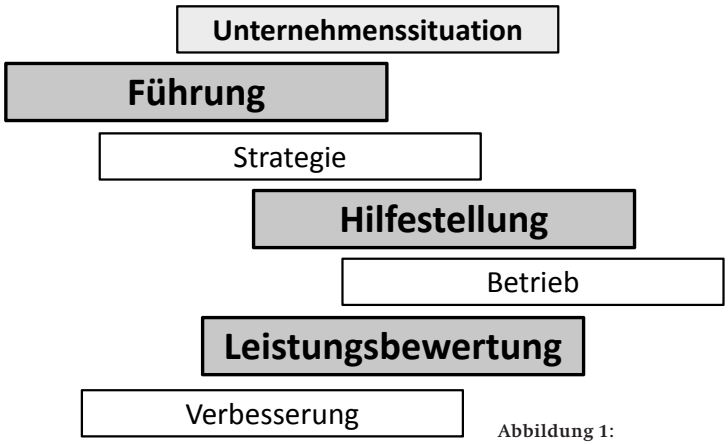


Abbildung 1: Bereiche eines Compliance-Management-Systems (CMS) nach ISO 19600

Den Schwerpunkt des Standards bilden die Bereiche Führung (2), Hilfestellung (4) und Leistungsbewertung (6). Auch der Unternehmenssituation (1) wird noch recht viel Aufmerksamkeit gewidmet – wenngleich deutlich weniger als bei den erstgenannten Bereichen. Weniger berücksichtigt werden Strategie (3), Betrieb (5) und Verbesserung (7).

3.1 Unternehmenssituation

Der Standard setzt als Grundlage auf einem Verständnis des Unternehmens, seines Umfelds und seiner Situation auf. Bemerkenswert ist, dass nicht alleine auf eine Compliance-Risikoanalyse abgestellt, sondern eine gesamtheitliche, umfassende Betrachtung des Unternehmens gefordert wird. Zwar muss die Evaluation der Unternehmenssituation unter Compliance-Bezug erfolgen, es wird aber nicht alleine auf Compliance-Risiken abgestellt.

Es müssen alle wesentlichen externen und internen Anhaltspunkte berücksichtigt werden: Der regulatorische, soziale und kulturelle Kontext (das gesellschaftliche Umfeld), der Unternehmenszweck, die wirtschaftliche Situation (das wirtschaftliche Umfeld), bereits bestehende interne Regeln, Verfahren (Prozesse), Vorgehensweisen (Prozeduren) und die zur Verfügung stehenden Ressourcen. Auch sind alle, für das CMS relevante Personen und deren Interessen einzubeziehen. Ferner sind die Wechselwirkungen auf Unternehmensergebnisse und Compliance-Ergebnisse zu beachten und einzuschätzen.

Die Unternehmenssituation bestimmt den Umfang des CMS und damit auch den

Grundlage für die ISO-Compliance ist die Unternehmenssituation.

der Compliance-Funktion (bzw. der Compliance-Organisation). Der ISO-Standard fordert – neben der eingangs erwähnten Unabhängigkeit und Integration – einen unmittelbaren Zugang zur Geschäftsleitung (Da wohl bei ISO eher von einem monistischen Verständnis einer Geschäftsleitung ausgegangen werden kann, bedeutet dies auch einen Zugang zum Aufsichtsrat und seinen entsprechenden Ausschüssen.), ausreichende Autorität und Ausstattung.

Im Rahmen der Evaluierung des Unternehmenskontextes sind auch bestehende Compliance-Pflichten (compliance obligations) zu ermitteln und ihre Auswirkungen auf die Unternehmenstätigkeit, -produkte und -dienstleistungen festzustellen. Die Erfüllung dieser Pflichten ist Grundlage dafür, dass Unternehmens-CMS aufzubauen, zu entwickeln, einzuführen, umzusetzen, zu prüfen, zu pflegen, zu betreiben und zu verbessern.

