KPMG
cutting through complexity

WisteV – Compliance Standards

Wirksamkeitsbeurteilung eines Compliance Management Systems nach IDW PS 980

WP / StB Verena Brandt
Partner, Governance & Assurance Services

Frankfurt, 4. Dezember 2014

Compliance
Sicher wachsen

Überblick

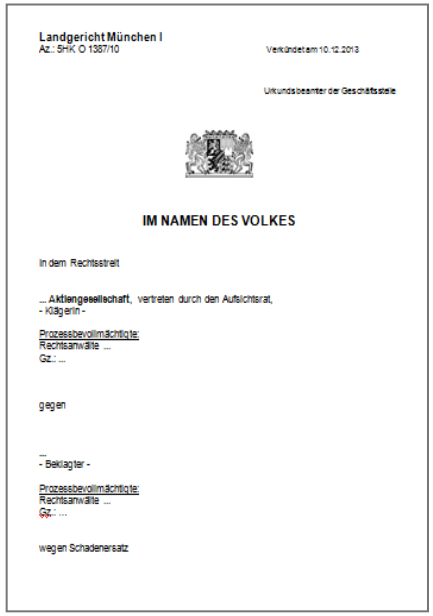
1. Relevanz und Nutzen einer CMS-Prüfung nach IDW PS 980
2. Prüfungsdurchführung – Erfahrungen aus der Praxis
3. Aktueller Marktüberblick und weitere Entwicklungen

1. Relevanz und Nutzen einer CMS-Prüfung nach IDW PS 980
Erfüllung von Compliance-Anforderungen

Anforderungen	Pflicht im Außenverhältnis, sämtliche Vorschriften einzuhalten, die das Unternehmen als Rechtssubjekt treffen	§§ 91 Abs. 2, 76 Abs. 1, 93 Abs. 1 AktG (LG München 5 HKO 1387/10)
	Pflicht zur gehörigen Aufsicht	§§ 30, 130 OWiG
Einrichtung	■ Auswahl- und Organisationsermessen ■ Sorgfalt eines ordentlichen und gewissenhaften Geschäftsführers ■ Notwendig: geeignete Basis für Entscheidung	■ Rückgriff auf allgemein anerkannte Compliance-Standards als Rahmenwerk, um eine **angemessene Basis für Ermessensausübung** zu haben (z.B. ISO/DIS 19600) ■ ISO/DIS 19600 **konkretisiert die Anforderungen hinsichtlich Compliance an Vorstand u. Management**
Überwachung und Nachweis	■ Wirksamkeit des eingerichteten CMS muss überwacht werden (Delegationsüberwachung) ■ Nachweis für angemessene Entscheidung im Rahmen der BJR muss vom Vorstand erbracht werden	■ IDW PS 980 eignet sich zur Delegationsüberwachung und als **Nachweis der angemessenen Ermessensausübung** ■ Anscheinsbeweis für gehörige Aufsicht nach § 130 OWiG

1. Relevanz und Nutzen einer CMS-Prüfung nach IDW PS 980
IDW PS 980 im Lichte aktueller rechtlicher Entwicklungen

Das Urteil des LG München I konkretisiert die Anforderungen an ein wirksames CMS und die Compliance-Pflichten des Vorstands



Landgericht München I
Az.: 5HK O 1387/10 Verkündet am 10.12.2013

Urkundsbeamter der Geschäftsstelle

IM NAMEN DES VOLKES

In dem Rechtsstreit

... Aktiengesellschaft, vertreten durch den Aufsichtsrat,
- Klägerin -

Prozessbevollmächtigte:
Rechtsanwälte ...
Gz.: ...

gegen

...
- Beklagter -

Prozessbevollmächtigte:
Rechtsanwälte ...
Gz.: ...

wegen Schadenersatz

Siemens-Korruptionsaffäre:
Ex-Finanzchef zu 15 Millionen Euro Schadensersatz verurteilt
Spiegel online, 10.12.2013

Gericht verlangt ein Kontrollsystem
Vorstände müssen Rechtsverstößen von Mitarbeitern systematisch vorbeugen
FAZ, 12.03.2014

