SCHAEFFLER

Aufbau eines Compliance Management Systems (CMS) in der Praxis

Eric Soong | Chief Compliance Officer | Schaeffler Group

Agenda

SCHAEFFLER

1 Schaeffler – Ein weltweit führendes Technologieunternehmen

2 Fachexpertise in einer Compliance Abteilung

3 Orientierung beim Aufbau eines Compliance Management System (CMS)

4 Das Compliance Management System (CMS): Prävention – Detektion – Reaktion

5 GRC Board als Lösungsansatz für ein ganzheitliches Compliance

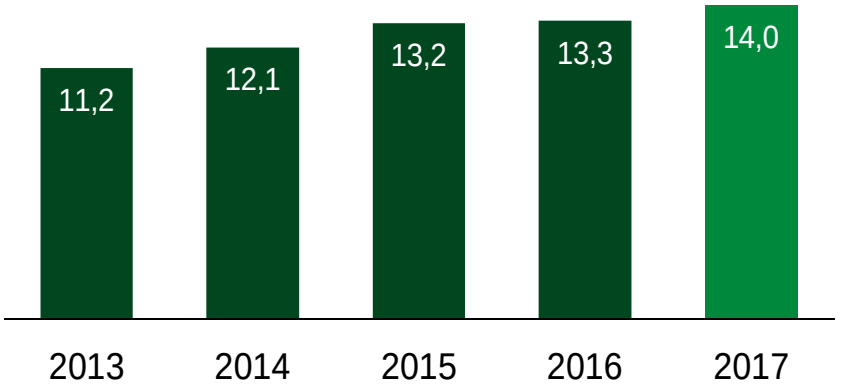
Schaeffler – Ein weltweit führendes Technologieunternehmen

SCHAEFFLER

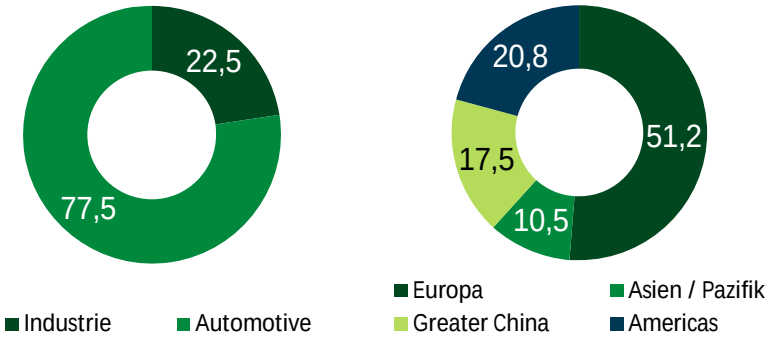
Überblick

- Integrierter Automobil- und Industriezulieferer
- Rund 92.000 Mitarbeiter in über 50 Ländern
- Überdurchschnittliches Umsatzwachstum und Profitabilität

Kontinuierliches Umsatzwachstum (in EUR Mrd.)



Umsatz nach Sparte und Region 2017 (in %)



EUROPA: Inkl. Deutschland, West-, Süd- und Ost-Europa, Mittlerer Osten, Afrika, Russland und Indien

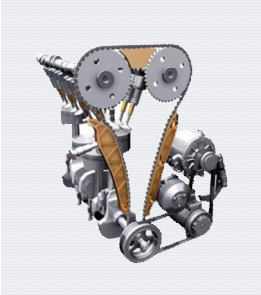
Weltweit

	#Werke	#F&E-Zentren
Europa	45	10
Americas	14	5
Greater China	8	1
Asien / Pazifik	5	2
Total	72	18

Drei Sparten – Automotive OEM, Automotive Aftermarket und Industrie

SCHAEFFLER

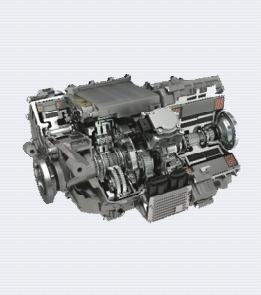
Automotive OEM (Systeme)



Motorsysteme

Getriebesysteme

Fahrwerksysteme



Hybride und elektrische Antriebssysteme

Automotive Aftermarket (Segmente)

Pkw

Leichte Nutzfahrzeuge

Schwere Nutzfahrzeuge

Traktoren & Landmaschinen

Services

Industrie (Sektorencluster)

