05.15

10 Jahre ZRFC

ZRFC

Risk, Fraud & Compliance

10. Jahrgang
Oktober 2015
Seiten 193 – 240

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

ESV ERICH SCHMIDT VERLAG

64683

Keywords:
ISO 19600
Zertifizierung
Compliance-Management-Systeme
Risk-Management
Compliance-Kultur

ISO 19600

Der neue Standard zur Zertifizierung von Compliance-Management-Systemen

Prof. Dr. Peter Fissenewert*

Kaum ein anderes Thema hat die Wirtschaft in den vergangenen Jahren so beschäftigt wie Compliance. Noch unbekannt vor wenigen Jahren, hat sich über eine Gereiztheit zum Thema, über ein Wegschauen eine völlig neue Diskussion und Entwicklung ergeben. Auch scheinen die Diskussionen um den Umfang und die Definition zu Compliance noch nicht abgeschlossen, da liegt plötzlich eine ISO Norm vor, die ISO 19600 – und zwar als internationaler Standard.[1]

1. Hintergrund der internationalen Standardisierung

Zwar gab es in der Vergangenheit erhebliche, gute Bemühungen um eine Standardisierung. Hier sticht sicherlich IDW PS 980 hervor.[2] International verlässlich waren diese Standardisierungsversuche bislang nicht. Das ist jetzt anders. ISO 19600 ist inhaltlich aufgeräumt, übersichtlich und verständlich und arbeitet nach dem Prinzip der fortlaufenden Verbesserung. Das Verfahren stammt aus dem Qualitätsmanagement.

Fast möchte man die Entwicklung einen Kulturwandel in der Gesellschaft nennen.

So existiert zwar die Managerhaftung seit Jahrzenten, praktiziert wurde sie aber bis vor wenigen Jahren eigentlich nicht. Das Schlimmste, was einem Manager in der Vergangenheit aufgrund eines vorwerfbaren Fehlverhaltens passieren konnte, war der Verlust des Arbeitsplatzes – mehr nicht, und dies auch noch häufig einhergehend mit enormen Abfindungszahlungen an den Manager. Heute ist es auch in Deutschland völlig normal, dass Manager und mittlerweile auch deren Aufsichtsräte für ihre Schäden einstehen müssen. Die Diskussion um ein Unternehmensstrafrecht zeigt, dass nunmehr auch die Unternehmen und nicht nur einzelne, handelnde Personen in den Fokus der Gesetzgebung und Rechtsprechung gelangt sind. Nicht zuletzt ist auch das Thema Reputation – positiv wie negativ – zu einem wesentlichen Teil von Compliance-Überlegungen geworden. Kaum jemand mehr lehnt Compliance ab. Die börsennotierten Unternehmen haben sämtlich mehr oder weniger gut funktionierende Compliance-Management-Systeme, im Wesentlichen aber ohne einheitlichen, internationalen Zertifizierungsstandard.

Prof. Dr.
Peter Fissenewert

Mit ISO 19600 sollen die Standards im Compliance-Management internationalisiert werden – und zwar weltweit. Als grenz- und branchenübergreifendes Regelwerk soll die Norm für international einheitliche Rahmenbedingungen bei der Einrichtung und Implementierung von Compliance-Management-Systemen in verschiedensten Organisationstypen sorgen. Der lediglich 33 Seiten umfassende Standard basiert auf den Prinzipien guter Unternehmensführung, Verhältnismäßigkeit, Transparenz und Nachhaltigkeit und legt Wert auf eine höchst flexible Anwendung.

Der Leitfaden des ISO 19600 verfolgt das generell von ISO-Normen angestrebte Ziel, ein effizienteres Wirtschaften zu ermöglichen.[3]

ISO 19600 verfolgt einen risikobasierten Ansatz. Zugleich steht im Mittelpunkt des Leitfadens die Compliance-Kultur. Die Norm ist auch bestens für den Mittelstand geeignet, wie weiter unten ausgeführt wird.

2. Chronik der Entwicklung des ISO 19600 Compliance-Management-Systems

Von der Initiative bis zur Veröffentlichung der Norm am 05. Dezember 2014 verstrichen mehrere Jahre, vom Vorschlag über die Bearbeitung, den Komitee-Entwurf, der Umfragestufe bis zur Annahmestufe.

Der Norm lagen die Organisationsprozesse (NAOrg 175-00-01 AA) sowie Compliance-Management-Systems (ISO/PC 271 und 278) zugrunde.

Im vorliegenden Fall wurden ca. zwei Jahre in Anspruch genommen.

Juni 2012

Australien ergreift die Initiative und schlägt einen Entwurf für eine ISO-Norm für Compliance Programme vor. Als Vorbild orientiert sich der Entwurf an der australischen Norm AS 3806-2006.

* Prof. Dr. Peter Fissenewert ist Rechtsanwalt und Partner der Kanzlei hww hermann wienberg wilhelm. 2005 erhielt er eine Professur für Wirtschaftsrecht. Seine Tätigkeitsschwerpunkte sind das Gesellschaftsrecht, Restrukturierung, Sanierung und Insolvenz sowie Compliance-Beratung und Managerhaftung. Er zählt zu den führenden Beratern und Autoren in diesem Bereich und nimmt regelmäßig als Redner an hochkarätigen Fachveranstaltungen teil. Peter Fissenewert ist Herausgeber des Handbuchs „Compliance für den Mittelstand" und des „Praxishandbuchs internationale Compliance-Management-Systeme Grundsätze – Checklisten – Zertifizierung gemäß ISO 19600". Darüber hinaus ist er Mitautor des Standardwerks „Compliance kompakt". Kontakt: Peter.Fissenewert@hww.eu

1 Ausführlich zu ISO 19600: Fissenewert, P.: Praxishandbuch Internationale Compliance-Management-Systeme Grundsätze – Checklisten – Zertifizierung gemäß ISO 19600, Erich Schmidt Verlag 2015.