Compliance-Pflichten können sich zum einen aus zwingenden Compliance-Anforderungen (requirements) gesetzlicher Art und zum anderen aber auch aufgrund freiwilliger Compliance-Versprechen (commitments) ergeben. Compliance-Pflichten können sich stets verändern und müssen an wandelnde zwingende und freiwillige Anforderungen angepasst werden. Dabei sollen Unternehmen alle verfügbaren Informationsquellen ausnutzen. Unter anderem werden im Standard als Beispiele explizit sowohl die Mitgliedschaft in entsprechenden Verbänden und die Teilnahme an deren Veranstaltungen (in Deutschland wäre hierzu etwa DICO zu zählen) als auch eine enge Zusammenarbeit mit Rechtsberatern genannt.

Gewissermaßen als letzter Schritt erfolgt eine Identifikation, Analyse und Bewertung von Compliance-Risiken. Nach dem Verständnis des Standards gelten als Compliance-Risiken sowohl die Ungewissheit des Erreichens gewünschter Compliance-Ergebnissen als auch Situationen, in denen erkannter Maßen Compliance-Verstöße vorkommen können. Selbstredend kann die Risikoanalyse nur im Hinblick auf die gesamte Unternehmenssituation erfolgen. Mögliche Quellen potenzieller Compliance-Verstöße, ihre Wahrscheinlichkeit und ihre eventuellen Auswirkungen (unmittelbare Schäden wie auch mittelbare Konsequenzen wie z. B. Sanktionen), sind ebenfalls zu ermitteln.

Für das CMS und seine Ausrichtung ist letztendlich aber nur die Risikobereitschaft des Unternehmens von Bedeutung. Auf der Grundlage der Risikoevaluation, hat die Geschäftsleitung eine unternehmens-individuelle Risikoeinstellung zu definieren. Hiervon sind insbesondere die Compliance-Kontrollen abhängig: Ist die Einschätzung der Risikolage kritischer als die beschlossene Risikobereitschaft, so besteht hier ein besonderer Handlungs- und Kontrollbedarf. Die jeweilige Einschätzung für einzelne Risikobereiche führt zu einer Priorisierung von Compliance-Risiken und Compliance-Maßnahmen sowie auch zur Bestimmung von Art, Umfangs und Häufigkeit von Kontrollmaßnahmen.

Risikoanalysen müssen kontinuierlich entlang der Entwicklungen und Veränderungen im Unternehmen vorgenommen werden. Insbesondere Änderungen der Unternehmenstätigkeit, der Produkte oder Dienstleistungen des Unternehmens, Änderungen der Unternehmensstruktur und der strategischen Ausrichtung Unternehmens – aber auch externen Entwicklungen (z. B. des wirtschaftlichen Umfelds, des Marktes, der Haftungsregeln und von Kundenbeziehungen) einschließlich des Wandels sowohl zwingender als auch freiwilliger Anforderungen und letztendlich auch Compliance-Verstöße erfordern eine Neuanalyse.

3.2 Führung

Führung und Engagement (commitment – auch Bekenntnis) für Compliance liegen bei Geschäftsleitung (governing body) und Topmanagement. Der Geschäftsleitung obliegt es, Unternehmenswerte und alle sonstigen Grundlagen für Compliance zu schaffen – gegebenenfalls durch Geschäftsleitungsbeschluss. Die Geschäftsleitung muss Übereinstimmung zwischen Unternehmens- und Compliance-Zielen herstellen. Auch die Compliance-Kommunikation, die Anweisung und Anleitung der Unternehmensmitarbeiter zur Unterstützung der Wirksamkeit des Unternehmens-CMS, ist eine Angelegenheit der Geschäftsleitung. Sie verleiht der Compliance-Funktion die notwendige Autorität und stattet sie mit den erforderlichen Mitteln aus. Letztendlich liegt bei der Geschäftsleitung auch die Verantwortung für eine kontinuierliche Entwicklung im Sinne der Verbesserung des CMS.

Gesamthaft sollte das Compliance-Management-System in einem CMS-Konzept (compliance policy – oder auch Compliance Handbuch bzw. Compliance Programm Manual) dargestellt und von der Geschäftsleitung als für das gesamte Unternehmen verbindlich verabschiedet werden.