Wind

Raw Materials

Aerospace

Railway

Offroad

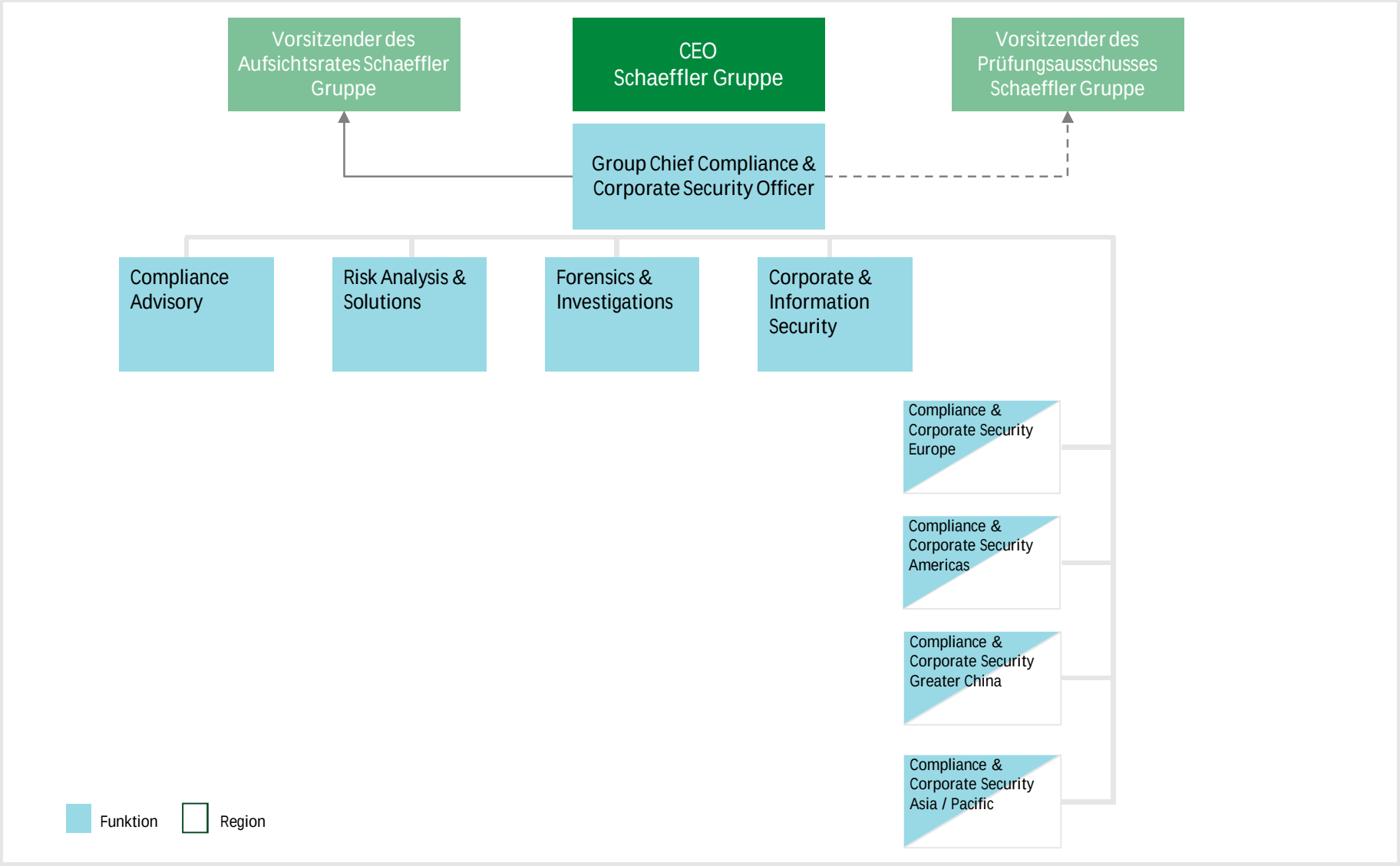
Two Wheelers

Power Transmission

Industrial Automation

Globale Compliance Organisation

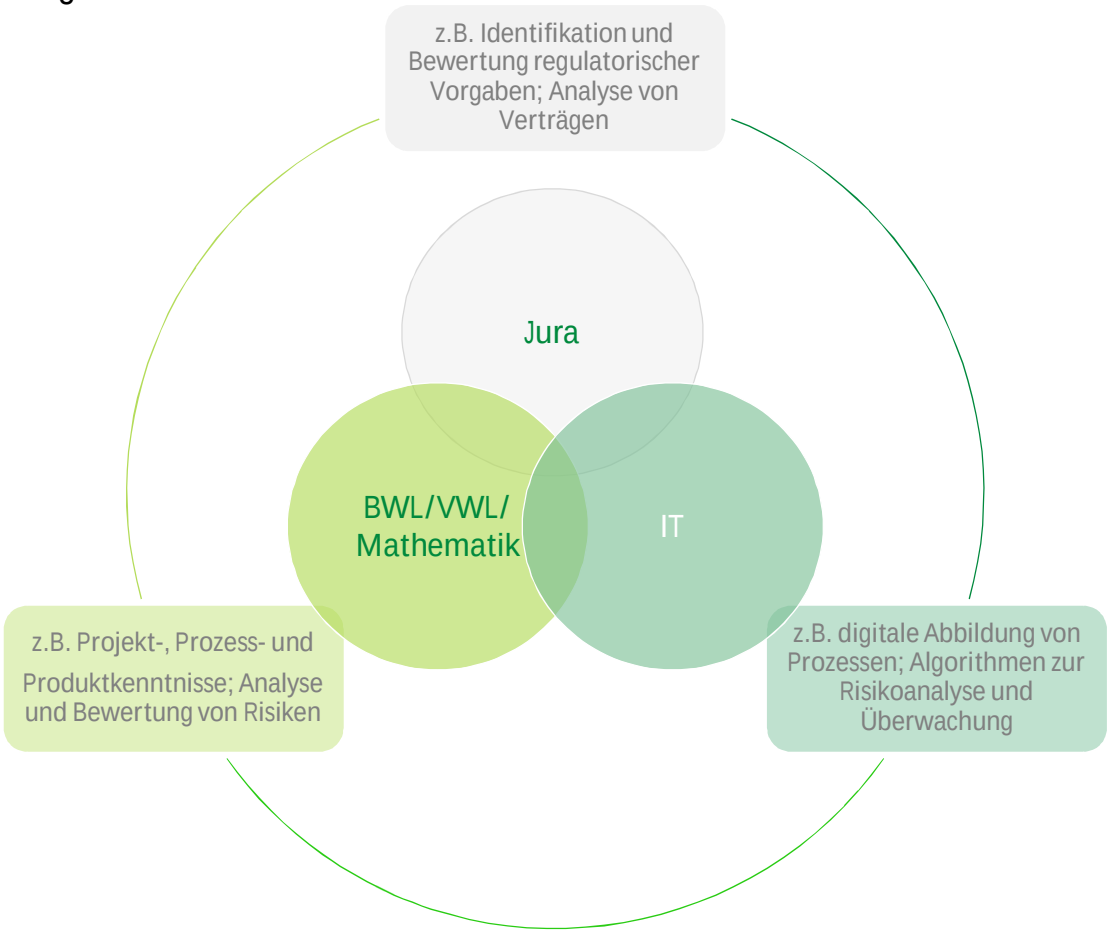
SCHAEFFLER



Fachexpertise in einer Compliance Abteilung

SCHAEFFLER

Praxisbewährter Dreiklang



Laufend veränderte Anforderungen → permanenter interdisziplinärer Austausch im Compliance Alltag

Rechtliche Grundlagen

SCHAEFFLER

Persönliche Verpflichtung des Vorstands und des Aufsichtsrats nach deutschem Recht

- §§ 91(2) AktG
  Pflicht der Geschäftsführung, ein Kontrollsystem einzuführen
- §§ 43 GmbHG, 93 (1) AktG
  Sorgfaltspflicht der Geschäftsführung
- § 116 AktG
  Sorgfaltspflicht und Verantwortlichkeit der Aufsichtsratsmitglieder
- §§ 30, 130 OWiG
  Ordnungswidrigkeit bei der Verletzung von Aufsichtsmaßnahmen.

Foreign Corrupt Practices Act (FCPA)

- Reguliert die Bestechung und Bestechlichkeit von Amtsträgern sowie Beschleunigungszahlungen und gilt für alle Personen mit einer engeren Verbindung zu den USA.
- Individualstrafen bis 5 Mio. $ oder 20 Jahre Gefängnis, Unternehmen können auf bis zu 25 Mio. $ verklagt werden.
- Durch Anwendung des Alternative Fines Act auch noch viel höhere Strafen möglich.

UK Bribery Act

- Stellt sowohl Bestechung als auch die Nicht-Verhinderung von Bestechung durch Unternehmen unter Strafe.
- Wird auf Einwohner, Menschen mit regelmäßigen Wohnsitz sowie auf Unternehmen mit Sitz UK, oder die Teile oder das komplette Business in UK durchführen, angewendet. Auch mit Unternehmen verbundene Personen sind erfasst.
- Mögliche Strafen: bis zu 10 Jahre Gefängnis für Einzelpersonen / unbegrenzte Unternehmensstrafen und Ausschluss von öffentlichen Ausschreibungen in der EU.
- 6 Prinzipien: Verhältnismäßigkeit, Top – Level Commitment, Risikobewertung, Due Diligence, Kommunikation & Training, Überwachung und Kontrolle

Rechtliche Grundlagen für Compliance in Deutschland

SCHAEFFLER

Kodifiziertes Recht:

- Keine standardisierte juristische Kodifizierung