2 Zum Vergleich von IDW PS 980 mit ISO 19600 siehe Withus, K.-H./Kunz. J.: Auswirkungen des neuen ISO 19600: 2014 zu Compliance-Management-Systemen auf die Prüfung nach IDW PS 980, BB 2015, S. 685 ff.

3 Ausführlich zum betriebswirtschaftlichen Nutzen Makowicz, B./Wüstermann, S.: Betriebswirtschaftlicher und juristischer Nutzen der Ausgestaltung von Compliance-Management-Systemen nach dem globalen Leitfaden ISO 19600, BB 2015, S. 1195 ff.

Unterschiedliche Rechtskulturen haben sich bei ISO 19600 auf einen umsetzbaren Kompromiss geeinigt.

Der Vorschlag der Australier basierte auf der ebenfalls australischen Norm AS 3806 aus dem Jahr 2006. Nachdem der neue Normvorschlag von den ISO-Mitgliedern mehrheitlich angenommen wurde, richtete die Organisation ein Entwurfskomitee mit dem Namen ISO/PC 271 ein. Fachexperten aus elf Ländern, darunter auch Deutschland, waren fortan mit der Erarbeitung der Norm befasst, unter Mitwirkung weiterer 20 Länder mit Beobachterstatus.

Hier werden bereits wesentliche Grundelemente der ISO 19600 vorgeschlagen. Compliance wird hier als Kernelement guter und sorgfältiger Unternehmensführung gesehen, die das Verhalten der Organisation unter Berücksichtigung der sozialen Verantwortung sieht.

Erstmals wird auch nicht nur die Beachtung des geltenden Rechts gefordert, sondern auch der ethischen Werte, Standards, Normen oder Erwartungen einer Gesellschaft.

Deutschland lehnt den Entwurf zunächst ab. Kritisiert werden insbesondere mangelnder Nutzen der Norm, unklare Zwecksetzung sowie Konflikte mit anderen existierenden Compliance-Standards, wie z. B. ICC und OECD. Im Übrigen wird kein Bedarf gesehen.

Oktober 2012

ISO-Mitglieder nehmen den Vorschlag mehrheitlich an. Bei ISO wird ein Entwurfskomitee Nr. 271 (ISO/PC 271) eingerichtet, das sich unter australischer Leitung mit der Erarbeitung der Norm befassen sollte.

Februar 2013

Deutschland beantragt offiziell die Mitgliedschaft im ISO/PC 271 und wird als teilnehmendes Mitglied aufgenommen. Für die deutsche ISO-Kommission waren mögliche Konflikte mit bestehenden Initiativen, wie etwa den Compliance-Richtlinien der OECD und des ICC Anlass, erst 2013 die aktive Mitarbeit an der Gestaltung der neuen ISO-Norm aufzunehmen, nachdem die Australier bereits im Juni 2012 eine entsprechende Initiative ergriffen und einen entsprechenden Entwurf eingebracht hatte.

April 2013

Die erste globale Sitzung des ISO/PC 271 findet in Sydney statt. Es werden große Arbeitsfortschritte erzielt, die zur Erarbeitung des Komitee-Entwurfs führen, ab jetzt heißt der Entwurf: ISO/CD 19600.

Juni 2013

Beim DIN wird der Arbeitskreis zur Spiegelung der Arbeiten im ISO/PC 271 eingerichtet. Nach ausführlicher Analyse reicht der Arbeitskreis rund 100 Kommentare, Anmerkungen und Änderungsvorschläge ein.

Oktober 2013

Die zweite globale Sitzung des ISO/PC 271 findet unter erstmaliger Beteiligung der deutschen Delegation in Paris statt. Es werden rund 400 Kommentare behandelt, darunter allein 100 aus Deutschland. Nahezu alle Kommentare der deutschen Delegation werden angenommen. Die nächste Stufe, der internationale Entwurf (DIS), wird erreicht. Der Entwurf heißt nunmehr ISO/DIS 19600.

Juli 2014

Nach einer weiteren Kommentierungsrunde findet die dritte und letzte globale Sitzung in Wien statt. Da nur geringe Änderungen eingeführt werden und alle einverstanden sind, wird die letzte finale Stufe (FDIS) übersprungen und die Veröffentlichung der Norm beschlossen.

September 2014

ISO 19600 Compliance-Management-Systems wird in finaler Fassung zur Veröffentlichung weitergeleitet.

Dezember 2014

Veröffentlichung der finalen Fassung. 50 Klauseln finden sich auf insgesamt 33 Seiten.

Der Leitfaden hat umfassende und universelle Geltung („organizations“) und zeigt sich außerordentlichen flexibel hinsichtlich der Handhabung.

3. Die Grundsätze von ISO 19600

Unterschiedliche Rechtskulturen aus den verschiedensten Ländern der Welt, wie Australien, Singapur, Malaysia, Deutschland, Österreich, Niederlande, Frankreich bis hin zu Kanada haben sich hier auf einen umsetzbaren Kompromiss geeinigt. Es ist ja eben auch die Internationalität, die Compliance-Verpflichtungen ausmacht und auslöst. Dieser Internationalität ist auch eine etwas verwirrende Begrifflichkeit geschuldet, die teilweise dem deutschen Rechtswesen fremd ist. So richten sich alle Hinweise oder Empfehlungen ausschließlich oder gemeinsam an das Unternehmen (The Organization) und an einzelne Unternehmenshierarchien wie The Governing Body, Topmanagement, Topmanagement and all other Levels of Management, Management oder The Governing Body, Management and all Employees. Die Aufgabenwahrnehmung durch The Governing Body und das Topmanage-

