



Neue Prüfungs- und Assurance-Instrumente zur Beurteilung von Systemen und Prozessen

Jens C. Laue, Head of Governance & Assurance

DRSC - IDW Symposium Berlin

29. November 2016





Anforderungen an den Aufsichtsrat und Vorstand



Anforderungen an den AR und Vorstand

Aufsichtsrat



Das BilMoG (Bilanzrechtsmodernisierungsgesetz) verankert die gesetzliche Verpflichtung des Aufsichtsrats zur Wirksamkeitsüberwachung der Corporate Governance Systeme (§ 107 Abs. 3 S. 2 AktG).

Vorstand



Es besteht eine Nachweispflicht des Vorstandes gegenüber dem Aufsichtsrat über die Sicherstellung der Wirksamkeit der Corporate Governance Systeme (§ 93 Abs. 1 AktG, § 43 Abs. 1 GmbHG).

Bei Nichterfüllung der Verpflichtung drohen hohe Reputations- und Haftungsschäden (§ 93 Abs. 2 i.V. m. § 116 AktG). Die Haftung trifft den Aufsichtsrat persönlich.




Bei Nichterfüllung dieser Sorgfaltspflicht drohen Reputations- und Haftungsschäden sowie hohe Bußgelder (§§ 30, 130 OWiG, § 93 Abs. 2 AktG, §§ 831, 823 ff., 31 BGB, § 43 Abs. 2 GmbHG). Die Haftung des Vorstandes erfolgt auch gegenüber dem Unternehmen.



Wird das nicht alles schon durch den
Abschlussprüfer oder die Interne
Revision geprüft?



Sicherheit durch bestehende Prüfinstanzen

	Jahresabschlussprüfer	Interne Revision	Ungeprüft bleiben....
	i. W. Risikofrüh- erkennung / bestandsgefährdende Risiken	i.W. Risikoinventuren und Bewertung der Risiken	<ul style="list-style-type: none"> • Risikoumfeld • Kontrollaktivitäten • Information und Kommunikation • Etc.
	Einzelne Kontrollen der Rechnungslegung	Ausgewählte Kontrollen/ Prozesse im Rahmen der Prüfungsplanung	<ul style="list-style-type: none"> • Kontrollumfeld • weite Teile des IKS außerhalb der Rechnungslegung • Etc.
	Verstöße bei Bekanntwerden im Rahmen der JAP	Verstöße sowie ausgewählte Kontrollen	<ul style="list-style-type: none"> • präventives CMS • sanktionierendes CMS
	Bei Verwertung von Arbeitsergebnissen der internen Revision	./.	<ul style="list-style-type: none"> • Prüfungsplanung • Jahresbericht • Qualität der Internen Revision