- Spezifische Regularien in den einzelnen Gesetzestexten (AktG, GmbH, HGB, WpHG, etc.)

Gesetzliche Bestimmungen für die Schaeffler Gruppe

- §91 (2) AktG

  Einführung geeigneter Maßnahmen, insbesondere ein gruppenweites Überwachungssystem.

- § 93 AktG

  Vorstandsmitglieder mit der Pflicht zur Anwendung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters.

- § 161 (1) AktG

  Erklärung, dass den Empfehlungen aus dem Deutschen Corporate Governance Kodex (DCGK) entsprochen wurde oder welche Empfehlungen nicht angewandt wurden und wieso.

- § 289a (1) HGB

  Pflicht zur Erklärung zur Unternehmensführung

- Ziffer 4.1.3. DCGK

  Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).

Orientierung beim Aufbau eines CMS

SCHAEFFLER

MaComp

- Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzpflichten
  - aktualisierte Fassung vom 19. April 2018, §§ 63 ff WpHG
  - Erstmalige Fassung vom 7. Juni 2010
  - Übernahme von geeigneten Elementen aus der MaComp

IDW PS980

- Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen
  - Detaillierte Übersicht der Anforderungen an ein CMS
  - Grundlagen der möglichen Prüfung (Konzeption, Angemessenheit, Wirksamkeit)

Weitere Voraussetzungen

- ISO 19600 - Richtlinie für den Einsatz von CMS
- Business Best Practices
- Stakeholder Expectation (bspw. Kunden, Versicherer, Investoren oder Shareholder)

Grundsätze und Maßnahmen, die auf den von gesetz. Vertretern festgelegten Zielen basieren und ein regelkonformes Verhalten der Schaeffler AG sicherstellen sollen

Inhalte eines CMS nach IDW PS 980

SCHAEFFLER

Grundelemente

Kultur

im Wesentlichen bestimmt durch:

- gelebten Wertekanon des Unternehmens und seiner Mitarbeiter.
- Grundeinstellungen und Verhaltensweisen des Managements („*Tone from the top*“)
- gesellschaftlichen Kontext des Interaktionsraums des Unternehmen.

Ziele

Festlegung wesentlicher Ziele, die mit Compliance erreicht werden sollen.

in Übereinstimmung mit den allgemeinen Unternehmenszielen insbesondere:

- Abgrenzung der Teilbereiche.
- Abgrenzung der in den Teilbereichen zu beachtenden Regeln.

