www.comply-online.de
5. JAHRGANG
OKTOBER 2021
SEITEN 1–84
ISSN 2364-7604

comply.

FACHMAGAZIN FÜR COMPLIANCE-VERANTWORTLICHE

© LdF – istockphoto.com

Standards

3/2021

IN KOOPERATION MIT:

Viadrina Compliance Center

DICO Deutsches Institut für Compliance

COMPLIANCE ACADEMY

Reguvis

Editorial

Prof. Dr. Bartosz Makowicz

Liebe Leserinnen, liebe Leser,

während sich der Sommer langsam verabschiedet, hat uns die Corona-Pandemie weiterhin im Griff, auch wenn sie es in Anbetracht des heißen Wahlkampfs nicht mehr so oft in die Schlagzeilen schafft. Es scheint aber, dass wir alle mit der Kraft der sich anbahnenden vierten Welle in das New Normal steuern.

Was wird uns diese Situation im Hinblick auf Compliance und Integrität bringen? Zunächst befassen wir uns in diesem Heft damit, was uns die letzten Monate gebracht haben. Diese waren, abgesehen von den gescheiterten Gesetzesentwürfen, recht ereignisreich. Allein in den letzten fünf Monaten hat es die Internationale Organisation für Normung (ISO) geschafft, drei neue grundlegende Standards zu veröffentlichen. Zum einen ist es die Nachfolgerin der ISO 19600 in Form der ISO 37301 Compliance Management Systems, zum anderen die brandneue ISO 37002 Whistleblowing Management Systems. Drittens und ganz frisch, da gerade jetzt im September, ist auch der ISO 37000 Governance of Organizations erschienen. Für uns in der Redaktion sind es ausreichende Gründe, um uns wieder einmal schwerpunktmäßig mit der Standardisierung im Bereich von Governance und Compliance Management zu befassen. Der weitere Grund ist aber ebenso gewichtig: So schließt das Deutsche Institut für Compliance (DICO e.V.) Ende dieses Jahres ein dreijähriges Projekt ab, im Rahmen dessen von Wirtschaft und Wissenschaft deutsche Standards für Compliance entstanden sind. Hierzu konnten wir die beiden Sprecher des DICO-Vorstands sprechen (S. 10 f.). Abgerundet wird der Brennpunkt mit Ausführungen zur Zertifizierung von CMS, bei der durchaus Vor- und Nachteile abgewogen werden sollten (S. 24 ff.).

Ergänzt wird das Heft durch die bewährten Regulars in den Bereichen Geldwäscheprävention, IT-Compliance, Whistleblowing und Sustainability. Wir danken den Themenpaten herzlich für die inhaltsreichen Beiträge in den Rubriken. Im Hinblick auf die Digitalisierung besonders erwähnenswert sind die beiden Beiträge zur Digitalethik (S. 40 f.) sowie ein Interview u.a. zur KI-Compliance (S. 49 ff.).

Nicht weniger spannend wird es in diesem Heft bei den Essentials. Neben einem höchst interessanten Aufsatz zur Bedeutung von Werten und Integrität (S. 72 ff.) konnten wir Frau Manuela Mackert, ehem. Chief Compliance Officer der Deutschen Telekom AG, für ein Fachgespräch gewinnen (S. 67 ff.). Sie teilte mit uns ihre besonders spannenden Einblicke und Erfahrungen zur Compliance-Entwicklung in Deutschland und wagte einen Ausblick.

Es ist September und obwohl es draußen kühl und trüb wird, steigen Unternehmen und damit Compliance Officer in die heißeste Phase des Jahres ein. Möge das Heft Ihre Pausen mit inhaltsreichen Beiträgen füllen!

Wir wünschen Ihnen eine ertragreiche Lektüre!

Ihr

Prof. Dr. B. Makowicz

Viadrina Compliance Center
Europa-Universität Viadrina Frankfurt (Oder)

Im Brennpunkt

> Standards

Regulars

> Geldwäscheprävention

> IT-Compliance

Regulars

> Whistleblowing

> Sustainability

> Finanzbranche

Essentials

Services

Impressum

comply.
Fachmagazin für Compliance-Verantwortliche

Schriftleitung und Redaktion
Prof. Dr. Bartosz Makowicz

Beirat
Holger Beutel, Dr. Günter Birnbaum, Michael Falk, Prof. Dr. Peter Fissenewert, Michael Kayser, Prof. Dr. Thomas Knobloch, Prof. Dr. Thomas Rotsch, Prof. Dr. Lena Rudkowski, Dr. Amr Sarhan, Prof. Dr. Stefan Siepelt, Martin Stadelmaier, Prof. Dr. Hans-Michael Wolffgang, Prof. Dr. Sonja Wüstemann

Redaktion Reguvis | Fachmedien GmbH
RA Jörg Schick
Telefon: 0221/9 76 68-186
E-Mail: joerg.schick@reguvis.de

Wiebke Schmidt
Telefon: 0221/9 76 68 -291 · Telefax: 0221/9 76 68-271
E-Mail: wiebke.schmidt@reguvis.de

Manuskripte
Manuskripte sind unmittelbar an die Redaktion im Verlag zu senden. Auch für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Der Verlag behält sich das Recht zur redaktionellen Bearbeitung der angenommenen Manuskripte vor.