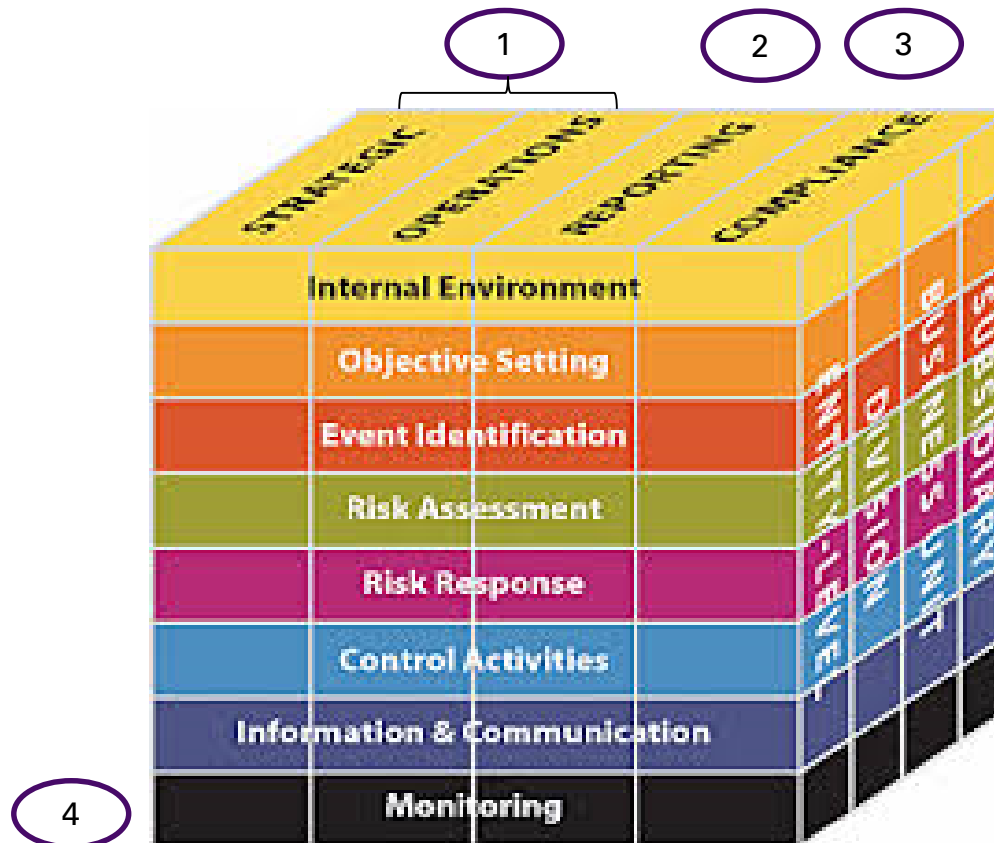


Welche Unterstützung bieten
Wirtschaftsprüfer für einen objektivierten
Nachweis der Erfüllung der
Überwachungspflichten?



Geltungsbereiche der neuen IDW Standards

Die Erarbeitung der Verlautbarungen erfolgten unter Zugrundelegung von COSO ERM (COSO II)