„Meilenstein der Compliance-Rechtsprechung"
Börsen-Zeitung, 3.5.2014

„Compliance ist Chefsache"
Ein effizientes Compliancesystem wird im Zusammenhang mit der Haftungsvorsorge in Unternehmen immer wichtiger
Deutscher AnwaltSpiegel, 23.04.2014

Entwurf eines Verbandsstrafgesetzes

- **Sanktionierung von Unternehmen** bei Verletzung von betriebsbezogenen Pflichten durch Entscheidungsträger
- Im Schadensfall können sich **nachweisliche Compliance- Maßnahmen** des Unternehmens **strafmildernd** auswirken

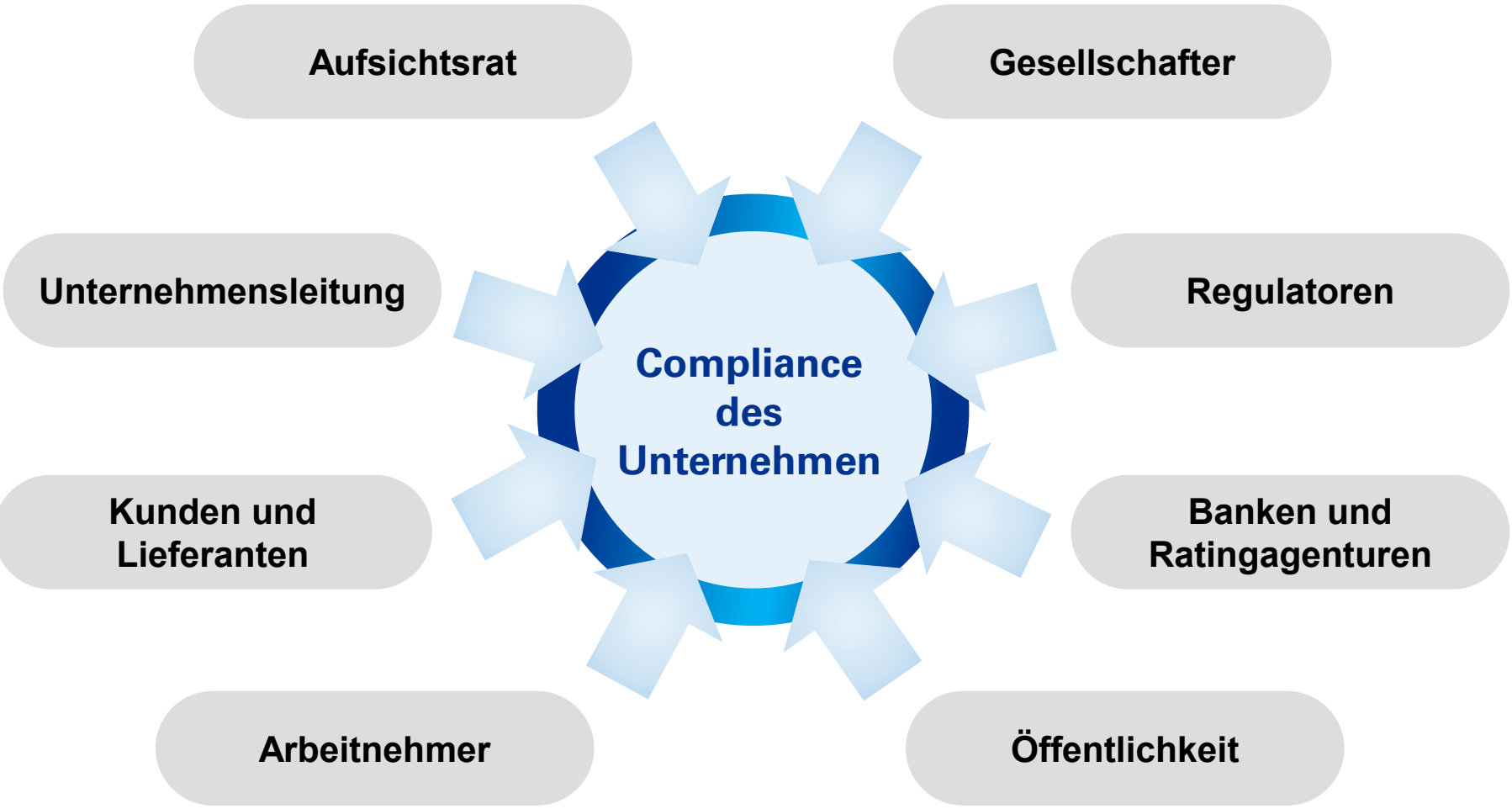
Vorschlag einer Reform des OWiG
(Bundesverband der Unternehmensjuristen)

