Herzlich Willkommen
Compliance - Risikomanagement

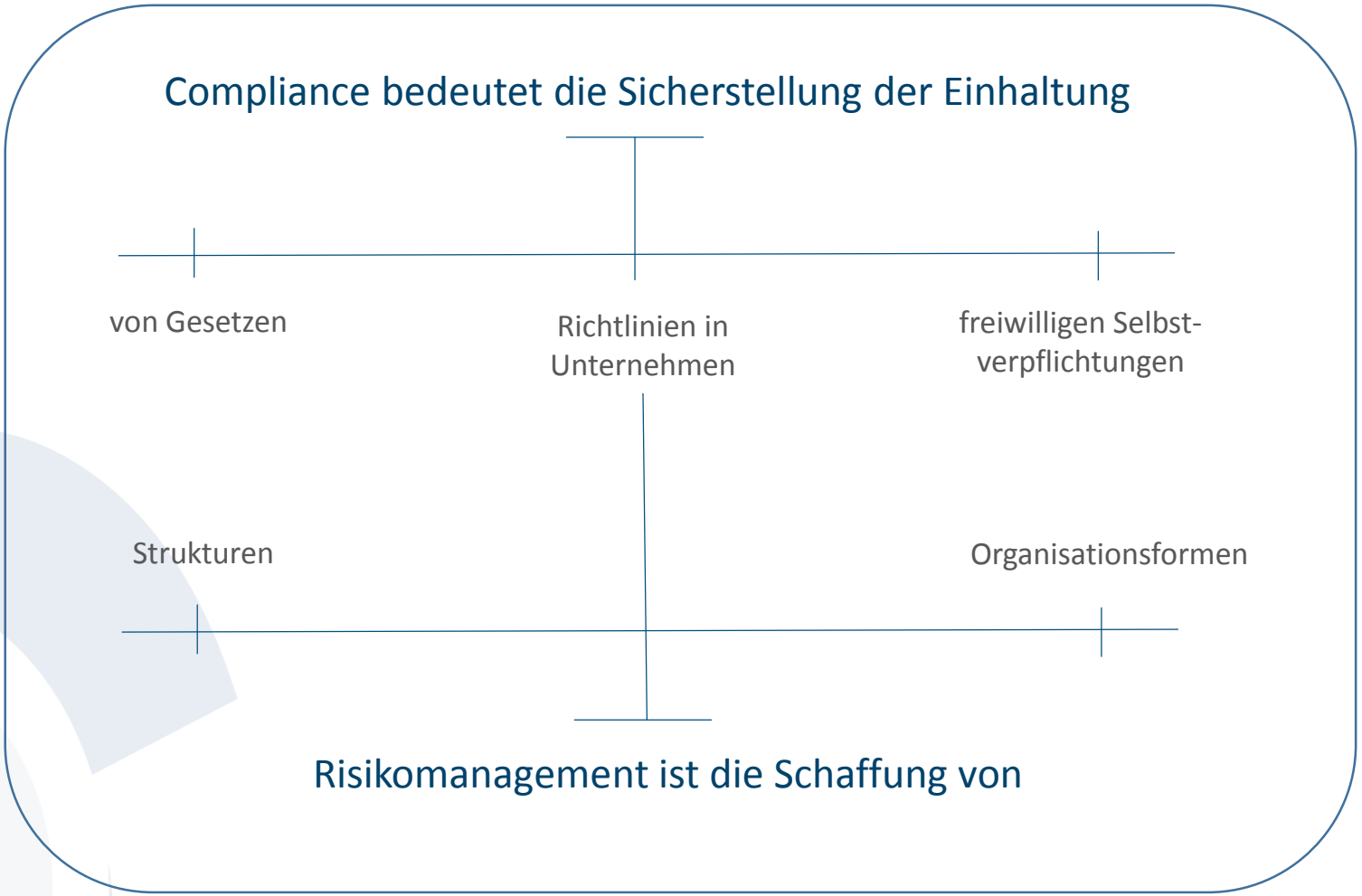
Agenda

- Management Alliance stellt sich vor
- Einführung in das Thema Compliance, Risikomanagement, IKS
- Der Blick in die Praxis
- Erfolgsfaktoren

Management Alliance stellt sich vor

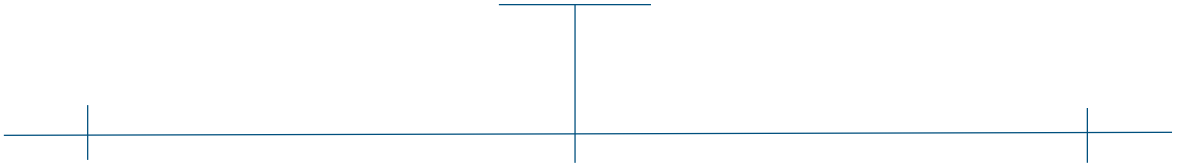
- Unternehmensberatung für Vorstände, Beiräte und Aufsichtsräte
- Zertifizierter Lehrgangsanbieter der Deutsche Börse AG zur „Qualifizierung von Aufsichtsräten“
- Servicedienstleister externer Aufsichtsratsbüro-, Compliance- und Risikomanagement - Dienstleistungen
- Erfahrenes Expertennetzwerk aus der Praxis für die Praxis
- Fachpartner des Arbeitskreises deutscher Aufsichtsräte - AdAR