Auch wenn Unternehmensleitung und Topmanagement primär für Compliance verantwortlich sind, ist eine Delegation der Verantwortung für Compliance im Unternehmen möglich. Hier erkennt der ISO-Standard verschiedene Optionen an: Die Delegation kann an eine besonders bezeichnete Person (Compliance-Officer), an ein Compliance-Komitee, aber auch an Externe „outgesourced“ werden. Ferner sind Mischformen möglich. Darüber hinaus ist jeder im Unternehmen und insbesondere jede Führungskraft (manager) im Unternehmen in seinem Verantwor-

ISO 19600 betont die Verantwortung der Geschäftsleitung.

tungs- und Tätigkeitsbereich für Compliance verantwortlich. In Stellenbeschreibungen muss eine klare Verantwortung zugeschrieben werden. Der Grad der Verantwortung bemisst sich am Level des Managements:

- 1. Unternehmensleitung/Topmanagement
- 2. Führungskraft in der Compliance Funktion
- 3. Führungskraft/Management
- 4. Mitarbeiter

3.3 Strategie

Das CMS-Konzept ist auf das erwünschte Ergebnis (oder Ziel) des CMS auszurichten. Compliance-Risiken sollen erkannt und verhindert werden. Dies ist insbesondere durch konstante Verbesserung zu erreichen. Die Planung umfasst vor allem die Compliance-Maßnahmen (u. a. Definition, Einschätzung der erforderlichen Mittel, Zuordnung der Verantwortung), ihre Integration in das CMS (insbesondere ein Zeitplan) sowie die Messung ihrer Wirksamkeit (z. B. Definition von Bemessungskriterien etwa in der Form von Key Performance-Indikatoren, den sogenannten KPI). Wie alle Compliance-Bereiche, ist auch das Vorgehen in der Planung zu dokumentieren.

3.4 Hilfestellung

Die Umsetzung von Compliance im Unternehmen bedarf einer bestimmten Unterstützung oder Hilfestellung gegenüber den Mitarbeitern des Unternehmens. Zunächst sind die erforderlichen Compliance-Kompetenzen der jeweiligen Mitarbeiter zu ermitteln und diese Kompetenzen gegebenenfalls durch Schulungen herzustellen. Wichtig ist eine Sensibilisierung der Mitarbeiter: Sie müssen sich des Compliance-Konzepts, ihrer Rolle im und ihrer Beiträge zum CMS sowie der Konsequenzen der Nichtbeachtung von Compliance-Pflichten bewusst sein. Schulungen sind bei bestimmten Situationsänderungen (Hierzu gibt es ebenfalls eine größere Aufzählung: Änderungen der Stelle, der Compliance-Pflichten, der Unternehmensstruktur, -tätigkeit, -produkte und -dienstleistungen sowie bei Compliance-Vorfällen und kritischen Rückmeldungen bzw. Hinweisen) zu wiederholen. Compliance muss belohnt werden; Compliance-Verstöße sind zu ahnden.

In der Hilfestellung und Unterstützung liegt auch eine besondere Verantwortung des Topmanagements: Eine Compliance-Kultur im Unternehmen kann nur entstehen, wenn das Unternehmens-CMS anerkannt und wirksam ist. Dies bedeutet, dass das Unternehmens-CMS nach der Überzeugung aller Interessenten an Compliance implementiert ist. Die Verantwortung für die Verbesserung nach Compliance-Verstößen muss auf allen Ebenen angenommen und Maßnahmen von allen umgesetzt werden. Die Rolle der Compliance-Funktion und ihr Wirken müssen anerkannt sein. Mitarbeiter kommunizieren unbeeinträchtigt über Schwachstellen des CMS an die zuständigen Ebenen des Managements.

In allen Bereichen des ISO-Standards wird immer auf die Notwendigkeit einer ausreichenden Dokumentation hingewiesen. Im Bereich der Hilfestellung erscheinen die Ausführungen zur Dokumentation des Compliance-Konzepts und des CMS besonders detailliert. Zur Dokumentation gehören Angaben über:

- Ziele, Struktur und Inhalte des CMS
- Rollen, Zuständigkeiten und Verantwortlichkeiten
- Auflistung der Compliance-Pflichten
- Auflistung der Compliance-Risiken und der Priorisierung anhand der Risikoanalyse
- Auflistung von Compliance-Verstößen und Compliance-Gefahrensituationen (near misses)

Der ISO-Leitfaden ist eine Ergänzung staatlicher Anforderungskataloge.