Risiken

- Identifikation und Beurteilung von Compliance- Risiken (Grundlage für die Entwicklung eines angemessenen Compliance-Systems).
- Systematische Risikoanalyse und Risikobeurteilung.

Programm

- Auf Grundlage der abgeleiteten Risiken Definition und Einführung von risikomitigierenden Grundsätzen und Maßnahmen zur Verhinderung von Regelverstößen („*Prävention*“ und „*Reaktion*“).

Orga-nisation

- angemessene und klare Organisation
- Rollen und Verantwortlich-keiten
- Ressourcenplanung

Kommuni-kation

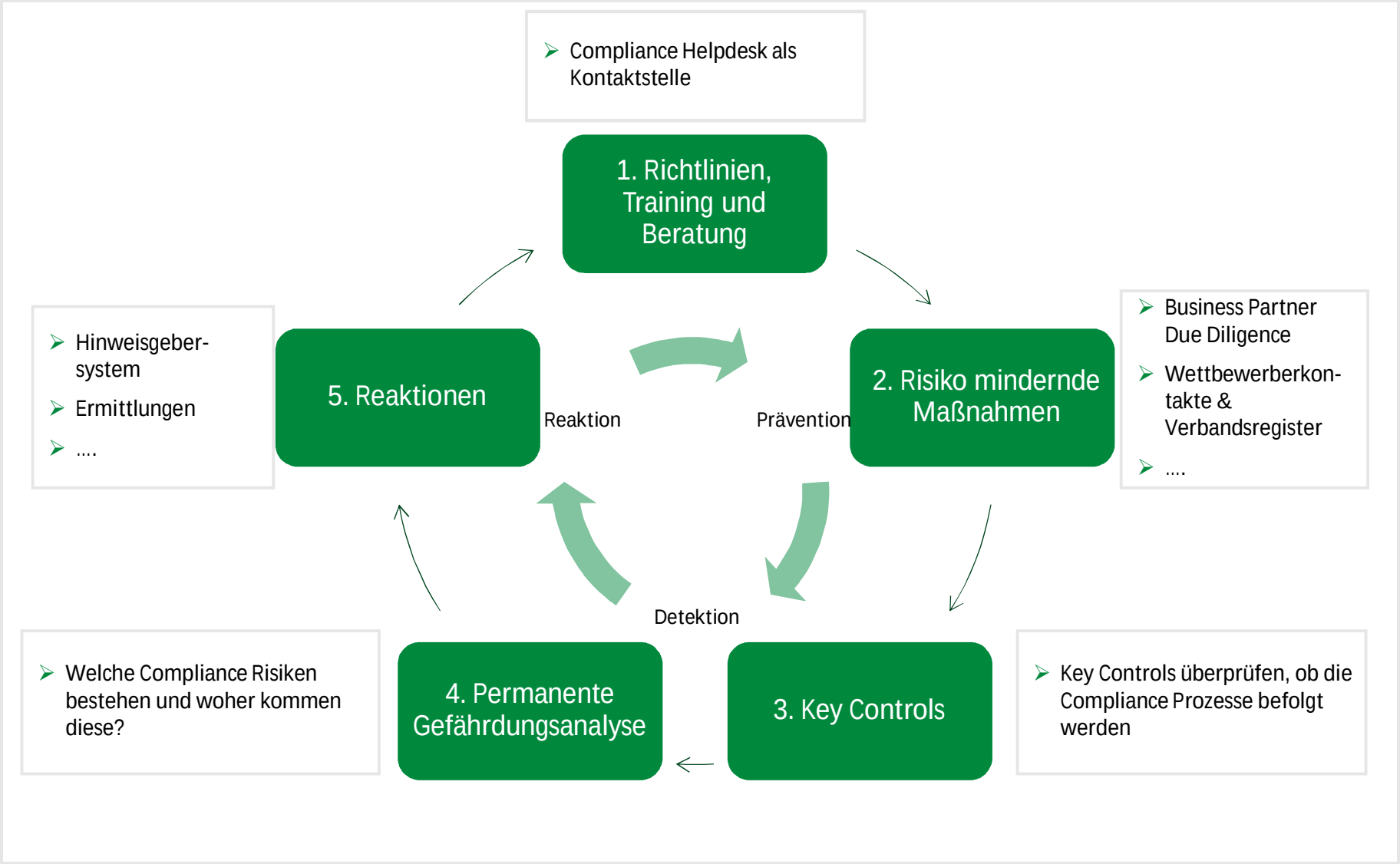
- ausreichende Information der betroffenen Mitarbeiter und ggf. Dritten über Programm und Organisation, insb. Rollen / Verantwortlich-keiten
- Definition eines Berichtsweges für identifizierte Risiken, Findings sowie eingehende Hinweise
- Schaffung des Bewusstseins für die Bedeutung der Kommunikation.