Compliance und Risikomanagement greifen Hand in Hand



Auch die Rechtsgrundlagen beruhen auf den Vorgaben zum Risikomanagement

Compliance ist Bestandteil der gesetzlichen Vorgaben zur Risikoüberwachung

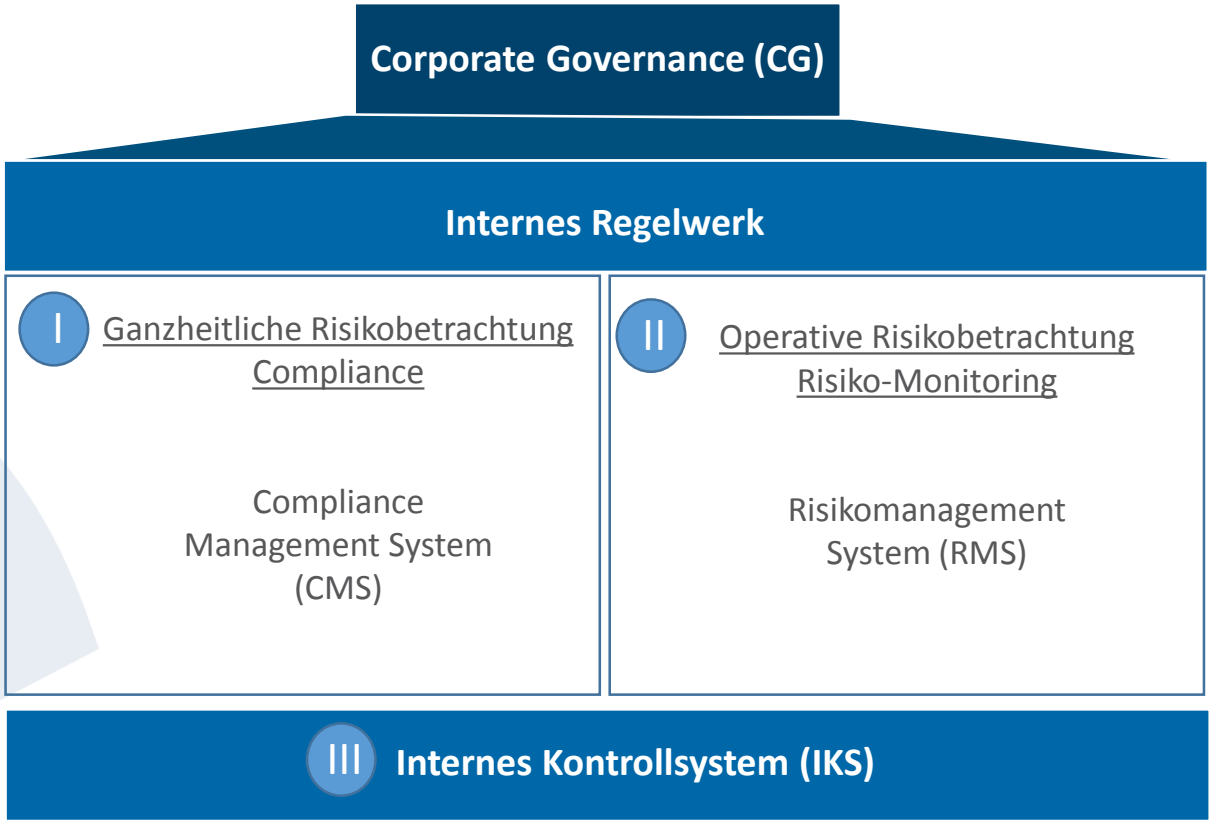


Pflicht die „Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“ (§43 Abs. 1 GmbHG; §93 Abs. 1 Satz 1 AktG.)

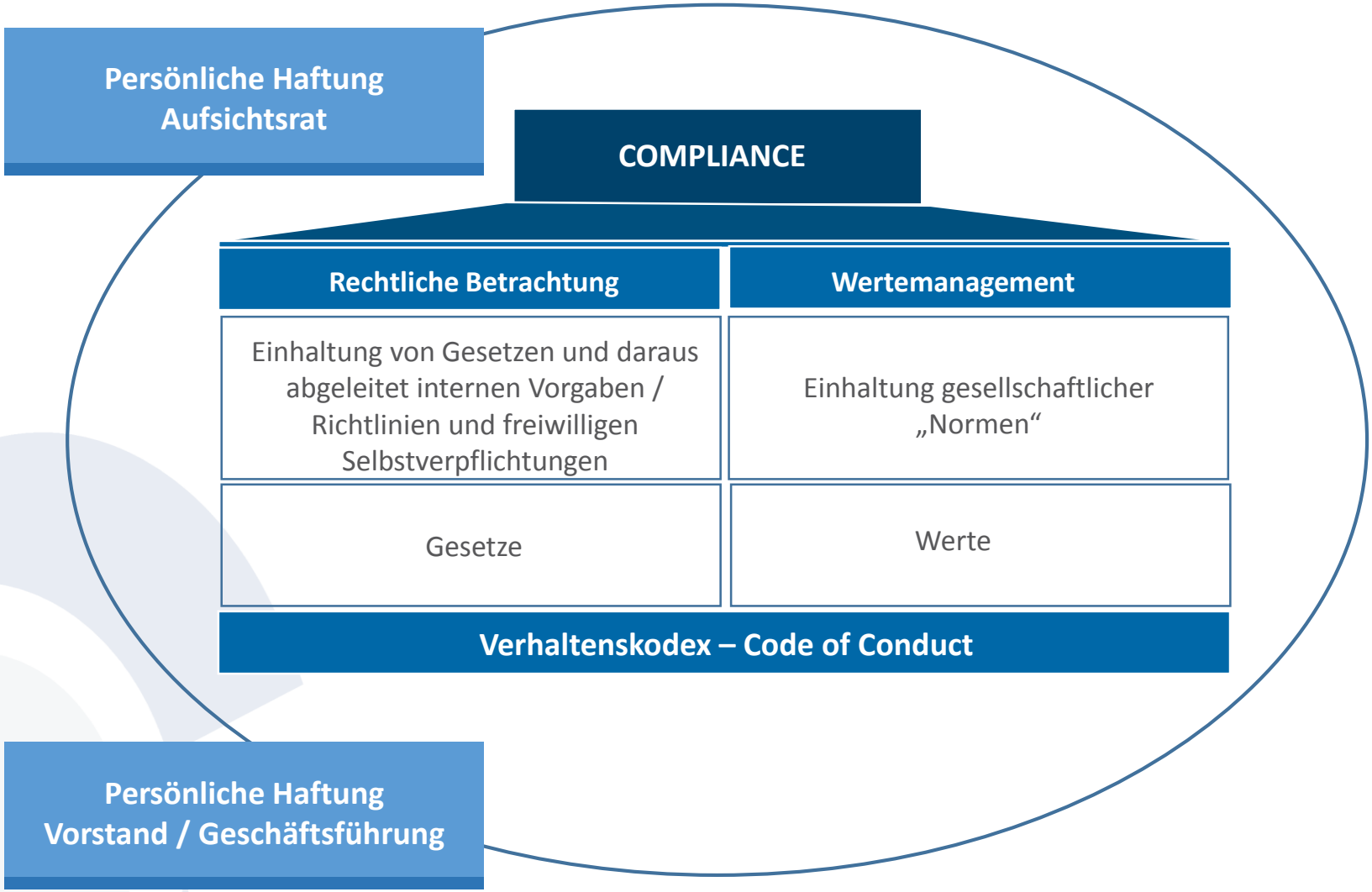
Verpflichtung des Vorstands zur Einrichtung eines Überwachungssystems, damit „den Fortbestand der Gesellschaft gefährdende Entwicklungen, früh erkannt werden“ (§91 Abs. 2 AktG.)

Business Judgement Rule: Keine Pflichtverletzung, wenn Entscheidung auf angemessener Information beruht (§93 Abs. 1 AktG.)

Risikomanagement und Compliance zwei Perspektiven zur Risikoprävention in der Unternehmensführung



I Compliance in der Theorie: Ein ganzheitliches Führungsinstrument



Was heißt das in der Praxis?