- Ergebnisse der jährliche Compliance-Planung
- Schulungsdaten (auch als Personaldaten)

Selbstredend ist auch die Dokumentation stets zu aktualisieren und ihre Richtigkeit wie auch Vollständigkeit zu kontrollieren. Der Umfang der Dokumentation hängt vom Unternehmen, der Kompetenz der Mitarbeiter und der Reife des CMS ab.

3.5 Betrieb

Der Betrieb setzt nach den Vorstellungen der Standardautoren schon bei der Detailplanung an. Er umfasst sowohl diese als auch die Umsetzung und Kontrolle der Prozesse, die erforderlich sind, die festgestellten Compliance-Pflichten zu erfüllen und die definierten Maßnahmen umzusetzen: Es sind die Verfahrensanweisungen [Prozesse: Eine Reihe zusammenhängender Aktionen, die aus gewissen Grundlagen (inputs) Ergebnisse (outputs) herbeiführen.] und Arbeitsanweisungen (Prozeduren: Beschreibungen, wie Prozesse oder andere Maßnahmen ausgeführt werden.). Hierzu gehören die Darstellung, wie Compliance-Prozesse (oder auch Maßnahmen) funktionieren sollen und ebenfalls die Definition ihrer Ziele, Umsetzungskriterien, Verfahrensabläufe sowie die damit verbundenen Kontrollen. Schließlich zählen auch die Prozessdokumentation sowie ihre Archivierung dazu. Auch die Kontrolle von Ergebnissen – ob planmäßig oder nicht – einschließlich der vorzusehenden Konsequenzen und auch die Einleitung von Anschlussprozessen und -maßnahmen zur Beseitigung oder Anpassung unerwünschter Ergebnisse und Auswirkungen sind Bestandteil davon.

3.6 Leistungsbewertung

Das Unternehmen muss stets die Leistung des CMS und seine Wirksamkeit bewerten. Während die Ausführungen zum Betrieb einen verfahrenstechnischen Ansatz zeigen, kann man an der umfangreichen Darstellung der Leistungsbewertung eines CMS, seiner Überwachung, Messung, Analyse und Bewertung den ingenieurtechnischen Hintergrund von ISO erkennen.

Zunächst ist festzulegen, was überwacht und gemessen werden soll – und warum. Ferner sind die Methoden der Überwachung, Messung, Analyse und Bewertung abzustimmen, um verwertbare Ergebnisse zu erhalten. Ein Überwachungs- und Messplan ist festzulegen und damit, wann die Überwachungs- und Messergebnisse analysiert, bewertet und berichtet werden sollen. Der Standard gibt hierzu Beispiele und führt auch einzelne typische Gegenstände der Überwachung aus.

Typische Feedback-Quellen sind für ISO zum einen die Mitarbeiter, Kunden und Zulieferer – insbesondere durch Hinweisgeber-Systeme. Ferner sollen Regulierungsbehörden ebenfalls Quellen sein. Dies erfordert einen steten Kontakt zu den Behörden und einen Austausch sowie Rückmeldung über externe Kontrollen. Die Kontrollen im Unternehmen und auch die Überwachungssysteme sind automatisiert und auch manuell auszuwerten. Als Methoden der Informationsgewinnung werden alle modernen Informationsquellen empfohlen: ad hoc-Informationsquellen, Hinweisgeber-Systeme, informelle Quellen (Diskussionen, Blogs, usw.), Integritätstest (mystery shopping), Stimmungsbilder, Beobachtungen, Audits und Prüfungen, Anfragen bei Trainings usw.

Informationen müssen analysiert und klassifiziert werden. Auch hier ist die Entwicklung und Definition von messbaren Indikatoren (KPIs) zur Quantifizierung der Compliance-Leistung erforderlich. Die vielfältigen Messungen und Messdaten können, mit den Ergebnissen des Risiko-Assessments kombiniert, zu vielfältigen Demonstrationen (statistische Informationen, Schaubilder u.v.m.) des Wirkungsgrades eines CMS führen. Kontrollergebnisse sind zu dokumentieren, zu berichten und zu archivieren.

Auch ein Auditing mit einem Audit-Plan und -Kriterien, einer Definition des Umfangs sowie der Benennung der Auditoren gehört dazu. Ferner ist auch ein Management-Review der Geschäftsleitung über eine Gesamtsicht der Bewertung erforderlich.