Erscheinungsweise
Vierteljährlich (März, Juni, September, Dezember)

Bezugspreise
Der Jahresabopreis inkl. Online-Archiv und Zeitschriften-App beträgt 134,40,– €, Sonderpreis für Verbandsmitglieder und Behördenvertreter 98,– € (inkl. MwSt. und Versandkosten (Inland 0,75 € pro Ausgabe/Ausland 3,– € pro Ausgabe))

Bestellungen über den Verlag
Kündigungen sind nach Ablauf von 12 Monaten möglich. Sie müssen bis zum 15. des Vormonats beim Verlag eingegangen sein.
Verlag: Reguvis Fachmedien GmbH
Amsterdamer Str. 192, 50735 Köln

Geschäftsführung: Jörg Mertens

Abo-Service
Telefon: 0221/9 76 68-315 · Telefax: 0221/9 76 68-271
E-Mail: wirtchaft@reguvis.de

Anzeigenleitung
Hans Stender
Reguvis | Fachmedien GmbH
Amsterdamer Str. 192, 50735 Köln
Telefon: 0221/9 76 68-343 · Telefax: 0221/9 76 68-288
E-Mail: hans.stender@reguvis.de

Anzeigenpreise
Es gilt die Anzeigenpreisliste Nr. 1 vom 1.1.2018

Herstellung
Günter Fabritius, Telefon: 0221/9 76 68-182

Satz und Layout
Anke Minge · E-Mail: mail@ankeminge.de

Druck
Appel & Klinger Druck und Medien GmbH

Warum Compliance-Management-Systeme zertifiziert werden sollten (und warum nicht)

Vor- und Nachteile von Zertifizierungen von CMS

Außerhalb der Compliance-Welt ist es schon lange unbestritten, dass ISO-Zertifizierungen deutliche Vorteile für Unternehmen im Kampf um neue Aufträge und Marktanteile bringen. In manchen Branchen – etwa der Automobilindustrie oder im Pflegebereich – ist sie heute sogar Voraussetzung, um überhaupt wirtschaftlich agieren zu können. Gesenkte Prozesskosten, geringere Fehlerquoten und reduzierte Risiken sind einige der wichtigsten zu nennenden Vorteile, die man mit einer ISO-Zertifizierung gewinnen kann. Letztlich gehört hierzu auch der Image- und Wettbewerbsvorteil, der auch längst schon für Compliance-Management-Systeme (CMS) erkannt wurde.

Natürlich gibt es auch Nachteile, wie Zeitaufwand und Kosten, um nur die wesentlichsten Faktoren zu nennen. Jeder kennt den Aufwand, der mit der Implementierung eines effektiven CMS verbunden ist. Auch wenn wir alle wissen, dass die Schäden, die bei nicht vorhandenem CMS eintreten können, deutlich höher sein können als der Aufwand, soll der Aufwand an dieser Stelle nicht geleugnet werden. Auch wenn – um es hier bereits vorwegzunehmen – am Ende dieses Beitrags herauskommen wird, dass sich jeder Aufwand lohnt und jedes „Kontra" hinter den vielen „Pros" zurückbleibt.

Zertifizierungskosten

Die Zertifizierungskosten sind der naheliegendste Kostenfaktor. Und nicht einmal dieser ist pauschal berechenbar. Unterschiedliche Zertifizierungsstellen haben verschiedene Methoden, die Kosten für die Zertifizierung zu berechnen. Als übliche Einflussfaktoren kann man aber festhalten:

- Branche/Branchenrisiko
- Größe des Unternehmens bzw. Anzahl der Mitarbeiter
- Anzahl der Standorte/Lage der Standorte

Vorlaufkosten bzw. Beratungskosten

Im Vorfeld einer ISO-Zertifizierung ist einiges zu tun, um den Anforderungen einer CMS-Zertifizierung zu genügen. Das ist in der Praxis in aller Regel nur mit dem entsprechenden externen Fachwissen zu bewältigen. Unternehmensintern sind Kräfte gebunden. Zudem ist im Bereich CMS der Markt der Berater zwar groß, wegen der Vielzahl der zu beachtenden rechtlichen Vorschriften ist der Markt aber auf weniger Experten beschränkt als z. B. in rein technischen Bereichen. Die notwendigen Spezialisten sind daher oftmals nicht so zahlreich verfügbar, dass man als Kunde ein großes preisliches Entgegenkommen erwarten darf. Qualität hat hier eben auch ihren Preis.