Überwachung/ Verbesserung

- durch prozess-unabhängige Stellen (z. B. Interne Revision, unabhängige Dritte).
- Untersuchung der Ergebnisse auf Schwachstellen und ggf. Ableitung von Maßnahmen.
- Überprüfung der Angemessenheit und Wirksamkeit (inkl. Reporting) → Grundlage: ausreichende Dokumentation
- Verantwortung des Managements

Good Governance in Compliance Prozessen

SCHAEFFLER



Das CMS: Prävention - Detektion - Reaktion

SCHAEFFLER

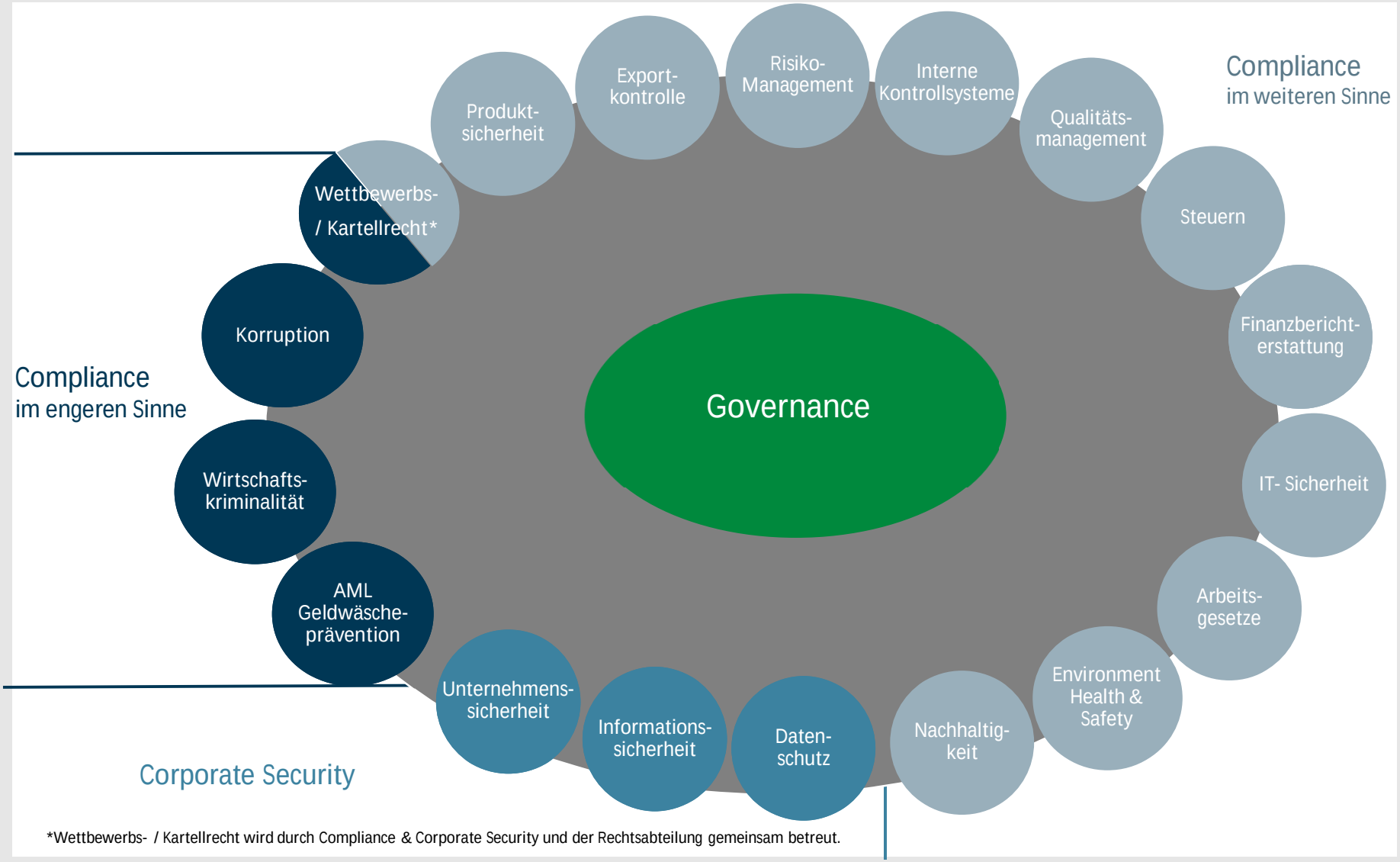
Tone from the top

Prävention	Detektion	Reaktion
• Kultur & Bewusstsein • Gefährdungsanalyse & Maßnahmen • Richtlinien & Prozesse • Training • Beratung & Unterstützung	• Hinweisgebersystem • Überprüfungen & Kontrollen • Due Diligence für Geschäftspartner	• Untersuchungen • Sanktionen • Ursachenanalyse • Verbesserungen