3.7 Verbesserung

In diesem Abschnitt macht der Standard deutlich, dass das Versagen eines CMS, Verstöße zu verhindern oder aufzudecken, nicht notwendigerweise bedeutet, dass das CMS im Hinblick auf seine Zwecke der Prävention und Aufdeckung von Compliance-Verstößen unwirksam und damit ungeeignet ist. Fehler in Form mangelnder Übereinstimmung tatsächlicher Ergebnissen mit geplanten Zielen, Zuwiderhandlungen und Korrekturmaßnahmen müssen aber zu Anpassungen führen. Notfalls ist der Anpassungsbedarf bis zur Geschäftsleitung (einschließlich Aufsichtsrat und seine Ausschüsse) und dem Topmanagement zu eskalieren. Für die Eskalation wird die Definition eines Prozesses empfohlen; so soll eine kontinuierliche Verbesserung auch organisatorisch sichergestellt werden.

4. Vergleich zu anderen Compliance-Standards

Der neue ISO-Standard ist nicht das erste Grundsatzpapier für Compliance-Programme. Daher bietet sich ein Vergleich zu einigen der bestehenden Standards oder Vorgaben an:

ISO 19600 werden schnell weitere ISO-Anforderungen folgen!

4.1 US Federal Sentencing Guidelines

Der ISO 19600 Standard enthält keine Bezugnahme auf bestimmte Normen und rechtliche Anforderungen; er erscheint aber durchaus als eine detaillierte Ergänzung des 1991 begonnenen und 2013 überarbeiteten Strafzumessungsleitfadens für Organisationen aus der Feder des US-Justizministeriums. In Kapitel 8 „Sentencing of Organizations" werden Minimalanforderungen für ein wirksames Compliance-Programm definiert, die unter anderem von straffälligen Unternehmen innerhalb der Bewährungszeit umzusetzen sind. Ziel dieser staatlichen Compliance-Anforderungen ist es, im Unternehmen Maßnahmen umzusetzen, die strafbares Verhalten vorbeugen und aufspüren helfen. Die Maßnahmen sollen nach §8B2.1 der Federal Sentencing Gudelines in einem Compliance and Ethics Program (compliance policy oder Compliance-Konzept) zusammengefasst werden, welches angemessen definiert und umgesetzt sowie auch allgemein im Unternehmen wirksam ist. Ein detaillierter Vorschlag zur Umsetzung kann nun in der ISO-Norm 19600 besichtigt werden.

4.2 UK Guidance

Die 2011 veröffentlichte Guidance des britischen Wirtschaftsministeriums zum UK Bribery Act 2010 bezieht sich allein auf Anti-Bribery-Compliance und besteht aus sechs Grundsätzen, die weiter ausgeführt werden: Die Selbstverpflichtung der Geschäftsleitung zu Compliance (Grundsatz 2) ist Grundlage eines Anti-Korruptions-Compliance-Programms. Das Programm setzt auf einer Risikoanalyse auf (Grundsatz 3), die die Grundlage für die Gestaltung eines angemessenen Verfahrens (Grundsatz 1), des Compliance-Programms darstellt. Zu dem Programm zählen insbesondere die sorgfältige Auswahl von Mitarbeitern und Geschäftspartnern, Kommunikation und Schulung und Überwachung (Grundsätze 4-6).

Der ISO-Standard ist für alle Compliance-Themenfelder anwendbar. Die Grundsätze der Guidance sind innerhalb der funktionalen Bereiche des ISO-Leitfadens abbildbar. Die Herausforderung droht aus einem anderen ISO-Projekt: Die ISO-Norm 37001 steht in den Startlöchern. Sie soll wirkliche Anforderungen für ein „anti-bribery management system" aufstellen. Diese Initiative stammt aus Großbritannien und soll die eher allgemeinen Vorgaben des UK Bribery Act und ihrer Guidance in konkreten Anforderungen präzisieren und verbindlich darstellen. ISO 37001 wird nach den entsprechenden ISO-Grundlagen zertifizierbar sein. Dies ist für den bloßen Leitfaden ISO 19600 noch nicht der Fall. Die weitere Entwicklung der Compliance-Vorgaben „nach ISO" ist damit offen.