Der Standard erklärt, wie CMS etabliert, entwickelt, umgesetzt, evaluiert und verbessert werden könnte.

ment folgt eher dem angelsächsischen One Board System, die der klaren Aufgabenteilung zwischen Aufsichtsrat und Vorstand einer deutschen Aktiengesellschaft fremd ist. Auch wird verschiedentlich der Governing Body als Adressat gemeinsam mit dem Topmanagement, dann aber auch mit dem Management und Dritten genannt. Vor diesem Hintergrund ist das Management für deutsche Unternehmen als Sammelbegriff für alle Managementhierarchien zu verstehen, einschließlich des Topmanagements, auch wenn es nicht ausdrücklich genannt ist.[4]

ISO 19600 ist eine sogenannte B-Norm. Sie gibt im Wesentlichen lediglich Empfehlungen (should). Diese Empfehlungen sind hilfreich. Ist eine Zertifizierung gewünscht, sollte aus dem „should" ein „must" werden.

Es sind bereits verschiedene Zertifizierungsangebote im deutschsprachigen Raum auf dem Markt, unter anderem von Austrian Standards als nationaler Normungsorganisation in Österreich oder von Wirtschaftsprüfungsgesellschaften im Zusammenhang mit einer Prüfung nach IDW PS 980.[5]

Der Standard versucht zu erklären, wie Compliance-Management-Systeme (CMS) in einer Organisation eingerichtet, entwickelt, umgesetzt, evaluiert, aufrechterhalten und verbessert werden können. Die Norm stellt ab auf Organisation und bringt damit eine sinnvolle Neuerung ein. Die Norm ist nicht ausschließlich auf große Unternehmen zugeschnitten, sondern definiert Empfehlungen für ein CMS, die von möglichst vielen Organisationstypen genutzt werden können. Hierzu zählen kleine bis große Unternehmen, aber auch Stiftungen, Verbände, Behörden und weitere Organisationen, gleich, ob sie privat oder öffentlich sind. Compliance quasi von A bis Z, von Aalräuchereien bis zum Zoobetrieb.

Berücksichtigt werden nicht nur Internationalität und Organisation, sondern auch Größe des Unternehmens, mithin auch der Mittelstand, indem in verschiedenen Klauseln der eindeutige Hinweis aufgenommen wurde, dass Anwendungsweite der Norm von der Größe, der Struktur und Komplexität einer Organisation abhängig ist. Compliance ist wie ein maßgeschneiderter, auf die Größe und Individualität des Unternehmens angepasster Maßanzug.[6]

Die Norm enthält darüber hinaus Empfehlungen, die Prinzipien von Good Governance, also den Grundsätzen guter Unternehmensführung, Verhältnismäßigkeiten, Transparenz und Nachhaltigkeit zu beachten. Dabei berücksichtigt ISO 19600 Wertekulturen und meint nicht nur Compliance-Verpflichtungen, die eine Organisation erfüllen muss, sondern auch solche, die sie erfüllen möchte, worunter auch die sozialen und ethischen Werte einer Gesellschaft fallen.

Good Governance findet sich in der Ziffer 4.4 der Norm und meint den Direktzugang zur Unternehmensleitung, die völlige Unabhängigkeit sowie die Zuweisung angemessener Befugnisse und Ressourcen.

Der Grundsatz der Flexibilität wird bereits im Geltungsbereich herausgestellt, ebenso wie die Organisation, Größe, Struktur und Komplexität des Unternehmens.

CMS sollte verhältnismäßig sein, das heißt Prozesse, Strukturen und Maßnahmen sollten in einem angemessenen Verhältnis zu den Zielen stehen und nicht übermäßig sein.

Der Grundsatz der Transparenz ergibt zugleich den Vorteil der Strukturen, nämlich Akzeptanz (höhere Bereitschaft der Mitglieder), Kontrolle sowie Außenverhältnis (Transparenz fördert Vertrauen).

Nachhaltigkeit ist ein weiterer Grundsatz der CMS-Ausgestaltung. CMS ist keine punktuelle Maßnahme, sondern ein fortlaufender Prozesse, gewährleistet durch die anhaltende Einbettung in die Organisationsstruktur und in das Bewusstsein ihrer Mitglieder.

Die einheitliche Gestaltung von CMS wird zu mehr Transparenz und Übersichtlichkeit insbesondere im Verhältnis zu ausländischen Geschäftspartnern, aber auch auf der nationalen Ebene beim Umgang mit Lieferanten führen und darüber hinaus unternehmensintern.

ISO 19600 beschreibt zunächst den Geltungsbereich und kommt über (nicht vorhandene) normative Verweise, Begriffe und Definitionen zum Kontext des Unternehmens, definiert Leitung, organisatorische Aufgaben, Verantwortlichkeiten und Befugnisse, Planung, Support, Arbeitsablauf, Leistungsbewertung, Managementauswertung und Verbesserung.

Das Normierungsgremium arbeitete mit der sogenannten Klammertechnik. Die definierten Grundsätze von CMS sollen bei allen weiteren Bestimmungen gelten.

Die Norm legt in logischer Abfolge dar, wie ein Compliance-Management-System funktionieren könnte. Dabei kommt der Risikoanalyse eine besondere Stellung zu. Um Compliance-Anforderungen bestimmen und kontrollieren zu können, werden Risiken identifiziert, analysiert und bewertet. Gewichtet nach Prioritäten sollen Gegenmaßnahmen gegen die größten Com-

4 Insoweit zutreffend Sünner, E.: Von der Sorge für gesetzeskonformes Verhalten – Zugleich eine Besprechung des ISO-Entwurfs 19600, CCZ 2015, S. 2 (3).

