

The background image shows a man and a woman in professional attire, a woman in a grey blazer and a man in a dark suit, both looking intently at a tablet device they are holding together. They appear to be in an office environment with blurred lights in the background.

Forensic & Integrity Services

Denkanstöße

Prüfung des Compliance-
Management-Systems

The EY logo consists of the letters 'EY' in a bold, white, sans-serif font. A yellow diagonal bar starts from the top right corner of the 'E' and extends towards the bottom left. Below the logo, the tagline 'Building a better working world' is written in a smaller, white, sans-serif font.

EY
Building a better
working world

CMS-Audit: Warum eigentlich?

Die kontinuierliche Entwicklung eines Compliance-Management-Systems (CMS) ist beeinflusst von der Unternehmensentwicklung, geopolitischen Entwicklungen, den Regulatoren und der Gesetzgebung, aber auch von der Unternehmensorganisation und -kultur. Es gibt kein „Fertig“, sondern ein stetiges Anpassen, Entwickeln, Überarbeiten und Beobachten. Ansonsten birgt das CMS die Gefahr, nicht risikospezifisch bzw. nicht wirksam zu sein oder zu bleiben.

Hinzu kommt die Aktualisierung des Deutschen Corporate Governance Kodex, der - neben anderen internationalen Standards - implizit die Wirksamkeit eines CMS verlangt.

Darum sollte man also eine externe Prüfung des CMS anstreben:

- ▶ unabhängige Beurteilung eines Externen zur Ausgestaltung und Geeignetheit des CMS für das Unternehmen
- ▶ Aussagen zur nationalen und internationalen Umsetzung und Wirksamkeit des CMS im Unternehmen
- ▶ Unterstützung der Geschäftsführung und des Vorstands/Aufsichtsrats bei der Beurteilung des CMS und des Risikoumfelds und damit Beitrag zur Enthaftung
- ▶ Empfehlungen zur Weiterentwicklung und zum Finden von Lücken
- ▶ Benchmarking und Awareness im Unternehmen

Wie prüft man ein Compliance-Management-System?

Viele Standards und auch Aufsichtsorgane fordern eine „Prüfung des CMS“. Auf den ersten Blick eine klare Sache - schaut man jedoch genauer hin, merkt man, dass es so einfach doch nicht ist.

Oft gibt es nicht „das CMS“. Welche Risikobereiche gehören dazu? Welche rechtlichen Anforderungen und Länder sollen berücksichtigt werden? Geht es um den Aufsatz und die Ausgestaltung oder die operative Durchführung? Gegen welchen Standard soll geprüft werden? Man könnte zwar auch alles prüfen, doch stehen dabei selten Kosten und Nutzen in einer akzeptablen Relation zueinander.

Daher gilt es, die Prüfung flexibel den individuellen Bedürfnissen und der Risikoumgebung eines Unternehmens anzupassen und trotzdem eine Vergleichbarkeit der Ergebnisse zu gewährleisten.

Dafür ist der IDW PS 980 nach wie vor das Maß der Dinge, da er durch seine Flexibilität sämtliche Anforderungen der Praxis erfüllen kann - speziell wenn mit ihm die Erfüllung der Anforderungen des ISO 37301 geprüft wird. Doch auch dabei gilt es ein paar Dinge zu bedenken.

Dazu ein paar Denkanstöße ...

Der Weg zum Testat

#1

Prüfungsumfang

Was soll geprüft werden?

- ▶ Legen Sie die relevanten Risikobereiche fest; bedenken Sie den Aufwand, den eine Prüfung mit sich bringt.
- ▶ Die Aussage für einen Gesamtkonzern ist oft sinnvoller als nur für Kernländer/-gesellschaften.
- ▶ Prüfen Sie, gegen welches Rahmenwerk nach IDW PS 980 geprüft werden soll. IDW PS 980 ist nur der Standard für die Durchführung einer Prüfung dahin gehend, ob die Anforderungen eines Rahmenwerks (ISO 37301, DOJ etc.) erfüllt sind, und kann nicht selbst als Rahmenwerk herangezogen werden.

Der Weg zum Testat

#2

Prüfungstiefe

Angemessenheit oder Wirksamkeit?