Principles nach Guidance / Bereiche nach ISO 19600	Bekenntnis (2)	Risikoanalyse (3)	Verfahren (1)	Due Diligence (4)	Schulung (5)	Überwachung (6)
Unternehmenssituation		■				
Führung	■		■	■		
Strategie						
Hilfestellung			■		■	
Betrieb			■			
Leistungsbewertung						■
Verbesserung						■

Abbildung 2:
UK Guidance ./. ISO 19600

4.3 AS 3806

Beim Betrachten unterschiedlicher Compliance Standards wird die enge Verwandtschaft zwischen dem ISO 19600 und dem Australian Standard 3806-2006 schnell offenbar. Trotz aller Unterschiede – schließlich ist das Modell „down under" schon etwas älter – gibt es im Aufbau und den detaillierten Aufzählungen von Anforderungen und Beispielen sowie auch der Wortwahl eine systematische Verwandtschaft. 1998 gab es die erste Version des Standards. Die derzeit gültige ist aus 2006 und möglicherweise ist die ebenfalls nach acht Jahren entstandene ISO 19600 nun gleichfalls die dritte Generation des AS 3806.

Die Integration der ISO- und der IDW-Welten wird eine Herausforderung sein.

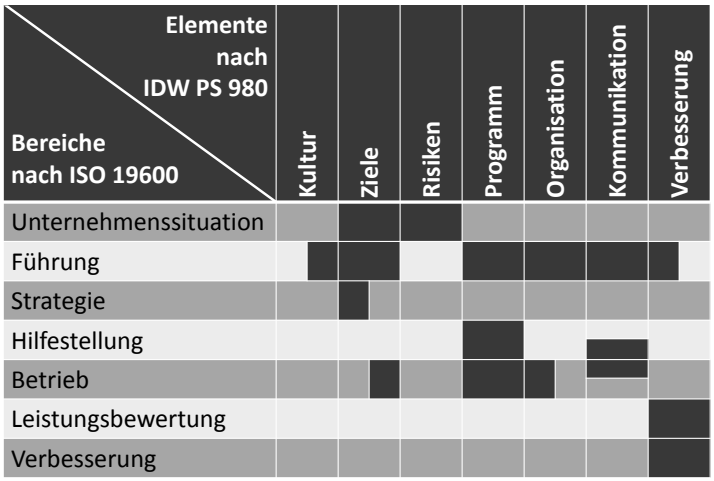
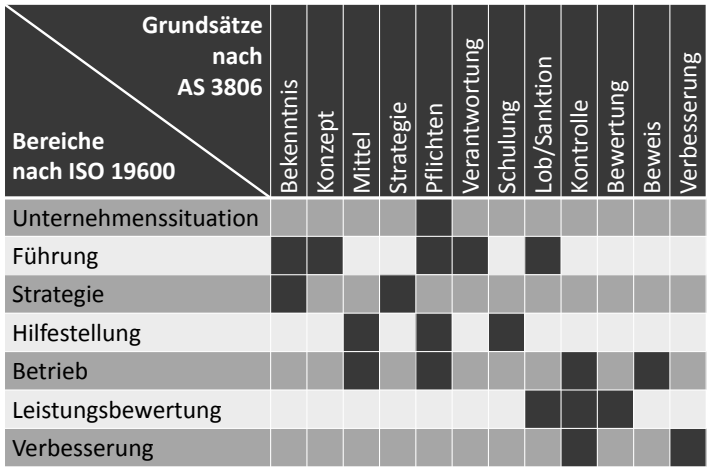


Abbildung 4:
IDW PS 980 ./. ISO 19600

Das Standards Australia Committee hat 12 Grundsätze für die Entwicklung, die Umsetzung und Weiterführung eines wirksamen Compliance-Programms sowohl innerhalb öffentlicher als auch kommerzieller Organisationen definiert. Diese Grundsätze sollen die Organisationen dabei unterstützen, mögliche Unzulänglichkeiten bei der Befolgung anwendbarer Gesetze, Regeln und Vorschriften festzustellen und zu beseitigen und Vorgehensweisen zu entwickeln, die auf diesem Gebiet kontinuierliche Verbesserungen ermöglichen. Der ISO-Standard hat das Modell der Grundsätze nicht übernommen und sich für eine Gliederung in funktionale Bereiche entschieden. Trotz dieser strukturellen Unterschiede bleibt der Stil beider Normierungswerke sehr ähnlich.