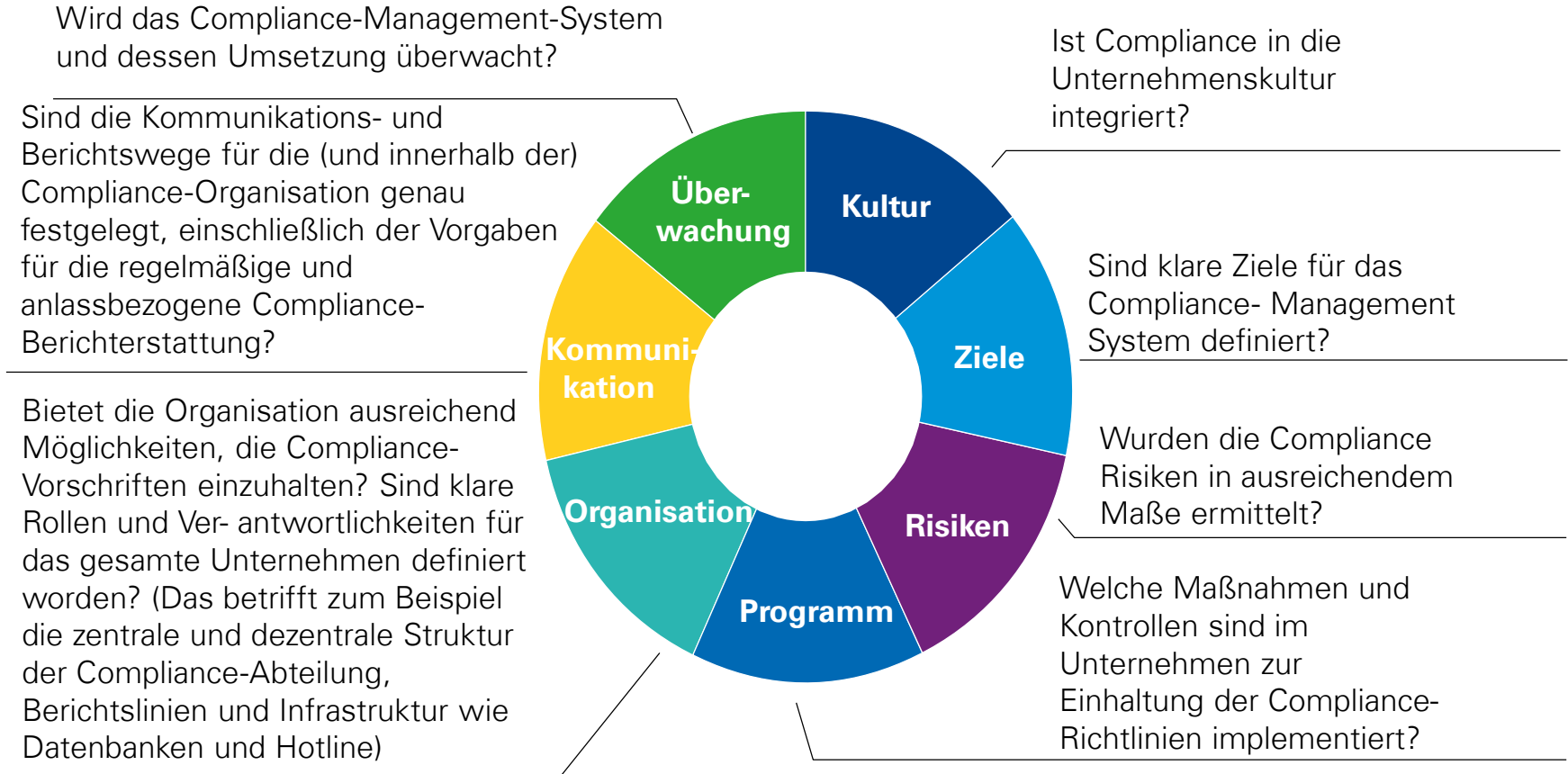
Gemeinsamkeiten der IDW-Prüfungsstandards

Wesentliche Übereinstimmungen auf einen Blick:

	PS 980 – CMS	PS 981 – RMS	PS 982 – IKS	PS 983 – IRS
Unterstützung der Unternehmensleitung durch den Wirtschaftsprüfer	Der Wirtschaftsprüfer kann mit der Prüfung einzelner oder aller vier Corporate Governance Elemente beauftragt werden. Ein effizienter und umfassender Wirksamkeitsnachweis für das ganze Unternehmen wird dabei idealerweise durch eine Verbindung der vier Prüfungen für die gesamte Corporate Governance erreicht.			
Gestaltung des Prüfungsumfangs	Prüfung auf der Grundlage einer formalen Systembeschreibung. Die Prüfungen können als Angemessenheitsprüfung (für einen Stichtag) oder Wirksamkeitsprüfung (für einen Zeitraum) ausgestaltet werden.			
Beispielhafte Möglichkeiten der Eingrenzung auf bestimmte Teilbereiche	Rechtsgebiete (z.B. Anti-Korruption), Gesellschaften, Geschäftseinheiten, Länder	Ausgewählte operative Risiken (z.B. Einkaufsrisiken), strategische Risiken	Geschäftsprozesse (z.B. der Einkaufsprozess)	N/A – Einhaltung internationaler IRS-Grundsätze insgesamt
Erstmalige Anwendung	Prüfungen seit dem 30. September 2011	Prüfungen, die nach dem 31. Dezember 2016 beauftragt werden. Eine freiwillige vorzeitige Anwendung ist jederzeit möglich.		