5 Ehnert, M.: Standardisierung mit Variablen – Compliance-Standards ISO 19600 und ISO 37001 – CCZ 2015, S. 6.

6 So auch Makowicz, B.: Grundsätze der Compliance, 1–10, S. 4 in Makowicz, B./ Wolffgang, H.: Rechtsmanagement im Unternehmen.

ISO 19600 ist ein offener und flexibler Standard in einem normierten Kontext.

pliance-Risiken ergriffen werden. Erheblicher Wert wird auch auf Kommunikation, Wertevermittlung und Kultur sowie die Effektivitätsbewertung sowie die laufende Prozessverbesserung gelegt. ISO 19600 widmet sich ferner den Rollen und Verantwortlichkeiten des Managements und der Mitarbeiter. Einen besonderen Stellenwert hat hier der Compliance-Officer und die Definition von Compliance: Gemäß ISO 19600 wird Compliance als die Erfüllung aller Compliance-Verpflichtungen eines Unternehmens verstanden. Compliance-Verpflichtungen sind gesetzlich verpflichtende oder freiwillige Verpflichtungen, also unternehmensspezifische sowie branchenspezifische Verpflichtungen. Die bereits erwähnten Compliance-Risiken werden als der Effekt der Unsicherheit in Bezug auf die Erreichung der Compliance-Ziele verstanden.

Die Compliance-Kultur ist entscheidend für den Erfolg eines funktionierenden Compliance-Managements. Compliance wird dann idealerweise als Standard für alle Mitarbeiter auf allen Unternehmensebenen verstanden. Mitarbeiter sollen sich nach ISO 19600 in jeder erdenklichen Unternehmenssituation compliant verhalten.

4. ISO 19600 – Ein offener und flexibler Standard in einem normierten Kontext

Der Begriff der Norm – wie auch bei ISO 19600 – lässt nicht unmittelbar auf Flexibilität schließen. Wie verträgt sich also Flexibilität mit Normen, die per se als starr gekennzeichnet sind? ISO steht für International Standard Organization. Die ISO ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik und der Elektronik, für die internationale elektrotechnische Kommission (IEC) zuständig ist, und mit Ausnahme der Telekommunikation, für die internationale Fernmeldeunion (ITU) zuständig ist. Sie ist quasi die internationale Ausgabe der DIN.

Standards bzw. Normen sind in der Gesellschaft oder in bestimmten Teilbereichen verbindlich anerkannte Regel oder Norm. „Ein Standard ist ein öffentlich zugängliches technisches Dokument, das unter Beteiligung aller interessierter Parteien entwickelt wird und deren Zustimmung findet. Der Standard beruht auf Ergebnissen aus Wissenschaft und Technik und zielt darauf ab, das Gemeinwohl zu fördern.“[7]

ISO 19600 ist alles andere als eine starre Norm. Sie hat einen sehr innovativen Ansatz, Übersichtlichkeit, klare Definitionen und einen weiteren Anwendungsbereich. Damit hat die Norm ein erhebliches Potenzial, zum weltweit einheitlichen meist genutzten CMS-Leitfaden zu werden.

Die neue Norm erhebt den Anspruch, universell auf möglichst viele Organisationstypen anwendbar zu sein. Damit werden nicht nur private Unternehmen erfasst, sondern auch Behörden, Vereine, Verbände und sonstige Organisationsformen.

4.1 High Level Structure

Bei aller gewollten und versuchten Flexibilität ist natürlich auch ISO 19600 Regeln unterworfen. Die Norm 19600 gehört in den Bereich der Management-Systeme, für den die ISO selbst einheitliche Strukturen vorgegeben hat. Die ISO/IEC-Direktiven ergeben eine sogenannte High Level Structure mit identischen Textbausteinen, gemeinsamen Begriffen und Definitionen vor. Sie soll, wenn immer möglich, den Kern von neuen und überarbeiteten Management-System-Normen bilden. Organisationen, die mehrere Management-Systeme (z. B. QMS, UMS, ISMS) gleichzeitig einführen, können diese besser integrieren und umsetzen. Die Regeln zur High Level Structure und die Textbausteine sind als öffentliche Informationen zugänglich.[8]

Die High Level Structure[9] umfasst die folgenden Stufen:

1. Scope (Anwendungsbereich)
2. Normative Reference (Normative Verweisungen)
3. Terms and Definitions (Begriffe und Definitionen)
4. Context of the Organization (Kontext der Organisation)
5. Leadership (Führung, Verantwortung der Leitung)
6. Planning (Planung)
7. Support (Unterstützung)
8. Operation [Betrieb (Produktion/Fertigung/Dienstleistungen)]
9. Performance Evaluation (Leistungsbewertung)
10. Improvement (Verbesserung)

Die Struktur von ISO 19600 war also von den Management-Normen vorgegeben, auch wenn in vielen Fällen später davon abgewichen wurde.

4.2 PDCA-Modell

ISO 19600 basiert zugleich auf dem sogenannten PDCA-Modell (Plan>Do>Check>Act).[10] Der PDCA-Zyklus als Sys-

7 Abrufbar unter www.bsi-global.com/en/Standards-and-Publications/About-standards/what-is-a-standard/ (Stand: 31.08.2015).

8 Abrufbar unter http://www.iso.org/iso/standards_development/processes_and_procedures/iso_iec_directives_and_iso_supplement.htm (Stand: 31.08.2015).

9 Anmerkung: Für die meisten Begriffe gibt es noch keine offiziellen deutschen Übersetzungen.

10 Sogenannter Deming-Kreis, benannt nach William Edwards Deming.

Die Verwaltung von Compliance-Risiken steht im Fokus des CMS nach ISO 19600.

tematik zur kontinuierlichen Verbesserung basiert auf dem Prinzip Gemba: „Gehe an den Ort des Geschehens“ und stellt vor allem die Mitarbeiter vor Ort mit ihrer exakten Kenntnis der Situation am Arbeitsplatz in den Mittelpunkt der Planung.