Gesetzliche Vorgaben

uneinheitlich und komplex

- Korruptionsgesetzgebung (UK-Gesetzgebung führend)
- Kartellrecht (deutsches Recht führend)
- Datenschutz
- Wirtschaftssanktionen (große Unterschiede zwischen USA und Europa)
- und vieles mehr

Ableitung interner Regeln aufgrund von Gesetzen

Individuell aus-zugestalten

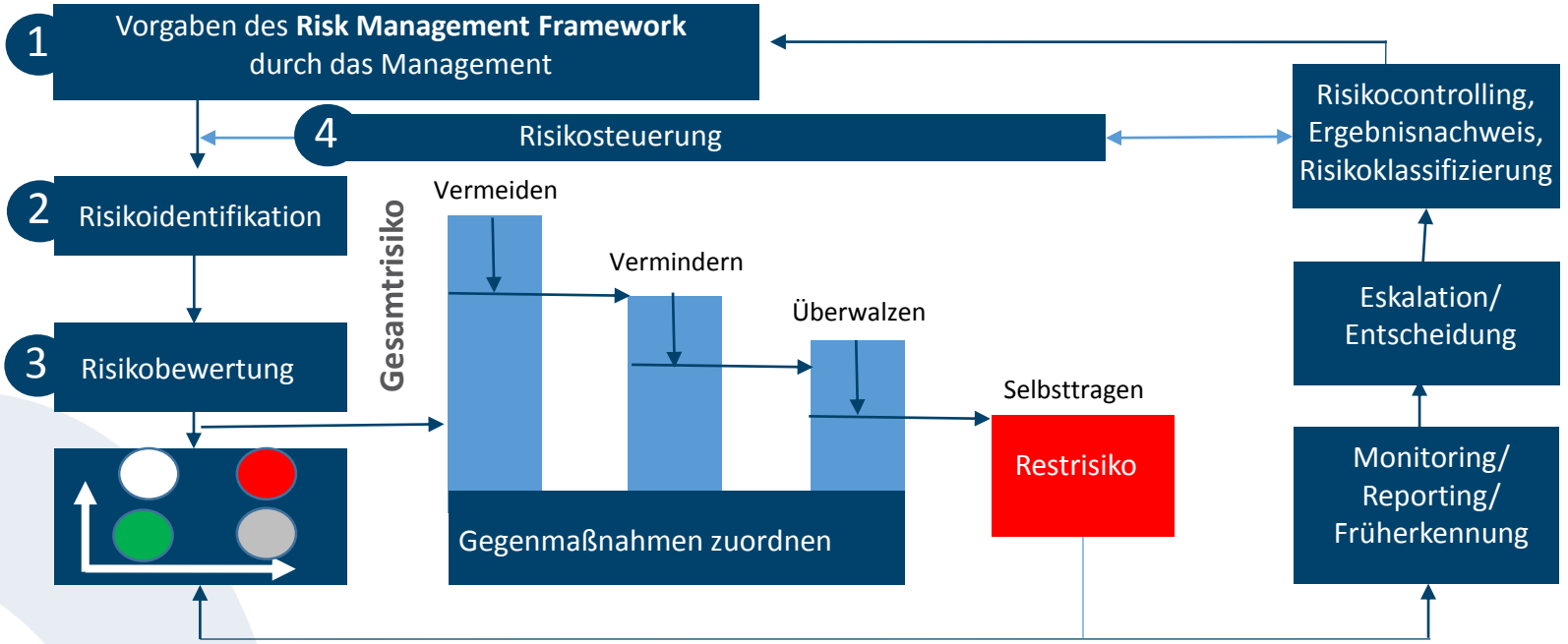
- Z.B. Einhaltung der gesetzlichen Anti-Terror-Vorgaben
- Z.B. Einhaltung Embargo-Richtlinien
- Z.B. Vermeidung / Verhinderung von Korruption
- Z.B. Einhaltung Kartellrecht
- Z.B. Einhaltung Datenschutz
- Z.B. Einhaltung Geschäftsethik
- und vieles mehr

Arbeitsanweisungen / internes Regelwerk

folgt operativem Handeln

- Z.B. 4-Augen Prinzip
- Z.B. Unterschriftenregelungen
- Z.B. Dienstwagenregelungen
- Z.B. Reiseverordnungen
- Z.B. Fachliche Arbeitsanweisungen (z.B. in der Produktion etc.)
- Z.B. Keine Diskriminierungen
- und vieles mehr

II Das Risikomanagementprinzip zur Prävention



Fazit: Jedes Risiko erfordert einen Risk Owner

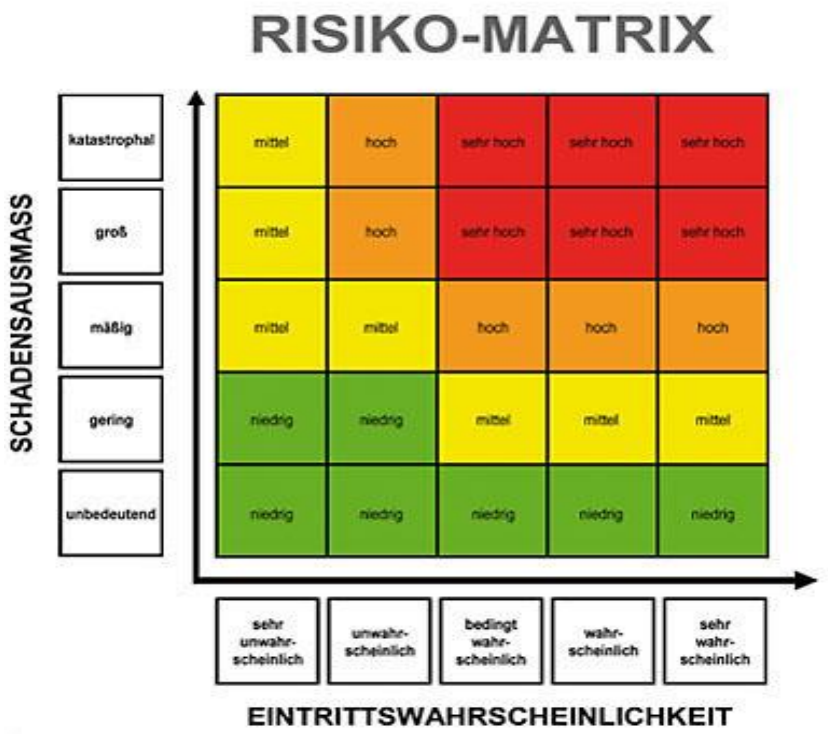
II Risikomanagement erfordert eine Einschätzung der Risiken und Ableitung der ertragsseitigen Auswirkungen

Der Zusammenhang zwischen Risiko und Rendite

- Risiko ist nicht gleich Risiko, denn
- Eintrittswahrscheinlichkeiten können variieren und
- Der Schadensausmaß durch Gegenmaßnahmen reduziert werden

Fazit: Die Nettobetrachtung, also Risiko nach Gegenmaßnahmen, ist für die Unternehmenssteuerung die relevante Kenngröße.