- **Gesetzliche Konkretisierung** der durch § 130 OWiG statuierten, bislang durch Rechtsprechung und Literatur ausgelegten, **Aufsichts- und Organisationspflichten**
- **Zwingende strafmildernde Berücksichtigung** eines **angemessenen und effektiven CMS**, wenn die Anknüpfungstat begangen wurde, obgleich die in § 130 Abs. 1 festgelegten Pflichten erfüllt wurden

Nachweis- und Dokumentationsfunktion einer externen Prüfung und Bescheinigung

1. Relevanz und Nutzen einer CMS-Prüfung nach IDW PS 980
Aktuelle Entwicklungen – wachsende Ansprüche von Stakeholdern

Die Ansprüche von Regulatoren, Vorstand, Audit Committee und Geschäftspartnern an die Compliance von Unternehmen und damit der Wirksamkeit des CMS wachsen



Nutzen einer IDW PS 980 CMS-Prüfung und Bescheinigung

- Reduktion gesellschaftlicher sowie persönlicher Haftungs- und Reputationsrisiken
- Stärkung des Ansehens in Märkten und der Öffentlichkeit Schaffung von Vertrauen
- Erfüllung gestiegener Dokumentations- und Nachweisanforderungen
- Erfüllung von Kundenanforderungen (Supplier Code of Conduct); Sicherheit für die Supply Chain
- Verbesserung der internen Compliance-Kultur und Akzeptanz; Schärfung des Bewusstseins für Compliance im Unternehmen
- Sicherheit bzgl. der Qualität der Compliance Grundsätze und Maßnahmen
- Effizienzsteigerungen durch integrative Ansätze: Optimierung der Schnittstellen zum RMS, IKS, IR
- Vergleich mit Good Practice Standards; Benchmarking
- Prüfung und Bescheinigung nach IDW PS 980 als anerkanntes und belastbares Qualitätsurteil für das CMS
- Rating- und Kapitalmarktrelevanz

2. Prüfungsdurchführung – Erfahrungen aus der Praxis
CMS-Rahmenkonzept nach IDW PS 980

Konzeptionsprüfung

- Sind die Aussagen der gesetzlichen Vertreter in der Beschreibung zur Konzeption des CMS in allen wesentlichen Belangen **angemessen dargestellt**?
- Geht die CMS-Beschreibung auf sämtliche Grundelemente eines CMS ein (**Vollständigkeit**)?
  - Kultur
  - Ziele
  - Organisation
  - Risiken
  - Programm
  - Kommunikation
  - Überwachung und Verbesserung

Angemessenheitsprüfung

- Sind aufbauend auf der Konzeption konkrete Prozesse und Maßnahmen entwickelt, die **angemessen und geeignet** sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch Verstöße zu verhindern?
- Sind die Grundsätze und Maßnahmen **zu einem bestimmten Zeitpunkt implementiert?**

Wirksamkeitsprüfung

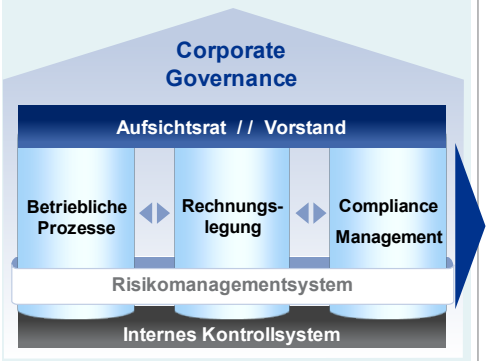
- Sind die konkreten Prozesse und Maßnahmen während eines **bestimmten Zeitraums wirksam?**
- **Konzernweite Gesamtaussage** beinhaltet dezentrale Prüfungen in ausgesuchten Konzerneinheiten (repräsentative Stichprobe); Auswahl erfolgt risikoorientiert auf Basis eines Compliance Risk Assessments
- Die Wirksamkeitsprüfung **beinhaltet** die Beurteilung der in der CMS-Beschreibung dargestellten Konzeption sowie deren Ange-messenheit und Implementierung