Der PDCA-Zyklus besteht aus vier Elementen:

- **Plan**: Der jeweilige Prozess muss vor seiner eigentlichen Umsetzung geplant werden. Dabei umfasst Plan das Erkennen von Verbesserungspotenzialen, die Analyse des Ist-Zustandes sowie die Entwicklung eines neuen Konzeptes.
- **Do**: Do bedeutet nicht das eigentliche „Tun“, sondern Ausprobieren bzw. Testen und praktische Optimieren des Konzepts mit schnell realisierbaren, einfachen Mitteln an einem einzelnen Arbeitsplatz.
- **Check**: Check bedeutet die Überprüfung der im kleinen realisierten Prozessabläufe und seiner Resultate und bei Erfolg die Freigabe für die Umsetzung auf breiter Front als Standard.
- **Act**: In der Phase Act wird der neue Standard auf breiter Front eingeführt, festgeschrieben und regelmäßig auf Einhaltung im Rahmen von Audits überprüft.

Das ISO 19600 zugrundeliegende Modell enthält im Wesentlichen zwei Phasen: Die Frühphase, welche im Einrichten des Systems besteht und die Spätphase, welche im Betrieb des Systems besteht. In der ersten Phase werden Ziele und Anwendungsbereiche des Compliance-Management-Systems im Unternehmen festgelegt, wobei die Prinzipien von Good Governance und Interessen aller Beteiligten zu berücksichtigen sind. Auf dieser Basis wird die Compliance-Policy im Unternehmen definiert. Die Schnittstelle zur zweiten Phase stellt der risikobasierte Ansatz dar, welcher die Compliance-Risiken und -Verpflichtungen identifizieren soll. Im Mittelpunkt des weiteren Prozesses stehen dann die Zuweisung von Zuständigkeiten sowie die Errichtung der CMS-Leitung und sonstiger fördernder Funktionen. Das ist eben die Entwicklung (Development), Umsetzung (Implementation), Evaluierung (Evaluation) und Aufrechterhaltung (Maintenance) des CMS, also der Basis des PDCA-Zyklus.

5. Der risikobasierte Ansatz von ISO 19600

ISO 19600 folgt zugleich einem risikobasierten Ansatz. Die Verwaltung von Compliance-Risiken steht im Fokus des CMS nach ISO 19600.

Nachdem Compliance lange Zeit ein Schattendasein im Risiko-Management von Unternehmen führte,[11] sind nunmehr Compliance und Risk-Management untrennbar miteinander verwoben.

ISO 19600 verweist wiederum auf den bereits vorhandenen Standard des Risk-Managements nach ISO 31000.

ISO 31000 bietet eine systematische Herangehensweise zum Risikomanagement, die sich sowohl für große wie auch für kleine und mittlere Unternehmen eignet.

Eine systematische Risikoanalyse liefert Unternehmen in jedem Fall sehr wertvolle Hinweise auf sich ändernd Rahmenbedingungen. Das systematische Risikomanagement erfordert:

- eine verantwortliche Person (dies kann die Unternehmensleitung selbst oder ein benannter Mitarbeiter sein);
- eine klar definierte Reihenfolge:
  1. Risikoidentifikation, das heißt möglichst vollständige, auf aktuelle Informationen beruhende Risikoerkennung;
  2. Risikobewertung (Wahrscheinlichkeit des Eintritts eines Risikos multipliziert mit dem potenziellen Schaden bei Eintritt);
  3. Risikobehandlung (Vermeidung, Verminderung, Begrenzung, Überwälzung auch mittels Versicherungen und Risikoübernahme);
- jeweils ggf. unterstützt durch einen moderierten Prozess mit entsprechenden Experten, die hinreichend sensibel für die Erkennung möglicher zukünftiger Krisen sind;
- Dokumentation der in diesem Prozess identifizierten Risiken sowie der Begründung der Auswahl einer speziellen Risikobehandlung;
- kontinuierliche Identifizierung und Beurteilung der Risiken.

Im Fokus des Compliance-Managements nach ISO 19600 steht die Verwaltung von Compliance-Risiken. Wer sich heute mit den Fragen rund um das Risikomanagement befasst, kommt an einer weiter Norm nicht vorbei: ISO 31000. Es handelt sich dabei um einen Standard, der aufzeigt, was internationale Experten unter Risikomanagement und seiner Anwendung in Organisationen verschiedenster Art verstehen. Ein internationaler Standard stellt – ebenso wie ISO 19600 – einen breit abgestützten Konsens unter maßgebenden Fachexperten dar, wie man mit einem bestimmten Problem heute umgehen soll. Es handelt sich um allgemein anerkannte Praktiken, sogenannte Best Practices.

Risikomanagement beinhaltet Prozesse und Verhaltensweisen, die darauf ausgerichtet sind, eine Organisation bezüglich Risiken zu steuern. Risikomanagement ist eine Führungsaufgabe. Die Leitung einer Organisation ist bewusst, dass sie stets unter Unsicherheit planen, entscheiden, handeln und korrigierend eingreifen muss. Das Risikomanagement ist zentrales Element jeder Führungstätigkeit. Je besser ein Management die Unsicherheiten zu erkennen vermag und mit ihnen umgehen kann, umso stabiler und verlässlicher sind die Ergebnisse. Risikoma-

11 Grüninger, S.: Werteorientiertes Compliance-Management-System, in Handbuch Compliance-Management, S. 55.

Im Mittelpunkt der Norm steht die Compliance-Kultur.

nagement soll zufällige Schwankungen, die eine Organisation schwer treffen bzw. ihre Ziele beeinträchtigen können, vermindern, besonders, wenn sie negativ und schwerwiegend ausfallen.