Risiko-Kontroll-Matrix (RKM) dient zur Veranschaulichung einzelner Risikoeinschätzungen

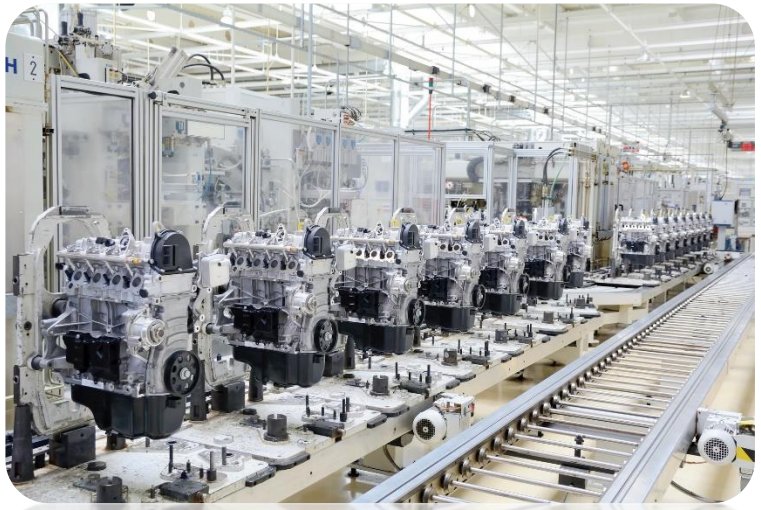


III IKS – Internes Kontrollsystem – dient zur Überwachung der Wirksamkeit und Effizienz von Prozessen

Manueller Prozess

- Menschenabhängig
- Fehleranfällig
- Zeitaufwändig

➢ Manuelle Kontrollen z. B. in Form von Belegprüfungen



Automatischer Prozess

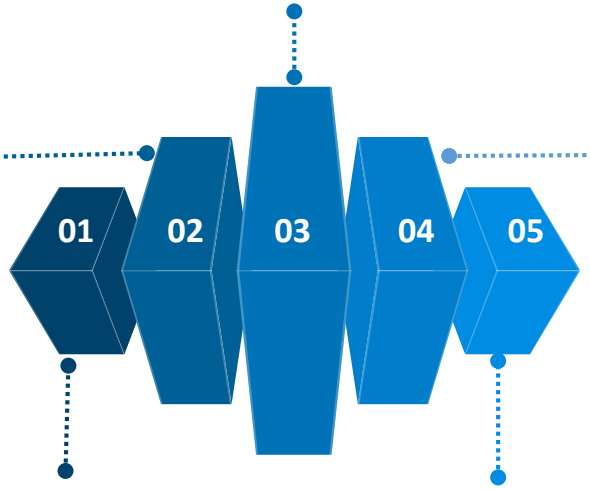
- Maschinengesteuert - Standards
- Geringe Fehlerquote
- Zeitoptimiert

➢ Systemkontrollen über Zugriffsrechte

III Das IKS-Konzept

IKS bietet eine **angemessene Sicherheit für die Geschäftsführung**.

IKS ist nur **dann wirksam**, wenn sich auch die **Mitarbeiter** mit den Zielen und Grundlagen **identifizieren.** IKS ist weit mehr als das bloße Einhalten von Richtlinien und Ausfüllen von Formblättern.



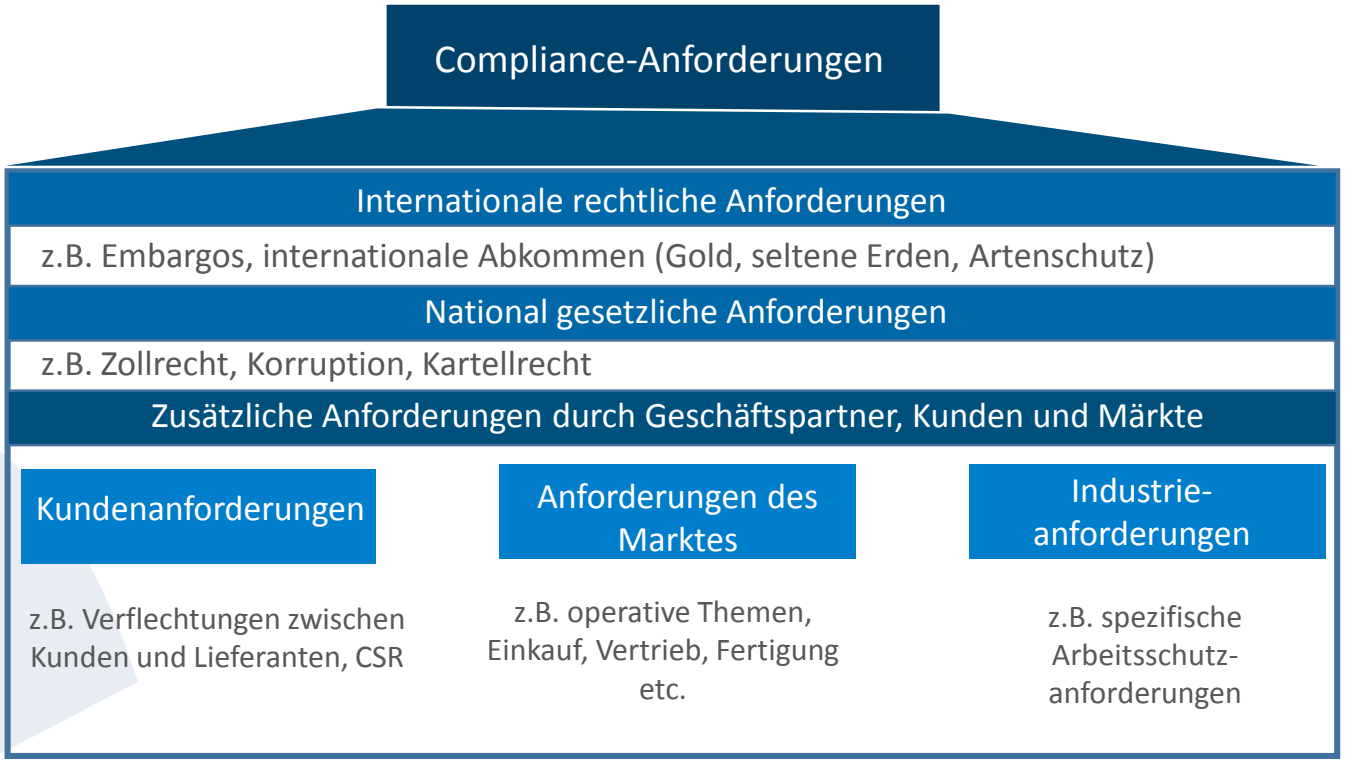
IKS ist darauf **ausgerichtet, Unternehmensziele** unter Einbindung unterschiedlicher Fachbereiche **zu erreichen**.

IKS ist ein laufender Prozess, der fest in den betrieblichen Alltag zu integrieren ist.

IKS **ist ein** wesentliches **Element**, um die **gesetzlichen Anforderungen** an die Geschäftsleitung **zur Risikoüberwachung zu** erfüllen.