Prüfung des Compliance Management Systems - PS 980

Grundelemente eines Compliance-Management-Systems nach IDW PS 980



Prüfung des Risikomanagements – EPS 981

Einheitliche Ausgestaltung eines RMS anhand von acht Grundelementen

Regelmäßige Überwachung der prozessimmanenten Kontrollen (zum Beispiel durch die Interne Revision)

Einstellung und Verhalten aller Mitarbeiter im Unternehmen beim Umgang mit Risiken

Berichtspflichten und -wege zur Kommunikation von Risiken an die zuständigen Stellen im Unternehmen

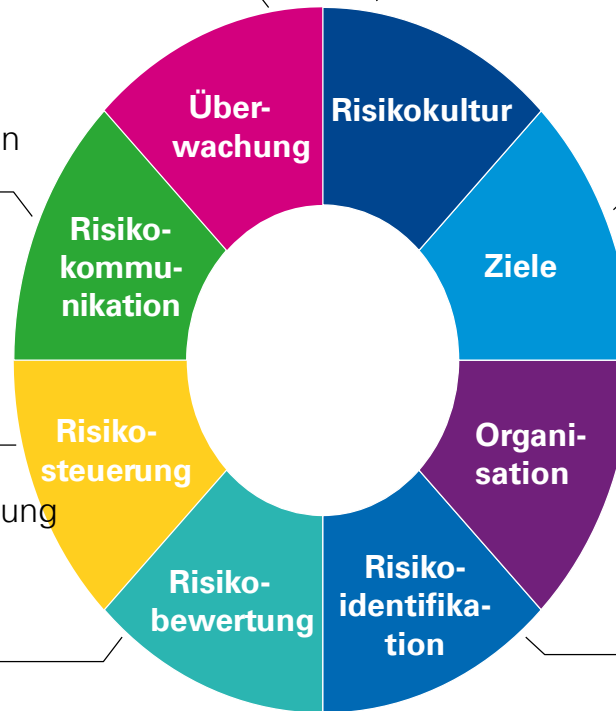
Risikostrategie einschließlich Risikoappetit und -toleranz

Maßnahmen und Kontrollen zur Vermeidung, Reduktion, Teilung und Akzeptanz von Risiken

Transparente, eindeutige Verantwortungsbereiche und Rollen

Quantitative und qualitative Bewertung der Risiken sowie Aggregation der Einzelrisiken

Systematische Analyse der Risikoursachen und Frühwarnindikatoren



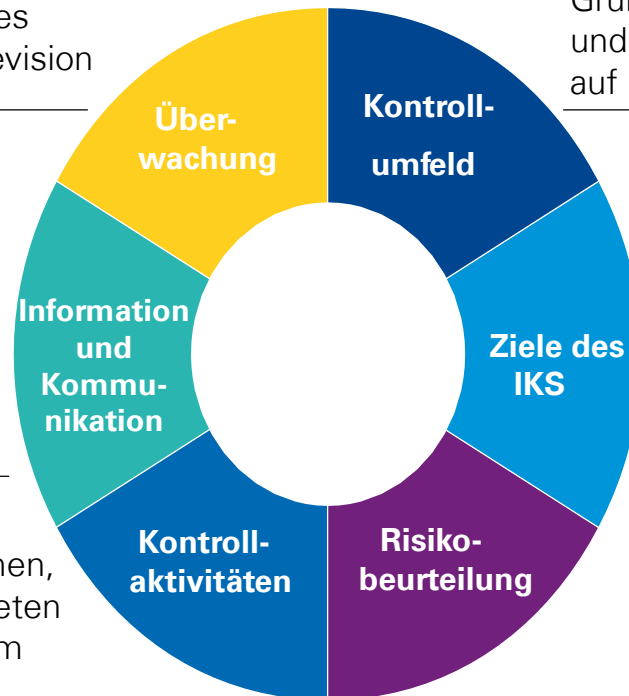
Prüfung des Internen Kontrollsystems – EPS 982

Grundelemente des IKS gemäß IDW EPS 982

Objektive Beurteilung der Wirksamkeit des IKS zum Beispiel durch prozessunabhängige Mitarbeiter des Unternehmens oder die Interne Revision