Abbildung 3:
AS 3806 ./. ISO 19600



4.4 IDW PS 980

Das Deutsche Institut der Wirtschaftsprüfer hat 2011 den Prüfungsstandard IDW PS 980 für Compliance-Management-Systeme veröffentlicht. Dieser Standard ist ein Prüfungsstandard, der auch Hinweise für Mindestanforderungen an wirksame Compliance-Management-Systeme als Audit-Grundlage beinhaltet. Diese Mindestanforderungen – wie überhaupt die Prüfungsanforderungen als solche – wurden von zahlreichen Compliance-Standards (u. a. AS 3806-2006, US-FSGO 2010 sowie der Guidance zum UK Bribery Act 2010) abgeleitet. Der Prüfungsstandard geht von sieben Elementen aus: Compliance-Ziele, -Risiken, -Programm, -Organisation, -Kommunikation, -Überwachung und -Kultur.[1]

Ein Vergleich zwischen dem neuen ISO-Standard 19600 und dem gar nicht so alten IDW Prüfungsstandard 980 ist spannend. Zunächst fällt die Verwirrung zwischen den unterschiedlichen Begriffswelten auf. Jeder Compliance-Ansatz arbeitet mit seiner eigenen Begriffswelt. Eine intensive Begriffsklärung ist insbesondere dann erforderlich, wenn der ISO-Standard als Rahmenkonzept zur Grundlage einer IDW PS 980 Prüfung genommen werden soll.

Es treffen offensichtlich unterschiedliche Welten zusammen: Im IDW-Standard die Welt des betriebswirtschaftlichen Risikomanagements sowie der Wirtschaftsprüfer und im ISO-Standard die Welt des technisch geprägten Qualitätsmanagement. Eine Welt ist daran interessiert, Compliance in die Prozesse und Prozeduren der Unternehmen einfließen zu lassen. Die andere Welt versucht eine zusammenfassende Gesamtschau aus der Perspektive der Geschäftsleitung sowie des Aufsichtsrates. Keinesfalls soll das aber bedeuten, dass im Unternehmensdampfer der ISO-Standard den Maschinenraum bedient, während der IDW-Standard allein auf der Brücke gilt.

5. Kritik

Der ISO Standard 19600 ist sehr detailreich. Der Leitfaden spricht viele Themen an, spart nicht an Informationen (sowie deren häufige Wiederholung) und führt das eine oder andere durch Beispiele aus. Das ist hilfreich! Was dem Compliance-Verantwortlichen im Unternehmen bei der Konzeption, Umsetzung, Bewertung und Verbesserung eines CMS aber hilft, gibt dem Prüfer – sei es ein QM-Zertifizierer, ein Wirtschaftsprüfer aber auch eine nationale Ordnungsbehörde oder ein Gericht – auch eine Checkliste für nahezu unbegrenzte Anforderungen. Es gelingt leider nicht darzustellen, in welchen Bereichen ein Mittelständler Empfehlungen des Leitfadens auf für ihn erträgliche Anforderungen reduzieren kann. Damit können hilfreiche Detailinformationen sich als Last herausstellen. Es wird in der Anwendung des ISO-Standards nicht nur eine Herausforderung sein, dem Ideal des Leitfadens nahe zu kommen, sondern auch, seine Anforderungen zu relativieren und gegebenenfalls wegzudiskutieren.

1 Vgl. Schefold, C.: Compliance-Management-Systeme nach deutschem Standard, in: ZRFC 5/11, S. 221 ff.

ISO lässt wichtige Themen internationaler Compliance leider unbeachtet.

Mit dem Leitfaden für die CMS-Gestaltung ist eine neue ISO-Dimension eröffnet, die über den der erfolgreichen Standards für Qualitätsmanagement (QM) hinausgeht. Qualitätsmanagement beeinflusst unmittelbar die Eigenschaft von Produkten und Dienstleistungen eines Unternehmens und damit auch die Akzeptanz auf internationalen Märkten. Nach der Ebene der Produktnormierungen konnten Standardisierungen für die Konzeption von Produktionsverfahren eine zweite Dimension der Nachhaltigkeit von Produkteigenschaft insbesondere für Massenprodukte eröffnen. Wie eingangs dargestellt, hat Compliance aber Auswirkungen in einer weiteren Dimension: Auch Unternehmen von zweifelhafter Integrität können durchaus Massenqualitätsware oder -dienstleistungen herstellen. Compliance eröffnet eine ethische Dimension mit Konsequenzen für internationale Wirtschaftsbeziehungen, indem auf den Integritätskontext der Unternehmen abgestellt wird. Hier aber gibt ISO nur eine Hilfestellung für die Konzeption eines Managementsystems.