Der Blick in die Praxis

Operative Herausforderungen nehmen stetig zu



Quelle: COMFORMIS GmbH und eigene Darstellung

Kundenanforderungen

Die Verflechtungen zwischen Kunden und Lieferantenbeziehungen nehmen stetig zu

Ausgangslage

- Unternehmen aus der Maschinenbauindustrie, Komponentenhersteller, wird einem Compliance und Risikomanagement Audit von Liebherr unterzogen.
- Eckdaten:

  Umsatz 2016: 20 Millionen Euro
  EBIT-Marge: 10%
  Mitarbeiter: 150
  internationaler Vertrieb via Handelsvertreter

Kundenanforderungen

Rechtsgrundlagen für Business Partner Audits im Zuge des CSR-Richtlinien-Umsetzungsgesetzes verschärft

Liebherr berief sich auf die Dokumentationspflichten im Rahmen der CSR-Gesetzgebung

- Gesetzliche Berichtspflicht betreffen nur Kreditinstitute, Versicherungen und börsennotierte Unternehmen *, aber

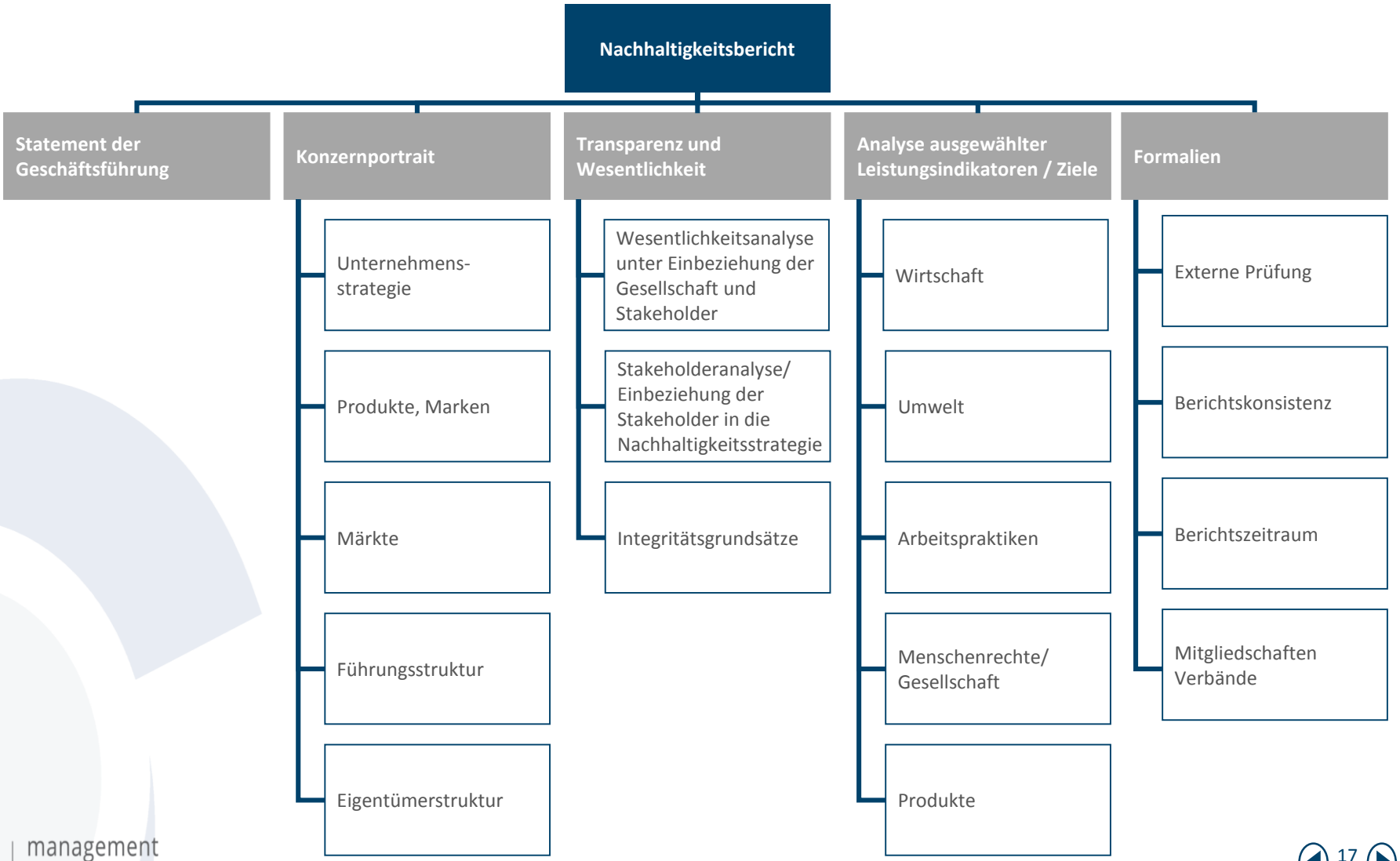
  1. auch große Mittelständische Unternehmen übernehmen diesen Standard, um wettbewerbsfähig zu bleiben
  2. nutzen das Berichtsmittel CSR zum Recruiting neuer Mitarbeiter und Imagebildung
  3. ist im internationalen Kontext oft Standard geworden.

- **Nach GRI-Standard (Global Reporting Initative) sind über die Ergebnisse von Compliance - und Risikomanagement Audits im Rahmen der vertikalen Lieferantenkette zu berichten**

* Wenn 500 Mitarbeiter, 40 Mio. € Umsatz und/oder 20 Mio. € Bilanzsumme

Exkurs: Der Aufbau eines GRI-Nachhaltigkeitsberichtes

Vorgaben zu Compliance und Risikomanagement gelten auch für andere Berichtsformen, z.B. EFFAS oder DNK



Audit Risiko lag vor allem darin, dass die eigene Freiheit in der organisatorischen Compliance-Umsetzung eingeschränkt wird

Dokumentationslage beim Kunden vor dem Audit

- Kunde berief sich auf vorhandene offene Vertrauenskultur im Unternehmen und hatte keinerlei Dokumentation und Richtlinien
- Es herrschte die Meinung vor, dass „Compliance-Risiken“ nur die Großen betreffen. „Als kleines Unternehmen hat die GL das besser im Griff.“
- Risikoreporting war nicht als eigenständiges Reportingtool implementiert, sondern galt als mündlicher Bestandteil der Management Gespräche

Auf dieser Basis wäre ein Audit nur mit großen Mängeln bestanden worden. Risiko: Liebherr diktiert Systeme und Konditionen in der Umsetzung von Compliance und Risikomanagement Standards. Kein Standard, keine Lieferbeziehung.

Audit gut bestanden!