Angemessener Informationsfluss im IKS, um erforderliche Informationen in pass- genauer Form sowie adressatengerecht weiterzuleiten (beispielsweise mittels Schulungen oder Richtlinien)

Steuerungs- und Kontrollmaßnahmen, um den identifizierten und bewerteten Risiken adäquat zu begegnen – zum Beispiel Funktionstrennungen, 4-Augen-Prinzip oder IT-Berechtigungskonzepte



Grundeinstellung, Problembewusstsein und Verhalten der Mitarbeiter in Bezug auf das IKS

Anforderungen an die Unternehmensberichterstattung, abgeleitet aus den Informationsbedürfnissen in Bezug auf entscheidungsrelevante Informationen

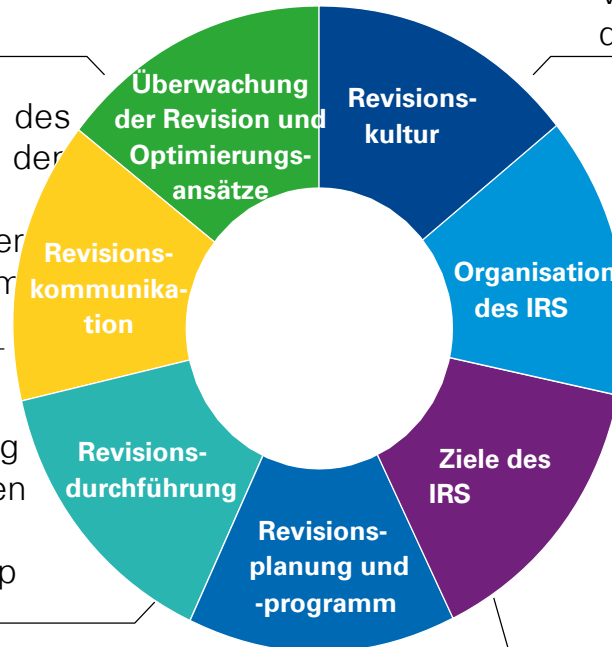
Identifikation und Bewertung von Risiken, die den Prozessablauf zur Erstellung der Unternehmensberichterstattung sowie das Erreichen der IKS-Ziele gefährden

Prüfung der **Internen Revision** – EPS 983

- Kontinuierlicher Verbesserungsprozess, verbunden mit internen und externen Qualitätsprüfungen
- Feedback-Gespräche

- Grundeinstellung des Managements und des Aufsichtsrats/Prüfungsausschusses zur Notwendigkeit einer Internen Revision
- Verabschiedung von Regelungen durch die Geschäftsführung

- Kommunikation innerhalb des Prüfungsteams sowie mit den relevanten Stakeholdern
- Interne Revision in den Verteilungswesentlichen Unternehmen Informationen aufnehmen



- Rollendefinition, Bestimmung der Verantwortlichkeiten und Bereitstellung der erforderlichen Ressourcen durch das Management
- Verbindliche schriftliche Revisionsrichtlinien

- Vor- und Nachbereitung der Prüfung unter Festlegung von Meilensteinen und Prüfungsdauer, Definition der Prüfungshandlungen und Follow-up

- Definition und Festlegung des Audit Universe (Prüfgebiete und -felder)
- Hierzu zählt auch die Beurteilung der Wirksamkeit der Maßnahmen zur Aufdeckung von dolosen Handlungen

- Risikoorientierte Gesamtplanung auf Basis des Audit Universe sowie der identifizierten und bewerteten Risiken
- Jährliche systematische Planung der Prüfungen

Ihre Ansprechpartner

Jens C. Laue

Partner

Head of Governance & Assurance Services

T +49 211 475-7901

jlaue@kpmg.com

KPMG AG

Wirtschaftsprüfungsgesellschaft

Tersteegenstr. 19-21

40474 Düsseldorf



www.kpmg.de/socialmedia

www.kpmg.de

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.

© 2016 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.