Weltweite Abdeckung

Governance-Themenfelder

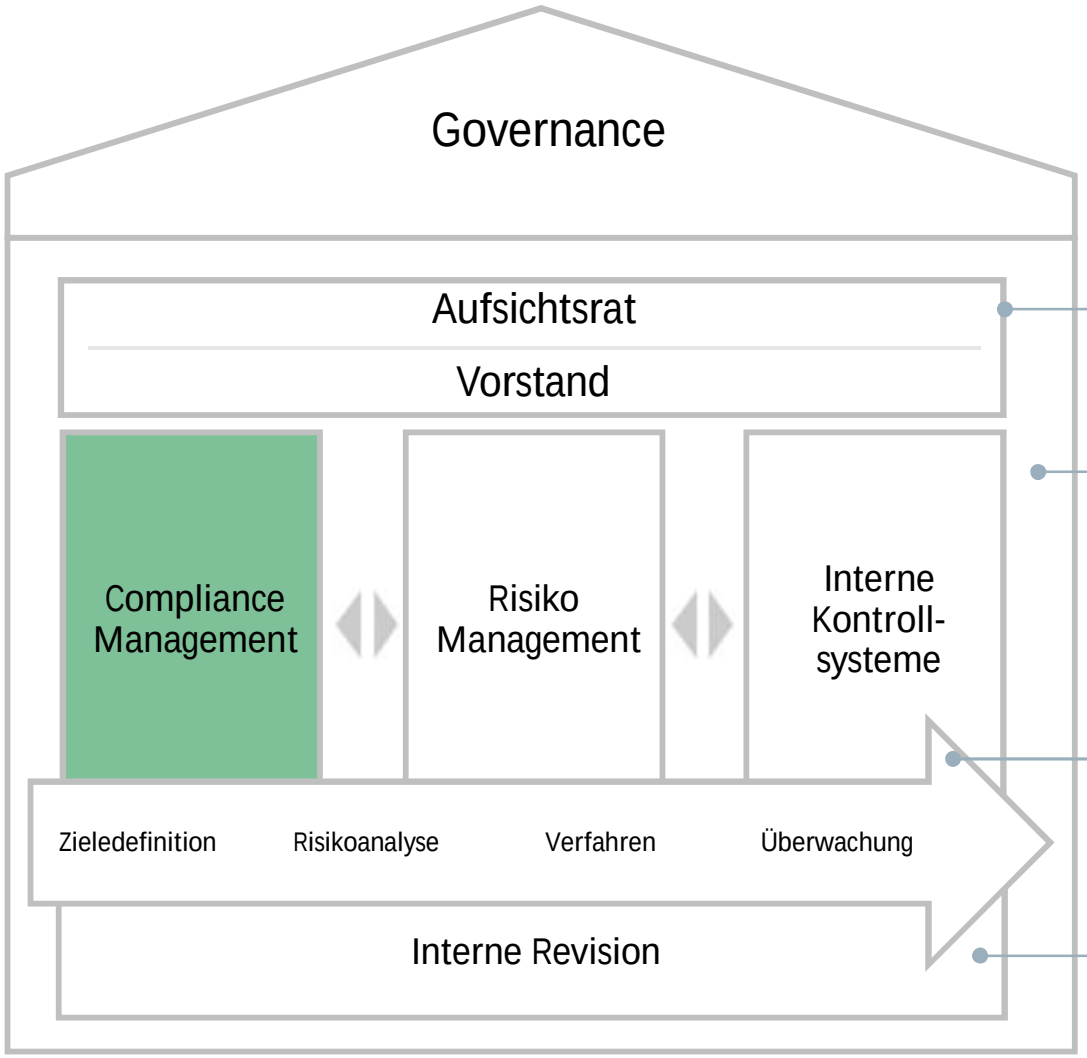
SCHAEFFLER



*Wettbewerbs- / Kartellrecht wird durch Compliance & Corporate Security und der Rechtsabteilung gemeinsam betreut.

Compliance ist Teil des Governance-Modells

SCHAEFFLER



Aufsichtsrat und Vorstand sind verantwortlich für die Etablierung von Corporate Governance Maßnahmen und die Sicherstellung von Compliance im Unternehmen.

Compliance Management, Risiko Management und das Interne Kontrollsystem dienen zur Identifizierung und Handhabung der Unternehmensrisiken.

Koordination & Kooperation
Zwischen den Funktionen ist enge Abstimmung für ein effizientes und koordiniertes Vorgehen erforderlich.

Interne Revision
Die interne Revision gewährleistet eine unabhängige Prüfung zur Effektivität der eingeleiteten Maßnahmen.

Governance, Risk & Compliance (GRC)

SCHAEFFLER

- Ein GRC umfasst die drei wichtigsten Handlungsfelder für eine erfolgreiche und integre Unternehmensführung
  - Governance
  - Risiko Management
  - Compliance

  →
  - geordnete Steuerungs- und Regelungsmechanismen in der Organisation
  - Maßnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken
  - Einhaltung von Gesetzen und Richtlinien
- Governance, Risk & Compliance (GRC) bezeichnet dabei die kontinuierliche, gesamthafte Betrachtung aller Funktionen einer Organisation um rechtliche, finanzielle und Reputationsrisiken effektiv zu steuern.
- Nur durch ein intensives Zusammenspiel dieser drei Funktionen lässt sich sicherstellen, dass Unternehmen in einem komplexen, globalen Geschäftsfeld auf auftretende Risiken und Herausforderungen entsprechend reagieren kann und das unternehmerische Handeln stets im Einklang mit bestehenden und zukünftigen Regularien ist.
- Dementsprechend sollten GRC Systeme darauf konzipiert werden, dass GRC-Bereiche wie Risikomanagement, Interne Kontrolle, Compliance und Internes Audit effizient und wirksam arbeiten und rasch auf verändernde Geschäftsanforderungen und Situationen reagieren können.
- Das Heben von Synergien durch gemeinsame, integrierte Prozesse ist entscheidend, um die Bildung von Insellösungen zu vermeiden, erhöht die Qualität und Effizienz und steigert die Transparenz sowie die Sicherheit über die Steuerungs- und Kontrollmechanismen im Unternehmen.

Three Lines of Defense

SCHAEFFLER

Three Lines of Defense:

Die drei Ebenen definieren die Zusammenarbeit zwischen der operativen Ebene, der Überwachungsfunktion (Compliance / Risiko Management) und der unabhängigen Prüfung (Interne Revision).