Vorbereitung auf das Audit mit Hilfe Management Alliance

- Auf Druck des AR-Vorsitzenden Schulung des Managements und der 1. Führungs-ebene

- Anschließend Workshop zur Risikoanalyse. Ergebnisse:

  a) Korruptionsprävention, insbesondere in Bezug auf die Einbindung der Handelsvertreter
  b) Export / Embargo
  c) Kommunikation innerhalb der Organisation

- Definition und Aufbau einer Organisationsstruktur durch Benennung von internen Verantwortlichen

- Erstellung einer Basisdokumentation:
  Code of Conduct – Korruptionspräventionsrichtlinie – Risikoreporting - Handelsvertreterverträge

Status Quo heute im Unternehmen

Risikomanagement als Chancenmanagement aufgebaut

- QS-Verantwortliche hat den Bereich Compliance / Risikomanagement übernommen
- Aufgrund der Größe des Unternehmens erfolgte keine Einführung eines systemischen Risikodokumentationstools
- Aber: Vierteljährliches Reporting eingeführt und akzeptiert
- Management Alliance übernimmt die Trainings und Schulungen der Mitarbeiter in regelmäßigen Abständen
- Jährliches Coaching des Risikomanagement Verantwortlichen durch Management Alliance

Marktanforderungen

Anforderungen des Marktes sind oft von operativen Gegebenheiten beeinflusst

Ausgangslage

- Unternehmen aus der Maschinenbauindustrie, Komponentenhersteller, hat ein Einkaufsvolumen zwischen 35% und 38% vom Umsatz

- Eckdaten:

  Umsatz 2017: 200 Millionen Euro
  EBIT-Marge: 15% p.a.
  Mitarbeiter: 2.500
  internationaler Vertrieb und Handelsvertreter

Marktanforderungen

Risikoprävention erfordert Schnelligkeit, Flexibilität und Verantwortung

Problemstellung

- Lieferanten können die gewünschten Lieferlaufzeiten wegen Überlast nicht einhalten.
- Angebotsanfragen werden mit einer Verzögerung von 4-6 Wochen bearbeitet

Folge: Eigene Liefertermine und Ertragskraft gefährdet

Aber: Kein aktives Gegensteuern durch das Management trotz eines etablierten Risikomanagements

Auch hier handelt es sich um ein Compliance Risiko, da es sich um die Einhaltung der Einkaufsrichtlinie handelt, die eine stets ausreichende Anzahl von mehreren Lieferanten vorschreibt.

Lösungsansätze bietet ein operatives Risikomanagement

Papiertiger und Strukturen ohne Inhalt schaden dem Prinzip

Warum es nicht funktioniert?

- Kein ganzheitliches Verständnis von Risikomanagement und Compliance im Management
- „Angst“ schlechte Nachrichten zu überbringen
- Hoffnungstendenz: „Es ist noch immer gut gegangen“
- Kein professioneller Ansprechpartner im Hause zum Thema Risiko-management und keine Rück-meldungen durch den Riskmanager

Best Practice

- Unabhängigkeit in der Risikobeurteilung schafft Professionalität, Outsourcing bietet eine Lösung
- Aber: Prozesskenntnisse sind zur Plausibilisierung von Maßnahmen absolut erforderlich
- Aktive Informationspolitik und Rückmeldungen vom Riskmanager. ansonsten verliert man Akzeptanz

Wie hätte man dieses Problem im Sinne es aktiven Risikomanagements lösen können?

1. Information laut VDMA, dass Vollbeschäftigung herrscht. Fazit: Längere Lieferzeiten sind zu erwarten.

2. Folge: Aufnahme einer Risikoposition „Lieferant und Lieferzeit“, auch wenn derzeit nicht bewertbar und aktuell

3. Zuordnung von Frühwarnindikatoren, um rechtzeitig Gegenmaßnahmen einleiten zu können und nicht es Reaktion, wenn bereits „Kind in den Brunnen gefallen ist“.

   Frühwarnindikatoren in diesem Fall können sein:

   a) Verschiebung von bereits zugesagten Lieferzeiten
   b) Brancheninformation (siehe VDMA und andere), Einkäuferindex etc.
   c) ungeplante Erhöhung der Materialquote

Wie hätte man dieses Problem im Sinne es aktiven Risikomanagements lösen können?

4. Frühwarnindikatoren zeigen eine Verschlechterung der Situation an

   => Folge: Konkrete Gegenmaßnahmen sind zu benennen und deren Umsetzung zu kontrollieren.

   Gegenmaßnahmen können sein:

   a) Erhöhung Lagerbestand
   b) Anpassung der Systeme hinsichtlich Mindestmengen und Lieferzeiten
   c) alternative Lieferanten suchen

   Fazit: Umsetzung erfordert erhöhte Personalkapazitäten im Einkauf und ggfls im Bereich Disposition.

Die Lösung des Problems ist eine originäre Einkaufsaufgabe. Risikomanagement ist an dieser Stelle ein Management-Tool zur Einhaltung der Ertragsziele. Interne Betriebsblindheit behindert oft einen aktiven Prozess.

Status Quo heute im Unternehmen

Risikomanagement und Compliance haben weiterhin keine Akzeptanz im Unternehmen

- Unternehmen strebte Outsourcing aller Compliance- und Risikomanagement-Aktivitäten an
- Aber: keine Bereitschaft bezüglich Änderungen von Strukturen und Verantwortlichkeiten

Management Alliance hat den Auftrag abgelehnt.

Industrieanforderungen

Basis sind in der Regel gesetzliche Vorgaben

Beispiele

- Arbeitsschutz
- Produktionssicherheit
- Strahlenschutz / Laserschutz / Röntgenverordnung
- Qualitätssichernde Vorgaben
- Abwasser und Entsorgungsvorgaben
- etc

Herausforderung: Wie bleibe ich stets aktuell und bekomme gesetzliche Änderungen mit? Ein Nichteinhaltung wäre nicht nur ein Compliance Risiko, sondern führt auch zu hohen Bußgeldern.

Ein Lösungsansatz bietet der Aufbau eines Gesetzeskatasters

Stets up to date durch systemische Unterstützung im Zuge eines Gesetzeskatasters

- Ermittlung aller relevanter Gesetzesgrundlagen für den Geschäftsbetrieb
- Durch systemische Unterstützung erfolgt eine automatische Information zu gesetzlichen Änderungen (Software-Anbieter)
- Auf Basis der Änderungsinformation Managemententscheidung möglich, ob Anpassungen in der Organisationsstruktur etc. erforderlich sind

Achtung: Aufbau eines Gesetzeskatasters für ausländische Aktivitäten schwierig.
1. Step sollte sich auf Deutschland beziehen.

Gesetzliche Anforderungen

Das Beispiel der Korruptionsprävention

Gesetzeslage in Deutschland

- Es gelten die Vorgaben des Strafgesetzbuches (§§ 331 – 337)
- Schwerpunkt liegt auf dem Aspekt der Bestechlichkeit von Amtsträgern
- Keine Vorgaben zu Organisation und Prävention

UK Bribary Act schlägt auf Deutschland durch, wenn Umsatz in UK besteht

- Transparente und umsetzbare **Richtlinien** zur Korruptionsprävention und deren konzernweite Implementierung
- **Management Commitment**
  - Verpflichtung der obersten Führungsebene (tone of the top)
  - Schaffung einer Kultur, die Korruption ablehnt
- **Risikobewertung**
  - Risiken kennen und verlässlich einschätzen als operativer Prozess
- **Due Diligence** von Geschäftspartnern
- **Kommunikation** und Training
- **Überwachung und Überprüfung**

Due Dilligence von Geschäftspartnern: Damokles-Schwert in Handelsvertreterbeziehungen

Risiko des Ausgleichsanspruch versus Einbindung in die Compliance-Strukturen

- Auch die Handelsvertreter sind im Zuge einer regelmäßigen Business Partner Due Dilligence in die Compliance-Strukturen einzubinden

- Risiko:

  Das Verschulden des Handelsvertreters wird dem Unternehmen zugerechnet.