Je nach Komplexität der vorhandenen Prozesse und Abläufe kann die Zertifizierung auch die Anschaffung neuer Software oder Hardware erforderlich machen. Ebenso müssen in größeren Organisationsbereichen ggf. neue Stellen geschaffen werden, die sich mit der Pflege des zu implementierenden CMS befassen. Bei Neuzertifizierungen bestehender Zertifikate sind die zu erwartenden Aufwände für die Beratung aber dann schon sehr viel überschaubarer und berechenbarer.

Mehraufwand durch Plan-Do-Check-Act

Wer sich auf ein effektives CMS einlässt, muss sich auch bewusst sein, dass er es zukünftig leben muss. Ohne zusätzliche Aufwände vor allem zur Dokumentation ist dies nicht zu machen. Ebenso müssen in vielen Branchen auch Änderungen und Anpassungen möglicher weiterer ISO-Zertifizierungen erfolgen, um nicht bei späteren Zertifizierungen plötzlich vor Problemen zu stehen.

Nicht zuletzt sollte das eigene CMS natürlich auch aus eigenem Antrieb heraus ständig verbessert und weiterentwickelt werden, denn nur dann kann es auch wirklich effektiv arbeiten. Mit der Implementierung oder gar Zertifizierung ist der Aufwand also nicht beendet, sondern er fängt gerade erst an.

CMS darf kein Papiertiger sein

Der Erhalt einer ISO-Zertifizierung ist ein Grund zur Freude für das eigene Unternehmen, kann aber auch schnell dazu führen, dass sich Genugtuung und Selbstverständlichkeit wieder breit machen. Man hat eben ein Zertifikat, welches einem bescheinigt, dass man sauber und compliant arbeitet. Mehr geht zu diesem Zeitpunkt nicht. Mehr geht aber über diesen Zeitpunkt hinaus. Denn diesem Effekt, dass man eigentlich nichts mehr machen muss, stehen schon die Anforderungen einer ISO-Management-Zertifizierung entgegen. Dies bedeutet, dass die Unternehmensführung ständig aktiv an der Fortführung des CMS arbeiten muss, etwa durch ständige Weiterbildung und Schulung etc. Die Zeit nach der Erstzertifizierung kann für betroffene Mitarbeiter schwierig sein. Zumeist sind ja neue Richtlinien geschaffen bzw. alte präzisiert worden, die eben ein neues Denken und möglicherweise auch neue Arbeitsprozesse erfordern. Dies bedeutet zusätzlichen Aufwand für Kontrolle und Dokumentation. Nur Mitarbeiter, denen die Vorteile des implementierten CMS auch bewusst gemacht werden, können zu dessen Akzeptanz auch aktiv beitragen.

10 Gründe „pro" Zertifizierung am Beispiel von ISO 37301

Die neue ISO 37301 bietet die Möglichkeit der Zertifizierung von CMS und folgt der ISO 19600 nach. Die Norm schafft einen Standard für CMS und fordert ein wirksames CMS, welches im Unternehmen, wenn es den Maßgaben der ISO 37301 entspricht, zertifiziert wird.

- ISO 37301 verkörpert einen weltweiten „Best-Practice Standard". Der Standard ist von der Entstehung her sehr breit abgestützt und wird schon kurzfristig von den Behörden als Benchmark für angemessene Compliance-Bemühungen genannt werden.
- ISO 37301 gewährt Unternehmen als Guideline-Standard große Flexibilität und ermöglicht diesen, bei der konkreten Ausgestaltung des CMS die Größe, vorhandene Ressourcen und andere relevante Faktoren zu berücksichtigen. Somit bietet sich eine Zertifizierung grundsätzlich für alle Unternehmen an. Kleine und risikoarme Unternehmen können zunächst den Weg einer Implementierung eines CMS nach ISO 37301 ohne Zertifizierung wählen.
- Die ISO 37301 gibt den Unternehmen die Möglichkeit zur Entscheidung, das CMS als separates System zu implementieren. Es sollte jedoch idealerweise in Verbindung mit den anderen Management-Systemen der Organisation wie etwa für Risiko, Qualität, Umwelt, Informationssicherheit, Lebensmittelsicherheit und zur Bekämpfung von Korruption implementiert werden. In diesen Fällen können die Unternehmen z. B. auf ISO 9001, ISO 14001, ISO/IEC 27001, ISO 22000, ISO 37001 sowie ISO 26000 und ISO 31000 verweisen. Unternehmen, die ihr CMS an der ISO 19600 orientiert haben oder dies vorhaben, können beruhigt sein. Da die ISO 19600 und die neue ISO 37301 die gleiche Ausrichtung haben, befindet man sich bei Verwendung der ISO 19600 auf