1. Level

Operative Ebene

Interne Kontrollsysteme innerhalb der operativen Einheiten wie zum Beispiel Produktion & Vertrieb

- Risiken Identifizieren und bewerten
- Durchführung von Kontrollen
- Risikowirksame Änderungen im Geschäftsumfeld erkennen und kommunizieren

2. Level

Kontrollebene

Compliance Management System

Risiko Management System

- Strategisches Risiko Management
- Anweisungen und Richtlinien definieren und implementieren
- Überwachung der Einhaltung

3. Level

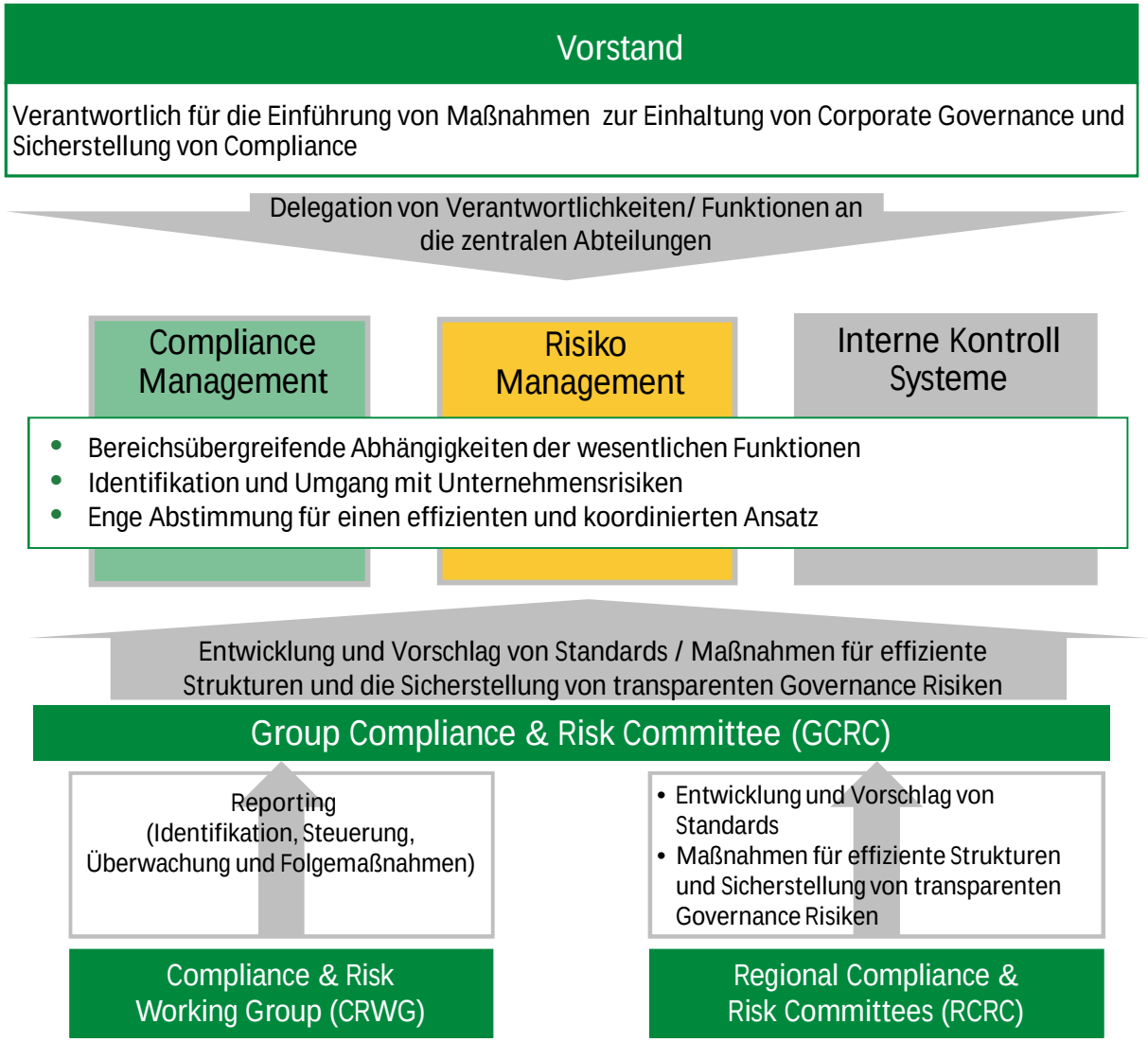
Prüfung

Interne Revision

- Unabhängige Prüfung
- Evaluieren der Effektivität
- Identifizieren von Verbesserungen für die Kontrollfunktionen