- Generelles Problem:

  a) Es bestehen zunächst keine Informations-, Auskunfts- und Schulungsrechte zwischen Unternehmen und Handelsvertreter
  b) Eine vertragliche Regelung im Handelsvertretervertrag kann dagegen Ausgleichsansprüche des Handelsvertreters gegen das Unternehmen begründen

- Lösungsvorschlag: Audits und formale Business Partner Due Dilligence

Beispiel Iran-Embargo: In Alternativen Denken schafft Sicherheit

Variante 1 kein Iran-Geschäft

- Geschäftsbeziehung in die USA ist führend, darum Einstellung aller Iran-Aktivitäten

Im Unternehmen zu regeln:

1. Klare Anweisungen um interne Missverständnisse zu vermeiden
2. Ausgleichsregelung für betroffene Vertriebsmitarbeiter treffen

Variante 2 kein USA-Geschäft

- Geschäftsbeziehung in den Iran wird als der strategische Zielmarkt gesehen, daher Rückzug aus den USA.
- Dennoch müssen die US-Embargo-Vorgaben eingehalten werden.

Im Unternehmen zu regeln:

1. US-Einkaufsteile durch andere Komponenten ersetzen
2. Ggfls neue Schnittstellen programmieren
3. Bankverbindungen aufbauen, die Geldeingänge aus dem Iran akzeptieren

Variante 3 Risiko

- Ein Wegfall des US-Geschäftes wäre Worst Case nicht tragisch, aber Versuch ist es wert, beide Länder zu bedienen.
- Die US- und EU - Embargo-Vorgaben müssen eingehalten werden.

Im Unternehmen zu regeln:

1. US-Einkaufsteile durch andere Komponenten ersetzen
2. Ggfls neue Schnittstellen programmieren
3. Bankverbindungen aufbauen, die Geldeingänge aus dem Iran akzeptieren

Ein Auszug jüngster Compliance Vorfälle

König & Bauer
Jahr 2017

- Vorwurf der Korruption von ausländischen Amtsträgern (Brasilien, Nigeria, Kasachstan) ggü. der schweizer Tochter
- Strafzahlung € 28 Mio. plus € 5 Mio. in einen Fonds zur ethischen Unternehmensführung
- Begründung: König & Bauer hat in seiner Organisation nicht alles dafür getan, um Korruption zu verhindern

Thyssen Krupp
Jahr 2016

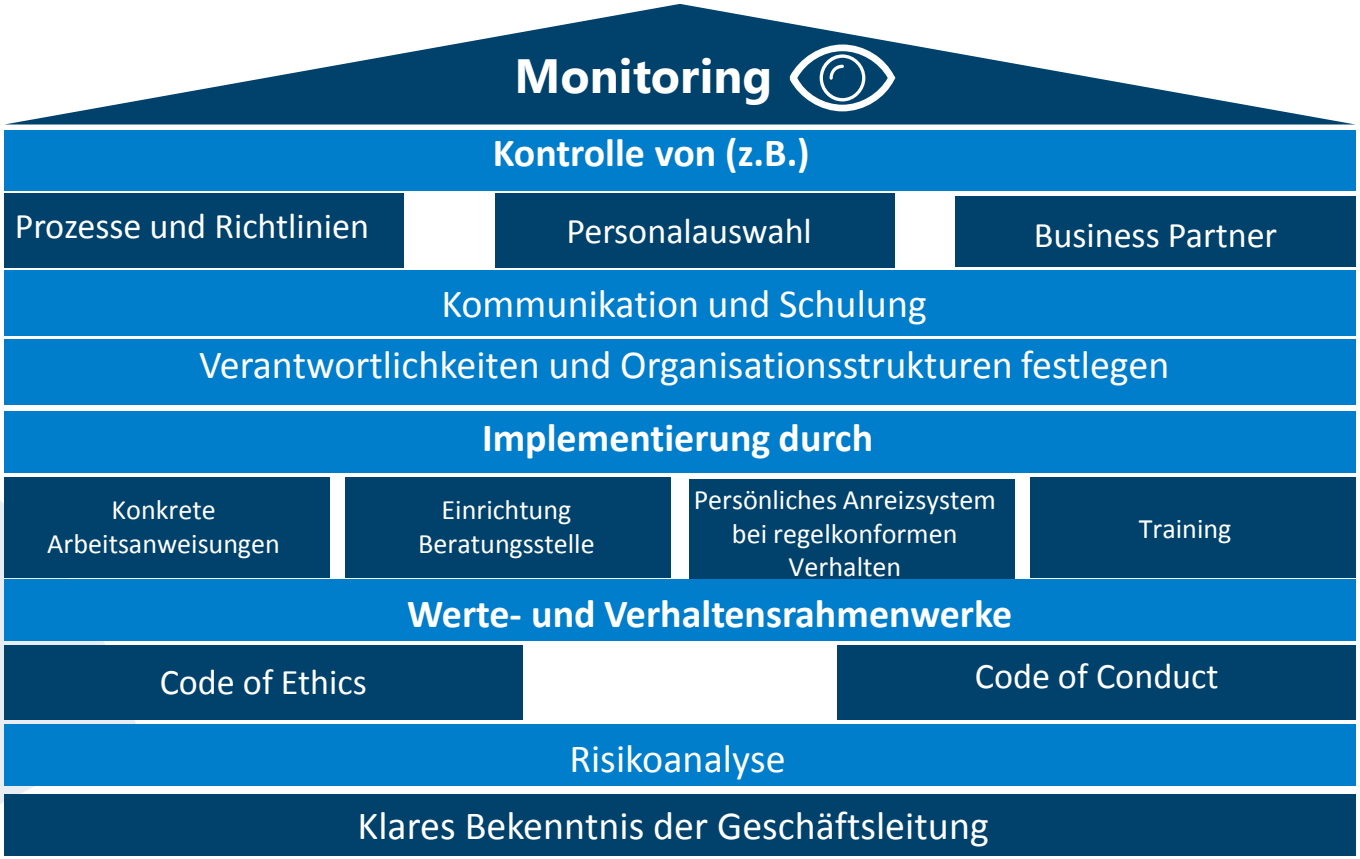
- GF einer Thyssen Krupp Sparte kommt in Erklärungsnöte, da dieser von einem pakistanischen Handelsvertreter ein persönliches Geschenk an dessen Ehefrau annimmt, Goldarmband im Gegenwert von rund T€ 4,3
- Der Handelsvertreter-Vertrag wird nicht verlängert
- Handelsvertreter klagt Ausgleichsansprüche in Höhe von € 20 Mio. ein