- Betriebswirtschaftliche Prüfung
- Risikoorientierte Sytemprüfung
- CMS-Beschreibung
- Scoping-Entscheidungen erforderlich
- Skalierung möglich
- Standard-Rahmenkonzept; Benchmark

2. Prüfungsdurchführung – Erfahrungen aus der Praxis
CMS-Rahmenkonzept nach IDW PS 980

Eine umfassende Risikoanalyse ist zwingender Ausgangspunkt eines wirksamen, risikoorientierten Compliance Management Systems

CMS ist Teil des Risikomanagements



- §130 OWiG
- UKBA/FCPA
- Sorgfalts-pflicht (AktG, GmbHG)
- Andere Jurisdiktionen
- IDW PS 980
- „Good practice“

Grundelemente des CMS nach IDW PS 980

- Überwachung der Angemessenheit und Wirksamkeit
- Voraussetzung: ausreichende Dokumentation
- Berichterstattung von Schwachstellen und Verstößen
- Management trägt Verantwortung

- Bewusstsein für die Bedeutung von Regeln als Grundlage für die Angemessenheit und Wirksamkeit des CMS
- Wesentlicher Einflussfaktor: Grundeinstellung und Verhaltensweisen des Managements („Tone at the Top“)

- Information betroffener Mitarbeiter und ggf. Dritter über das Compliance Programm sowie der Rollen/Verantwortlichkeiten
- Festlegung der Berichtswege für Compliance-Risiken und für Hinweise auf Regelverstöße

- Festlegung wesentlicher zu erreichender CMS-Ziele auf Grundlage der allgemeinen Unternehmensziele
- Festlegung der relevanten Teilbereiche und der darin einzuhaltenden Regeln

- Alle eingerichteten Grundsätze und Maßnahmen, die der Umsetzung des CMS dienen, einschließlich der bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen.
- Das Compliance-Programm wird zur Sicherstellung einer personenunabhängigen Funktion des CMS dokumentiert

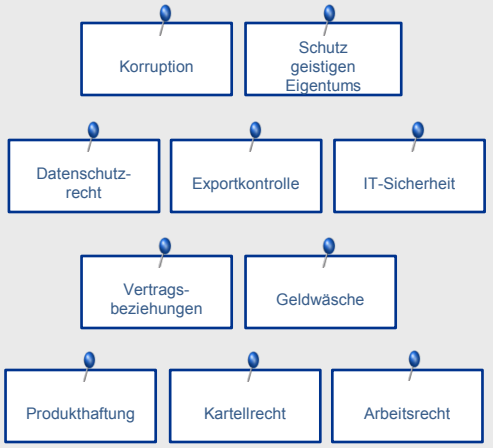
- Bestimmung der Aufbau- und Ablauforganisation
- Festlegung von Rollen, Verantwortlichkeiten und Berichtswegen
- Zurverfügungstellung notwendiger Ressourcen

- Identifikation wesentlicher Compliance-Risiken
- Einführung systematischer Verfahren zur Risikoerkennung und -berichterstattung

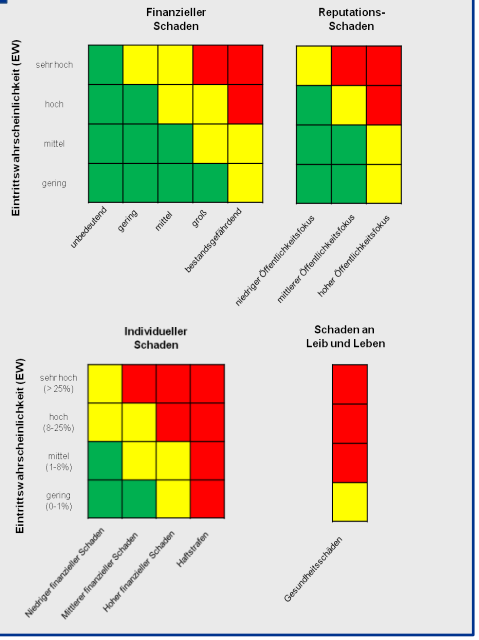
Wesentliche Schritte eines Compliance Risk Assessments