Risikomanagement ist in Deutschland Aufgabe des Vorstands und der Geschäftsführer.

Die Aufgabe des Aufsichtsratsvorsitzenden besteht darin, mit dem Vorstand die Strategie, die Geschäftsentwicklung, die Risikolage, das Risikomanagement und die Compliance des Unternehmens zu beraten. Überdies soll der Aufsichtsrat einen Prüfungsausschuss (AuditCommittee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung, des internen Kontrollsystems, des Risikomanagements oder auch der Compliance befasst.

Bei jeder unternehmerischen Entscheidung ergeben sich zwangsläufig Risiken, die häufig unbedeutend, manchmal aber auch existenzbedrohend sein können. Einige Risiken haben kurzfristige Auswirkungen, anderen erst nach langer Zeit. Risiken können im Unternehmen selbst begründet oder durch Wettbewerb, technologische Neuerungen oder veränderte gesetzliche Grundlagen extern bedingt sein

6. Compliance-Kultur nach ISO 19600

Im Mittelpunkt der Norm steht die Compliance-Kultur. Die Compliance-Kultur wird von ISO 19600 definiert als Werte, Ethik und Glaubensinhalte, die in der gesamten Organisation existieren und mit den Strukturen und Kontrollsystemen des Unternehmens interagieren, um Verhaltensnormen zu erzeugen, die für Compliance-Erfolge förderlich sind.

Die Norm befasst sich an vielen Stellen mit dem Thema Kultur. So wird dies beim Tone from the Top[12] ebenso berücksichtigt wie beim Ziel des Compliance-Trainings[13] und der Sensibilisierung der Organisationsmitglieder[14] sowie bei der Compliance-Überwachung.[15]

Ohne Unternehmenskultur funktioniert Compliance nicht. Die Unternehmenskultur beschreibt die Grundeinstellung und Verhaltensweisen des Managements. Eine gute Compliance-Kultur herrscht dann, wenn Management und Mitarbeiter verinnerlicht haben, dass rechtliche und moralische Standards eingehalten werden müssen. Dabei spielen auch die Aufsichtsorgane eine besondere Rolle. Nur wenn beide Institutionen, Geschäftsführung und Aufsichtsorgane, die Wichtigkeit und Relevanz von Compliance hervorheben und durch ihr Verhalten unterstreichen, kann dieses erfolgreich gestaltet werden (Tone from the Top). Aus dem Tone from the Top muss ein Verständnis und eine Unternehmenskultur für alle von allen werden.

Erforderlich ist. ein unmissverständliches Bekenntnis zur Einhaltung eben der Compliance. Dabei sollte verdeutlicht werden, dass im Interesse eines regelkonformen und wertorientierten Verhaltens auch wirtschaftliche Einbußen in Kauf genommen werden müssen. Ebenso wichtig ist die Betonung, dass Regelverletzungen nicht geduldet, sondern verfolgt und sanktioniert werden, da anderenfalls das Bekenntnis Gefahr läuft, als Erklärung eines Papiertigers zu gelten, und eine hinreichende Akzeptanz kaum zu erwarten ist .

Bereits nach dem Prüfungsstandard 980 des Instituts der Wirtschaftsprüferkammer (IDW PS 980) zählt die Compliance-Kultur zu den Grundelementen eines angemessenen CMS. Auch international stellt die Compliance-Kultur einen unverzichtbaren Bestandteil eines wirksamen CMS dar, wie ausdrücklich niederlegt im UK Bribery Act oder dem US-amerikanischen Federal Sentencing Guidelines Manual.

Neben dem klaren Bekenntnis des Topmanagements zu Compliance ist auch die Sanktionskultur des Unternehmens wichtig, die nicht nur Verstöße ohne Ansehen der Person aufdeckt und angemessen sanktioniert, sondern auch Hinweisgeber fair behandelt und vor Schäden schützt. Letztlich hält regelmäßige Kommunikation und Schulung zu relevanten Compliance-Themen die Kultur lebendig. Dabei gilt es, die Mitarbeiter dort abzuholen, wo sie stehen, also sie gezielt zu Themen anzusprechen, die für ihren Arbeitsalltag von Bedeutung sind, ohne sie zu überfordern oder zu ermüden.

Die Unternehmenskultur entwickelt sich im Laufe der Implementierung eines Compliance-Management-Systems zunehmend. Nach Abschluss der Implementierung verstehen viele Mitarbeiter erstmals, womit sich das Unternehmen beschäftigt, welches die Werte sind etc. Den Mitarbeitern wird immer wichtiger, zum Unternehmen zu gehören und ihr Unternehmen zu schützen.

Nur über die Wertevermittlung gelingt es, ein tatsächlich funktionierendes CMS zu implementieren. Allein die Einführung eines statischen CMS führt zu Missverständnissen und zur kompletten Ablehnung des CMS bei den Mitarbeitern. Insbesondere bei Unternehmen und auch bei Behörden, die lediglich Verbote aussprechen, um sich zu schützen, ist die Akzeptanz von CMS – verständlicherweise – gering. Die Mitarbeiter verstehen nicht und sie können es nicht verstehen, warum plötzlich Verbote aufgestellt werden, angeblich allein zur „Korruptionsprävention“. Dies suggeriert dem Mitarbeiter, dass er selbst im Fokus eines Kor-

12 Vgl. Ziff. 5.1 Abs. 1 ISO 19600.
13 Vgl. Ziff. 7.2.2.2 Abs. 2 ISO 19600.
14 Vgl. Ziff. 7.3.2.2 f) ISO 19600.
15 Vgl. Ziff. 9.1.2 Abs. 4 ISO 19600.