- ▶ Angemessenheit beinhaltet auch immer Implementierung und ist stichtagsbezogen.
- ▶ Wirksamkeit beinhaltet immer auch Angemessenheit und Implementierung und ist zeitraumbezogen. Der Zeitraum beginnt frühestens mit dem Stichtag der Angemessenheit.
- ▶ Nur Berichte zur Wirksamkeit können (in Kurzform) veröffentlicht werden.
- ▶ Der DCGK fordert Angemessenheit und Wirksamkeit.

Der Weg zum Testat

#3 Ausschreibung

Worauf ist bei der Ausschreibung zu achten?

- ▶ Die Ausgestaltung des Compliance-Programms, speziell in anderen Abteilungen (Einkauf, Vertrieb, Finance, HR etc.), variiert stark und macht die Schätzung des Aufwands schwierig. Erstellen und teilen Sie Risiko-Kontroll-Matrizen, um vergleichbarere Angebote zu erhalten.
- ▶ Je einheitlicher ein CMS (global) ausgestaltet ist, desto einfacher wird eine Prüfung - nehmen Sie hierzu Stellung!
- ▶ Für Prüfungen gelten die IDW-Auftragsbedingungen.

Der Weg zum Testat

#4

Ihr Anteil

Unterschätzen Sie nicht den Aufwand der CMS-Prüfung!

- ▶ Binden Sie frühzeitig unterschiedliche Funktionen zur Vorbereitung und zeitlichen Planung ein - die Prüfung findet nicht nur in der Compliance statt.
- ▶ Halten Sie wesentliche Dokumente final vor bzw. stellen Sie sicher, dass Sie schnell darauf zugreifen können.
- ▶ Planen Sie ausreichend Zeit Ihres internen Projektleiters zur Koordination und Begleitung der Prüfung ein, insbesondere bei internationalen Wirksamkeitsprüfungen.
- ▶ Kommunizieren Sie intern frühzeitig und aktiv den Mehrwert der Prüfung für die ganze Organisation.

“

Eine externe Prüfung des CMS nur auf den Nutzen der Prüfungsaussage zur Angemessenheit bzw.

Wirksamkeit beispielsweise gegenüber Geschäftspartnern oder Aufsichtsgremien zu reduzieren ist zu kurz gedacht.

Sie hilft auch, das Bewusstsein für Compliance innerhalb des Unternehmens zu stärken, betont die Wichtigkeit von Compliance und kann als

Gradmesser der Zielerreichung im Bereich Compliance dienen. Nicht selten führt sie auch zu interessanten und überraschenden Einblicken für die Compliance-Organisation.



Felix Kraft

Director

Forensic & Integrity Services
Integrity, Compliance & Ethics (ICE)
CMS-Audit Leader Deutschland

Wenn wir Sie auf Ihrer Compliance-Reise begleiten sollen, kontaktieren Sie uns!



Andreas Pyrcek

Partner, CCEP (International)
Forensic & Integrity Services
Integrity, Compliance & Ethics (ICE)
Global Leader

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Graf-Adolf-Platz 15
40213 Düsseldorf

Telefon +49 211 9352 26881
andreas.pyrcek@de.ey.com
[LinkedIn](#)



Felix Kraft

Director
Forensic & Integrity Services
Integrity, Compliance & Ethics (ICE)
Solution Leader Deutschland

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Rothenbaumchaussee 78
20148 Hamburg

Telefon +49 89 14331 20904
felix.kraft@de.ey.com
[LinkedIn](#)



Weitere Informationen finden Sie hier: de.ey.com/integrity-compliance

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

„EY“ und „wir“ beziehen sich in dieser Präsentation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten.
Informationen darüber, wie EY personenbezogene Daten sammelt und verwendet, sowie eine Beschreibung der Rechte, die Einzelpersonen gemäß der Datenschutzgesetzgebung haben, sind über ey.com/privacy verfügbar. Weitere Informationen zu unserer Organisation finden Sie unter ey.com.

In Deutschland finden Sie uns an 20 Standorten.

© 2023 Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft
All Rights Reserved.

ED None

ey.com/de