Sowohl in der Top-down- als auch in der Bottom-up-Phase erfolgt die Risikobewertung in drei Schritten

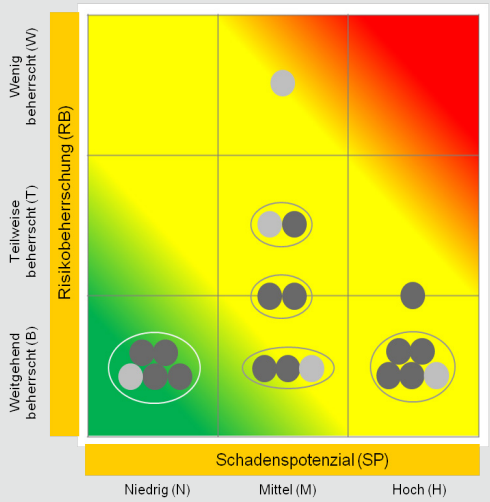
1. Relevanz- und Risikoanalyse



2. Brutto-Risikobeurteilung



2. Netto-Risikobeurteilung



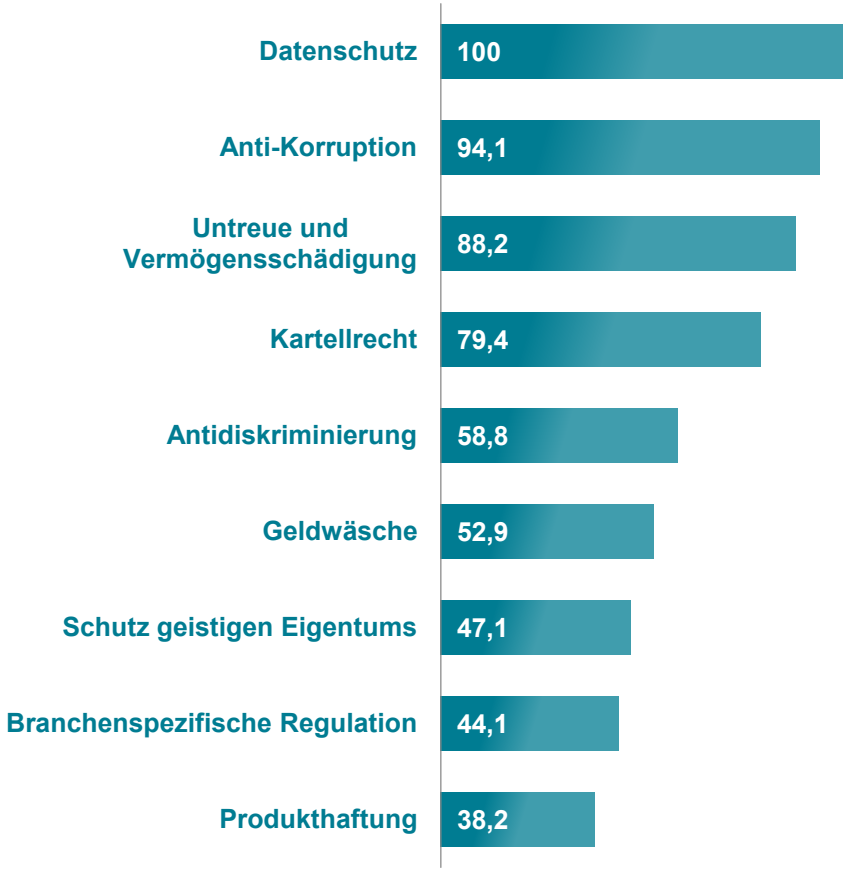
Entwicklung eines umfassenden Risikoinventars

Bewertung des Schadenspotenzials und der Eintrittswahrscheinlichkeit

Identifikation bestehender Maßnahmen (Risikobeherrschung)

2. Prüfungsdurchführung – Erfahrungen aus der Praxis
Festlegung der prüfungsrelevanten Rechtsgebiete

Compliance-Risiken[(a)]