Auch der deutsche Mittelstand wird von der Norm profitieren und die Grundsätze begrüßen.

ruptionsverdachts steht. Überdies muss er bei Nichtbeachtung der Verbote stets mit erheblichen arbeitsrechtlichen Konsequenzen rechnen.

Eine derartige Ablehnung ist bei den Unternehmen nicht zu spüren, die ihre Werte und ihre Kultur tatsächlich vermittelt haben. Hier wird der Mitarbeiter „mitgenommen" und er versteht, warum ein CMS wichtig für das Unternehmen ist, warum es das Unternehmen und warum es ihn schützt und zuletzt, warum es wichtig ist, dass er selbst aufpasst, dass weder das Unternehmen noch der Arbeitsplatz beschädigt werden. Dies sind Beispiele funktionierender Compliance, die deshalb funktionieren, weil eben auf Werte- und Kulturvermittlung so ein erheblicher Wert gelegt wird.

7. ISO 19600 als maßgeschneiderte Compliance-Lösung für den Mittelstand

Auch der deutsche Mittelstand wird von der Norm profitieren und die zugrundeliegenden Grundsätze der Flexibilität und Verhältnismäßigkeit begrüßen. Compliance hat längst den Mittelstand[16] erreicht. ISO 19600 nimmt diese Entwicklung beispielhaft auf und setzt sie um.

Die genannten Schwerpunkte von ISO 19600, nämlich Risikominimierung und Kultur, spielen auch für den Mittelstand eine herausragende Rolle. Kultur wird in der mittelstandsspezifischen Fachliteratur als Basiselement jedes CMS bezeichnet.[17] Dies belegen aktuelle Umfragen zu Compliance.[18]

Der Mittelstand ist selbst dann auf eine internationale Norm angewiesen, wenn das mittelständische Unternehmen im Einzelfall noch nicht international tätig sein sollte. Nicht nur die Gesetzgebung und die Gerichte verlangen eine zunehmende Hinwendung zu Compliance. Längst verlangen dies auch Verbraucher, Kunden und natürlich auch die Auftraggeber, die ihrerseits auf verlässliche zertifizierbare internationale Compliance-Standards angewiesen sind. Auch bei Ausschreibungen spielt das Thema eine immer größere Rolle. Der Mittelstand reagiert auch hier flexibel und implementiert CMS dann gleich auch nach einem internationalen Standard.[19]

Wie bereits oben dargestellt, ist Flexibilität eines der zentralen Themen und Herausforderungen von ISO 19600. Nicht zuletzt aufgrund seiner Flexibilität ist ja der deutsche Mittelstand unbestritten das Rückgrat der deutschen Wirtschaft. Diese These hat sich nicht zuletzt in der erst wenige Jahre zurückliegenden Finanzkrise eindrucksvoll bestätigt. Mittelständische Unternehmer sind die eigentlichen Champions der deutschen Wirtschaft und vieler anderer entwickelter Volkswirtschaften weltweit. Der deutsche Mittelstand genießt weltweit großes Ansehen. Zwar klagt der Mittelstand oft über die mangelnde Beachtung durch die Politik. In der Bevölkerung genießt der Mittelstand jedoch zu Recht ein Vertrauen, das nur noch von wenigen übertroffen wird. Großunternehmen stehen viel schlechter dar. Mehr als 75 Prozent der Deutschen vertrauen dem deutschen Mittelstand. Der Mittelstand liegt damit an vorderster Stelle einer Vertrauensumfrage, weit vor den großen Wirtschaftsunternehmen sowie vor Institutionen wie Kirche, Gerichten und Polizei. Dieses Vertrauen kommt nicht von ungefähr. Der Mittelstand trägt in erheblichem Umfang zur Stabilisierung der gesamtwirtschaftlichen Entwicklung bei und unterscheidet sich in seiner Flexibilität erheblich von Großunternehmen. Während letztere häufiger mit großen Tankern verglichen werden, die sich nur schwer bewegen und beeinflussen lassen, haben sich mittelständische Unternehmen durch eigenständige Geschäftsmodelle, schlankere Strukturen und eine besondere Kultur von Großunternehmen abgesetzt. Mittelständler besetzen Nischen und finden sich in internationalen Spitzengruppen wieder, häufig sogar als Weltmarktführer. Für Mittelständler ist Internationalität keine Zukunftsvision, sondern gelebter Alltag. Innovation kennen wir eher von den Mittelständlern als von Großunternehmen. Mittelständische Unternehmen kennen ihre Kunden persönlich. Flache Hierarchien gehören zum Modell des erfolgreichen Mittelstands.

Diese Flexibilität macht eben auch den Unterschied zum Großunternehmen aus, letztlich auch im Erfolg. Daher sind die für die Großunternehmen erprobten, aber häufig starren Modell, letztlich auch die Compliance-Modelle, nur bedingt auch für den Mittelstand geeignet, da die bisherigen CMS-Konzepte überwiegend von großen Unternehmen für ihre Zwecke entwickelt worden sind.[20] Durch die neue ISO-Norm 19600 können nicht nur die in Großunternehmen erprobten und bewährten Compliance-Modell für den Mittelstand angepasst genutzt werden, sondern erheblich darüber hinaus.

Der deutsche Mittelstand wird es aufgrund seiner Flexibilität sein, der das einstmals starre Thema Compliance mit mehr Flexibilität, mehr Offenheit gestalten wird.

16 Siehe ausführlich hierzu Fissenewert, P.: Compliance für den Mittelstand, München 2013; Makowicz, B./Stadelmaier, M.: Compliance im Mittelstand auf Basis des ISO 19600?, CB 2015, S. 89.