© Peter Badge

Prof. Dr. Peter Fissenewert

Der Autor ist Rechtsanwalt und Partner der internationalen Kanzlei BUSE Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB. Seine Tätigkeitsschwerpunkte sind das Gesellschaftsrecht sowie die Restrukturierungs- und Sanierungsberatung. Er hat als Mitglied des DIN-Normenausschusses Organisationsprozesse (NAOrg) NA 175-00-01 AA „Governance und Compliance-Management" u.a. an der neuen ISO 37301 mitgewirkt.

der sicheren Seite. Nach Einführung der ISO 37301 wird ein Abgleich erforderlich werden, der jedoch im Aufwand überschaubar sein dürfte.

- ISO 37301 folgt derselben Systematik und Terminologie wie die übrigen ISO-Normen. Unternehmen, welche bereits über andere ISO-Zertifizierungen verfügen, finden sich deshalb mit dem neuen ISO-Standard rasch zurecht.
- Mit einer Zertifizierung kann das Unternehmen der Erwartungshaltung einer Vielzahl von Stakeholdern gerecht werden (Behörden, Aktionäre, Geldgeber, Mitarbeitende, Kunden und Lieferanten, Öffentlichkeit, NGOs, Medien, Ratingagenturen etc.); diese stellen zunehmend höhere Erwartungen an ein CMS.
- Im jetzigen Zeitpunkt kann eine Zertifizierung als Image- und Wettbewerbsvorteil gegenüber Wettbewerbern angeführt werden; je mehr Unternehmen sich zertifizieren lassen, umso mehr wird alsdann der Druck auf die übrigen Unternehmen zunehmen, nachzuziehen.
- Im Falle einer behördlichen Untersuchung wegen eines möglichen Compliance-Verstoßes wird die Ausgestaltung des CMS nach ISO 37301 und die Zertifizierung im Sinne einer „corporate defense" angeführt werden können. Das geplante Verbandssanktionengesetz (VerSanG) wird den Fokus verstärkt auf CMS legen.
  Das VerSanG verfolgt das Ziel, Compliance-Maßnahmen zu fördern und rechtssichere Anreize für Investitionen in Compliance zu schaffen. Bei der Bemessung einer Geldsanktion sollen die Behörden unter anderem „vor der Verbandstat getroffene Vorkehrungen zur Vermeidung und Aufdeckung von Verbandstaten" berücksichtigen.
  Zwar soll bei kleineren und mittleren Unternehmen der „Zukauf" eines Compliance-Programms oder von Zertifizierungen regelmäßig nicht erforderlich sein. Es ist dennoch damit zu rechnen, dass einer Zertifizierung zukünftig als Beleg für die getroffenen Vorkehrungen zur Vermeidung von Verbandstaten eine wesentliche Bedeutung zukommen wird.
  Wichtige Stimmen in der Wirtschaft fordern bereits, bei Vorliegen einer Zertifizierung des CMS gar keine Sanktion gegen das Unternehmen zu verhängen
- Den internen Compliance-Bemühungen wird mit einer externen Zertifizierung zu mehr Visibilität und Legitimation verholfen.
- Die Zertifizierung belegt, dass Compliance in einem Unternehmen systematisch betrieben wird und alle relevanten und anerkannten Elemente eines CMS adressiert sind und ist zugleich Ausdruck eines starken Bekenntnisses des Unternehmens zu Compliance.
- Die Zertifizierung gewährt der für Compliance verantwortlichen Unternehmensführung eine gewisse Sicherheit, dass das Unternehmen in der Tat über ein wirksames CMS verfügt.

FAZIT

Im Grunde gibt es keine nennenswerten Gründe, die gegen eine Zertifizierung sprechen. Die Vorteile liegen klar auf der Hand und jegliche Investition zahlt sich hier mehrfach aus.

Der Aufwand ist häufig geringer als gedacht. Unternehmen, die bislang über noch kein implementiertes CMS verfügen, sind häufig weiter, als sie dachten. Die meisten Unternehmen haben bereits Richtlinien, beachten die Gesetze, haben bereits die Anforderungen der DSGVO umgesetzt, verfügen über eine Tax-Compliance, haben klare IT-Strukturen etc. Dies alles sind bereits Bestandteile eines CMS, die „nur" intelligent und kulturell miteinander verknüpft werden müssen. Der Aufwand ist daher überschaubar.

Kleine Unternehmen mit risikoarmen Tätigkeiten können zunächst noch die Zertifizierung hintanstellen. Je mehr Unternehmen sich allerdings zertifizieren lassen, umso mehr geraten andere Unternehmen, auch kleine und risikoarme, unter Druck, hier nachzuziehen.