- Welche Risikogebiete im Fokus des CMS liegen, ist eine **strategische Entscheidung**, die von der Geschäftsführung zu treffen ist.
- Die dargestellten Rechtsgebiete bilden die am **häufigsten genannten Themen**, die bei börsennotierten Unternehmen zumeist im Rahmen des Verhaltenskodex geregelt sind.
- Oftmals wird die **Risikoexposition des Unternehmens unterschätzt bzw. nicht wahrgenommen**, etwa im Hinblick auf Antikorruptionsgesetze mit extraterritorialem Anwendungsbereich wie UK Bribery Act und Foreign Corrupt Practices Act

IDW PS 980

„Unter Berücksichtigung der Compliance-Ziele werden die Compliance-Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können“ (Tz. 23).

Anm.: (a) Mehrfachnennungen möglich
Quelle: KPMG CMS-Benchmark Studie 2013

3. Aktueller Marktüberblick und weitere Entwicklungen
Der Markt für CMS-Prüfungen im Wandel

	CMS-Prüfungen bisher…	… und Tendenzen für die Zukunft
Unternehmen, die sich prüfen lassen	■ Überwiegend große Unternehmen (DAX30) ■ Zumeist aus Branchen, die anfällig sind / waren für Verstöße	■ Auch nicht börsennotierte Unternehmen / Mittelstand ■ Diverse Branchen
Geprüfte Teilbereiche	Am häufigsten: ■ Kartellrecht ■ Anti-Korruption	Weitere Teilbereiche: ■ Exportkontrollen, Intellectual Property, Geldwäsche, Datenschutz,…
Rahmen-bedingungen	■ IDW PS 980 seit 2011 ■ Keine analogen Standards im Ausland ■ Meist einmalige Prüfung	■ Überlegungen zu Anpassungen des IDW PS 980 ■ ISO/DIS 19600 als ergänzendes Rahmenkonzept zu IDW PS 980 ■ Wiederkehrende Prüfungen

ISO 19600 – ein globaler Standard für Compliance Management

Der ISO 19600 wird voraussichtlich gegen Ende des Jahres veröffentlicht

Hintergrund

- Global tätige Unternehmen stehen vor der Herausforderung, **einheitliche Compliance-Standards** zur Stärkung der Integrität ihres weltweiten, heterogenen Konzernverbunds zu implementieren, um ein homogenes Compliance-Niveau gewährleisten zu können.
- Der von internationalen Fachexperten entwickelte ISO 19600 soll als **allgemein anerkannter Compliance-Standard** mehr Einheitlichkeit in der globalen Compliance-Umsetzung und damit Erleichterung im globalen Geschäft bieten.
- Der ISO 19600 ist als **flexibler Leitfaden** konzipiert – nicht als zertifizierbares Pflichtenheft mit Sollvorgaben. Er lässt ausreichend Gestaltungs- und Entscheidungsspielraum, um der Anforderung, dass das konkrete CMS auf die Bedürfnisse und Notwendigkeiten des Unternehmens zugeschnitten sein muss, Genüge zu tun.
- Er erhebt den Anspruch, auf **alle Organisationsformen anwendbar** zu sein. Er richtet sich damit nicht nur an Großkonzerne, sondern auch an kleine und mittelständische Unternehmen sowie Behörden und sonstige Organisationen.
- Der Standard fügt sich in die bestehende ISO-Standardlandschaft ein und nimmt teilweise auch Bezug auf andere ISO-Standards (z.B. ISO 31000).