17 Remberg, A.: DB Heft 3/2001, „Die erste Seite".

18 Ausführlich hierzu Achauer, E.: Compliance-Management im deutschen Mittelstand, Eine komparative Betrachtung aktueller Studienergebnisse, ZRFC 5/14, S. 198 ff.; siehe hierzu auch Fissenewert, P.: Compliance für den Mittelstand, NZG 2015, S. 1009 ff.

19 Siehe hierzu auch Fissenewert, P.: Compliance für den Mittelstand – Alte und neue Herausforderungen, CB 2015, S. 265 ff.

20 So auch Makowicz, B./Stadelmaier, M.: Compliance im Mittelstand auf Basis des ISO 19600? Compliance-Berater 2015, S. 89.

ISO 19600 ist ein nützliches Tool zur Implementierung funktionsfähiger Compliance-Management-Systeme.

So wie der Einsatz eines CMS die Entwicklung von Mittelstandsunternehmen sichern wird, so wird der Mittelstand auch die Verbreitung von Compliance im deutschen Wirtschaftsraum fördern.[21]

Mittelständische Unternehmen stehen vor denselben Herausforderungen und Risikofeldern wie Großunternehmen. Dabei sind sie hinsichtlich ihrer personellen, organisatorischen und finanziellen Ressourcen regelmäßig im Nachteil gegenüber den großen. Dies berücksichtigt der Standard aber ausdrücklich, wenn er feststellt, dass Größe, Struktur, Natur und Komplexität der Organisation insbesondere bei der Festlegung des Compliance-Programms, der Zuweisung der Compliance-Zuständigkeiten und Ressourcen sowie dem Umfang der Dokumentation und Informationsbeschaffung zu beachten sind. Mit diesem Instrument können daher Mittelständler den Compliance-Anforderungen durch weniger stark formalisierte Organisations- und Kontrollstrukturen begegnen.

Berücksichtigt werden also nicht nur Flexibilität, Internationalität und Organisation, sondern auch Größe des Unternehmens, mithin auch der Mittelstand, indem in verschiedenen Klauseln der eindeutige Hinweis aufgenommen wurde, dass Anwendungsweite der Norm von der Größe, der Struktur und Komplexität einer Organisation abhängig ist. Compliance ist wie ein maßgeschneiderter, auf die Größe und Individualität des Unternehmens angepasster Maßanzug.[22]

Der Mittelstand hat eine weitere Herausforderung zu meistern. Während er sich bei Fragen zum Produkt nebst Innovation und technischer Anforderungen sowie in der Kommunikation zu Kunden und Lieferanten wohl und sattelfest in heimischen Gefilden wähnen kann, fehlt ihm häufig bezüglich rechtssicherer Organisation und bei Fragen zu Antworten der Behörden, Gerichte und Gesetzgeber die Klarheit, wie das Richtige richtig zu machen ist.[23]

8. Fazit

ISO 19600 ist ein sehr nützliches Tool zur Implementierung funktionsfähiger Compliance-Management-Systeme in den unterschiedlichsten Organisationen. Die teilweise an der Norm geübte Kritik ist nicht nachvollziehbar, wenn etwa die fehlende Transparenz des Verfahrens bemängelt wird.[24] Der Bundesverband der Unternehmensjuristen (BUJ) Fachgruppe Compliance, der Bundesverband Deutscher Compliance-Officer (BDCO) sowie das Deutsche Institut für Compliance (DICO) sehen ISO-Standards im Bereich Compliance „als nicht zielführend" an, weil sie unter anderem aufgrund der behaupteten Komplexität der Regelwerke „eine große Belastung insbesondere für KMU darstellen, mit verschiedenen Regelungen des deutschen Rechts und auch bereits bestehenden Compliance-Standards kollidieren, und dadurch letztlich die Entwicklung effektiver Compliance-Programme behindern.[25] Das ist nur schwer nachvollziehbar. Zuzugeben ist aber, dass internationale Herausforderungen, wie etwa die Kunst, in einem global agierenden Mittelstandsunternehmen eine einheitliche Compliance-Kultur unter Berücksichtigung unterschiedlicher Rechts- und Gesellschaftskulturen zu etablieren, nicht abschließend bzw. nur unzureichend angesprochen werden. Methoden, die einen sogenannten conflict of laws oder gar clash of cultures lösen, bietet ISO 19600 nicht,[26] hingegen bieten die vielfältigen kulturellen Hinweise und Verweise einen ausreichenden Spielraum.

Nach allem ist ISO 19600 ein neuer Standard, der seinerseits Standards setzen wird.

ISO 19600 wird sich als internationaler Standard durchsetzen, auch im Mittelstand. ISO-Normen sind weltweit anerkannt und haben ein erhebliches Durchsetzungspotenzial. Weltweit einheitliche Compliance-Standards haben Auswirkungen auf Transparenz und die operativen Geschäfte global tätiger Unternehmen.

21 Fissenewert, P.: Compliance für den Mittelstand, S. 1.

22 So auch Makowicz, B.: Grundsätze der Compliance, 1–10, S. 4 in Makowicz, B./Wolffgang, H.: Rechtsmanagement im Unternehmen.

23 Scherer, J./Fruth, K.: Der Einfluss von Standards, Technikklauseln und des „anerkannten Standes von Wissenschaft und Praxis" auf Organhaftung und Corporate Governance – am Beispiel der ISO 19600 (2015) Compliance-Management-System, CCZ 2015, S. 9 (10).

24 So Hauschka, C. E.: CCZ 1/2015, Editorial.

25 DICO, BDCO, CCZ 2015, S. 21.

26 So zutreffend Schefold, C.: ISO-Compliance – Ein internationaler Leitfaden für das Unternehmens-CMS, ZRFC 1/15, S. 10 (17).