Internationale Herausforderungen, wie etwa die Kunst, in einem global agierenden Mittelstandsunternehmen eine einheitliche Compliance-Kultur unter Berücksichtigung unterschiedlichste Rechts- und Gesellschaftskulturen zu etablieren, werden nicht angesprochen. Wer Methoden sucht, um einen „conflict of laws“ oder gar „clash of cultures“ erfolgreich zu lösen, wird bei der Lektüre von ISO 19600 enttäuscht werden. Es fehlt dieser internationale Bezug und damit das Angebot einer Lösung für die unzweifelhaft bestehende dritte Dimension der Integrität im internationalen Wirtschaftsverkehr. Eine weiteres Standardthema von Compliance im internationalen Kontext fehlt ebenfalls: Der Umgang mit Geschäftspartnern in anderen Ländern und Kulturen. Vermutlich werden die Autoren des Standards auf die Existenz der ISO-Norm 19600 selbst hinweisen und behaupten, dass ähnlich der QM-Standards ein Nachweis über deren Einhaltung hier weiterhelfen kann. Im Leitfaden fehlen aber schon allein Empfehlungen für den Umgang mit Geschäftspartnern, etwa Anhaltspunkte für eine Integritätsbeurteilung. Diese Thematik hätte einen eigenen funktionalen Bereich des ISO 19600 gerechtfertigt.

Der ISO-Standard öffnet sich zudem sehr weit selbst gegenüber gesellschaftlichen Erwartungen an Unternehmen. Es besteht die Gefahr, dass damit das Thema Compliance und auch ein CMS gewaltig überfordert werden. Zudem kann die Berücksichtigung gesellschaftlicher Erwartungen den Grundzielen der ISO entgegenwirken: Nicht überall stehen gesellschaftliche Erwartungen anderen Kulturen oder gar dem Freihandel offen gegenüber.

Der ISO-Standard spricht eines deutlich aus: Ein Compliance-Management-System dient primär dem Nachweis der Compliance-Kultur insbesondere gegenüber nationalen Behörden und Gerichten. Der Leitfaden kann Grundlage behördlicher und auch gerichtlicher Entscheidung über Sanktionen sein. Pflichtgemäß enthält der Text zwar auch einen Appell an den Nutzen von Compliance und Integrität für wirtschaftliche Chancen und Nachhaltigkeit – im Hinblick auf die bereits im Vorwort formulierte explizite Zielrichtung, geht dieser Apell aber verloren. Noch weit gravierender sind einzelne unreflektierte Bezüge zur Rechtswirklichkeit in vielen Ländern: Wie können die Anforderungen der Dokumentation und Compliance-Leistungsmessung mit Arbeitsrecht und Arbeitnehmerdatenschutz in Einklang gebracht werden? Ein ständiger offener Kontakt zu Behörden sowie allgemeine Hinweissysteme sind eine der geforderten Informationsquellen für ein ISO 19600 CMS; wie können dabei Verfahrensrechte der Betroffenen und auch der Unternehmen selbst gewahrt werden?

Nach den vielversprechenden Ankündigungen zum ISO-Standard 19600 haben die ersten Eindrücke enttäuscht. Der Leitfaden fasst bereits bekanntes Grundlagenwissen zusammen und ergänzt dies detailreich mit Einzelaspekten, die auch als Checklisten dienen können. Die Rolle und Möglichkeiten der ISO als internationale Nichtregierungsorganisation zur Förderung des internationalen Wirtschaftsaustausches wurden nicht genutzt und auch nicht reflektiert. Hier hätten sich Ansatzpunkte für wirklich innovative Hilfestellungen an global agierende Unternehmen eröffnen können. Das Agieren in internationalen Einheiten und mit ausländischen Geschäftspartnern bleibt weiterhin eine Herausforderung, die Unternehmen für sich selbst lösen müssen.