Vielen Dank für Ihre Aufmerksamkeit

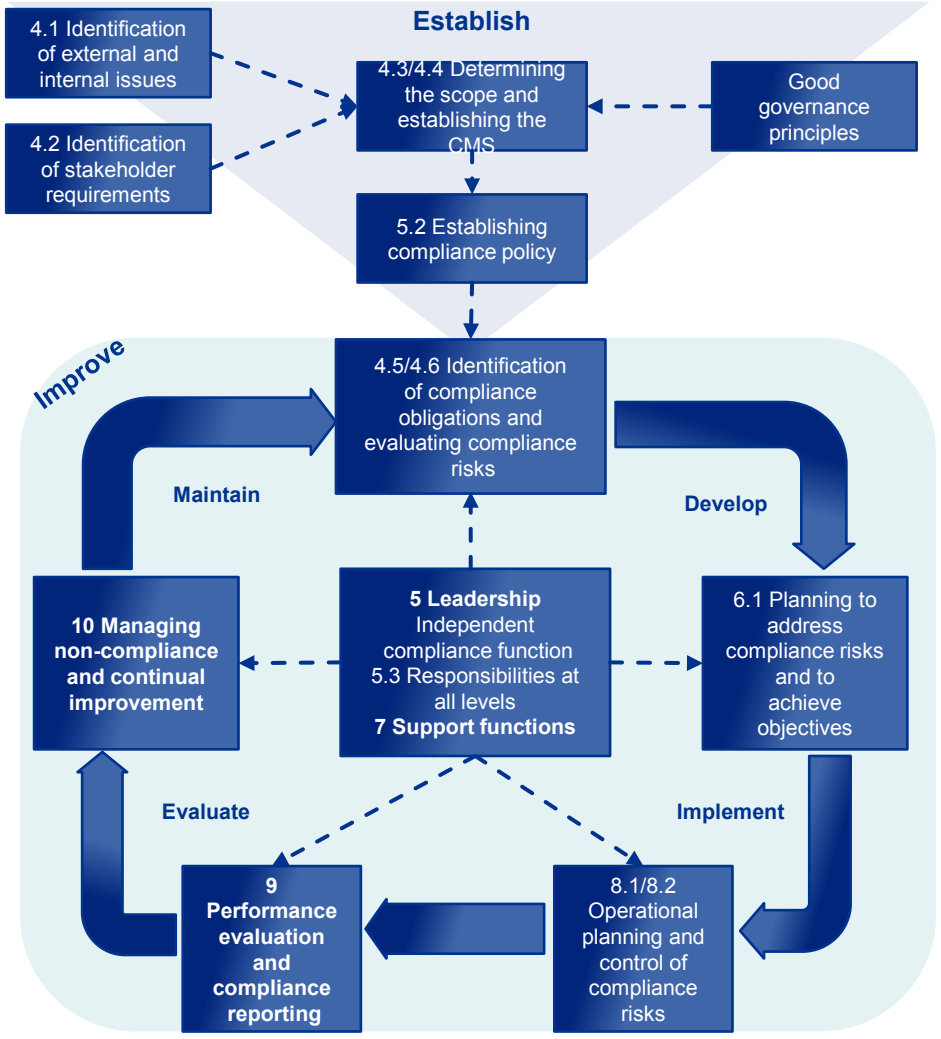
Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

Verena Brandt
Wirtschaftsprüferin, Steuerberaterin
Partner, Governance & Assurance Services

KPMG AG Wirtschaftsprüfungsgesellschaft
Tel: +49 (211) 475 6562
Mobil: +49 (0) 174 323 1754
Email: vbrandt@kpmg.com

Back-Up: CMS-Modell nach ISO 19600

CMS nach ISO 19600



Komponenten	Grundsätze
(4) Context of the Organisation	■ Analysis of the environment in which the organisation operates (context, issues, stakeholders and their requirements, needs and expectations) ■ Scope of the compliance management system ■ Identification of compliance obligations ■ Assessment of the compliance risks
(5) Leadership	■ Policy, commitment, leading by example ■ Roles, responsibilities and authorities with respect to compliance for the board, top and line management, employees and an independent compliance officer
(6) Planning	■ Planning of measures to control compliance risks ■ Establishing compliance objectives
(7) Support	■ Awareness, competence and training in compliance ■ Behaviour and culture ■ Communication and documentation
(8) Operation	■ Implementation of controls for compliance (technical, procedural, ■ directing the attitude and behaviour of personnel)
(9) Performance evaluation	■ Monitoring of compliance, application of indicators ■ Analysis of information and reporting of results (internal and external) ■ Internal Audit and Management Review
(10) Improvement	■ Actions on non-compliance with requirements and escalation to higher management levels when necessary ■ Corrective action ■ Improvement activities

Back-Up: Synopse von ISO 19600 und IDW PS 980