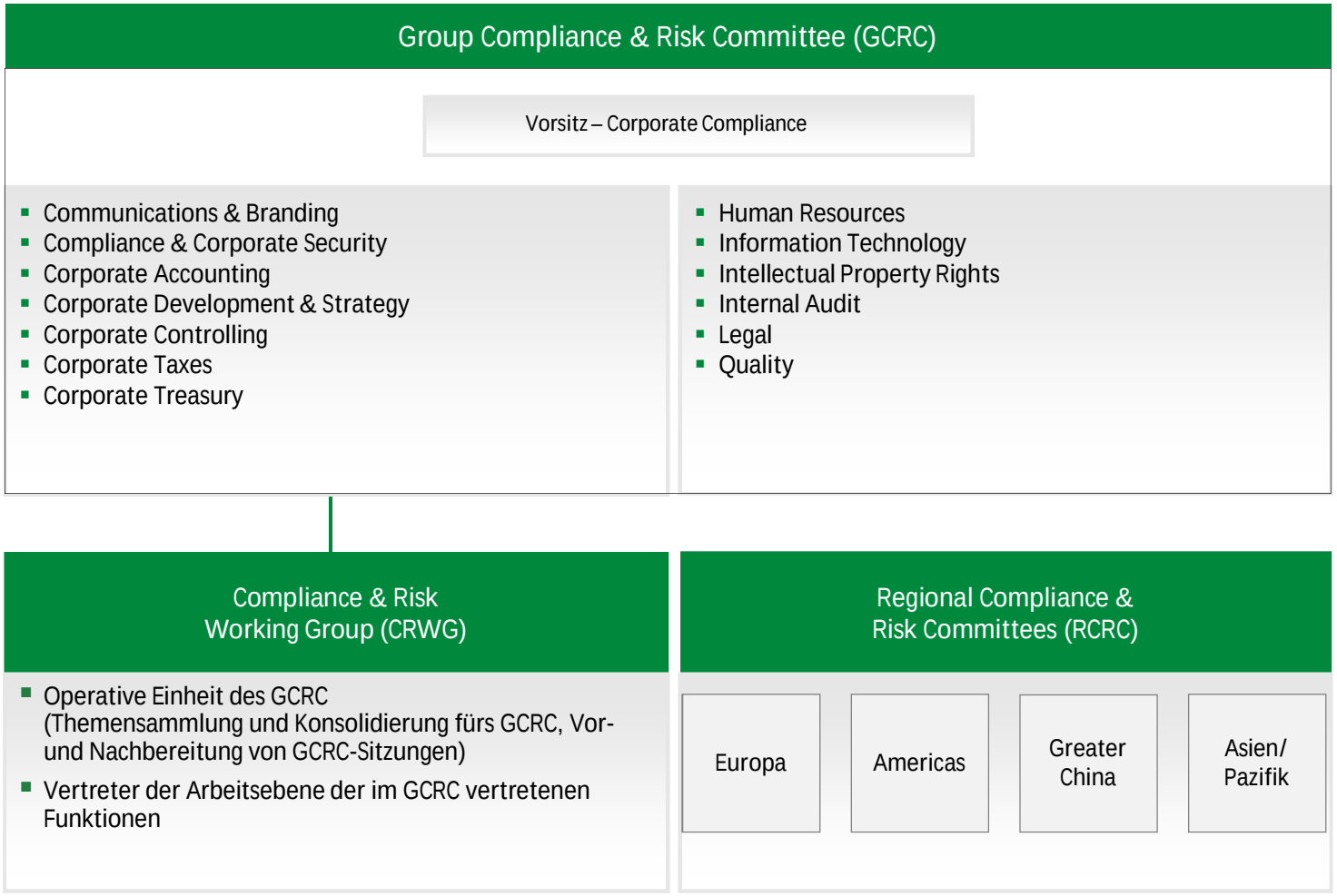
Group Compliance & Risk Committee (GCRC)

SCHAEFFLER



GCRC - Struktur

SCHAEFFLER



GCRC - Ziele

SCHAEFFLER

Ziele des GCRC:

- Das GCRC ist ein funktionsübergreifendes Komitee, dass auf die Wirksamkeit des Compliance-Managements, Risikomanagements und der Risikokontrolle in der Schaeffler Gruppe hinwirkt. Ziel des GCRC ist, den Vorstand beim weiteren Ausbau der einheitlichen und systematischen Risikosteuerung über alle Funktionen der Schaeffler Gruppe zu unterstützen.
- Das GCRC ...
  - ... soll für Transparenz sorgen und einen Überblick über alle Governance-Risiken der Schaeffler Gruppe schaffen.
  - ... setzt Standards für Maßnahmen zur Risikominderung.
  - ... zielt darauf ab, eine konsistente Risikolandschaft zu schaffen, um sicherzustellen, dass alle relevanten Risiken betrachtet wurden.
  - ... ist verantwortlich für die Initiierung und die Überwachung von Maßnahmen zur Prävention, Kontrolle, Minderung und/oder Eliminierung identifizierter Schwächen in Bezug auf Governance-Risiken.
- Weitere Ziele sind unter anderem das Setzen von Richtlinien, Standards und Methoden, die Einführung und Pflege des Kontrollrahmenwerkes und das Definieren von Maßnahmen sowie die Überwachung ihrer Umsetzung.

Schlüsselfaktoren

SCHAEFFLER

- Entscheidend für den Erfolg einer Compliance Organisation ist nicht nur die Aufbauorganisation sondern gerade auch die Ablauforganisation, also die Integration von Compliance in die regulären Geschäftsprozesse
- Compliance viel mehr als nur Regelwerk und „*Kontrolleure*" – Compliance ist Grundlage und Ausgangsbasis für jegliches nachhaltiges und integres Wirtschaften
- Eine unabhängige und exponierte Einordnung innerhalb der Organisationsstruktur (eigene Abteilung, direktes Reporting zum Vorstand) eines Unternehmens ist zwingend notwendig um effektive und funktionierende Compliance Tätigkeiten zu gewährleisten
- Die thematische Ausgestaltung ist, in bekannten Rahmen, für jedes Unternehmen individuell wählbar und sollte stets auf einer grundlegenden Risikoanalyse bestehen.
- Compliance Abteilungen sollten stets interdisziplinär aufgebaut sein, um alle Aspekte der Tätigkeit entsprechend abbilden zu können und dem Mantra der "*Integration in bestehende Geschäftsprozesse*" gerecht zu werden.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen und Diskussion

Eric S. Soong
Eric.Soong@schaeffler.com