Thyssen Krupp
Jahr 2017/2018

- Im Rahmen eines 1,5 Mrd. € U-Boot Deals mit der isrealischen Regierung steht der israelische Handelsvertreter von Thyssen unter dem Verdacht der Korruption
- Sachverhaltsaufklärung und juristisches Verfahren läuft derzeit noch
- Thyssen hat sich offiziell distanziert und macht derzeit keine Geschäfte mehr mit/über den israelischen Handelspartner

Erfolgsfaktoren

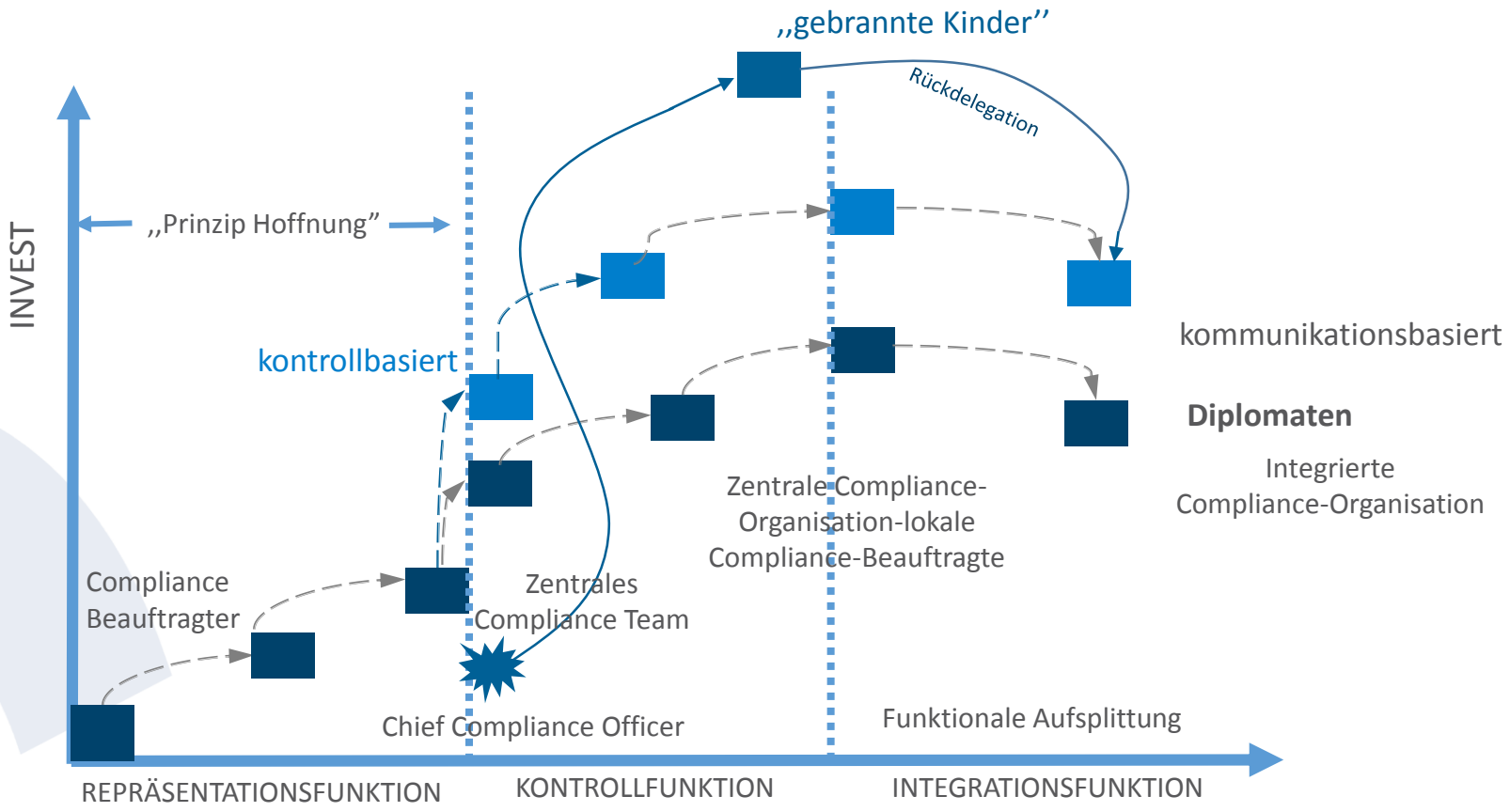
Erfolgreiche Compliance-Strukturen sind fest in die Unternehmensorganisation integriert



Quelle: ComplianceProgramMonitor ZFW und eigene Darstellung

Entwicklung von Compliance-Organisationen folgt oft der Not

Erfolgsfaktor: Diplomatie und Prozesskenntnisse



Quelle: COMFORMIS GmbH

Zwischenfazit

Es besteht keine Pflicht zum Aufbau einer Compliance-Abteilung, aber

sind die Grundvoraussetzungen für eine mögliche Enthaftung der Organe im Schadensfall.

Strukturen und Kultur: Die Mindestanforderungen

- Erstellung und Einführung eines Code of Conduct
- Risikoanalyse
- Regelmäßige Compliance Trainings zu

  a) Organisationsstruktur
  b) Themen der Risikoanalyse
- Offene Feedback-Kultur und Mitarbeitereinbindung in das System (Nutzenargumentation)
- Best Practice: persönliche Whistle Blower Hotline (mit Gesicht) schafft Akzeptanz und deckt mehr Vergehen auf
- Systemische Unterstützung

Prüfstandard PS 980 Bestandteile des CMS

- Compliance-Kultur
- Compliance-Ziele
- Compliance-Organisation
- Compliance-Risiken
- Compliance-Programm
- Compliance-Kommunikation
- Compliance-Überwachung und Verbesserung

Verantwortlichkeiten: Akzeptanz die größte Herausforderung

Was der Akzeptanz schadet

- Ausschließliche organisatorische Verknüpfung mit den Stabsbereichen Recht und Revision
- Fehlende Prozesskenntnisse und kein Verständnis für die „Grauzonen“ am Markt
- Hardliner Mentalität
- Keine positiv vorgelebte Praxis (Man spricht mit „2“ Zungen)
- Wenn es keine Ausgleichslösungen für Vertriebsmitarbeiter gibt, die durch Compliance-Entscheidungen ihre Provision verlieren (aktuell bei politischen und/oder kurzfristigen Embargo-Änderungen)
- Mangelhafte Feedback-Kultur
- **FEHLENDES COMMITTMENT DES TOP MANAGEMENTS**

Die aktuellen Rechtsfälle beruhen vorrangig auf dem Thema Organisationsverschulden

Fazit:

Compliance und operative Risiken können nicht vermieden werden. Mit der Schaffung von Verantwortlichkeiten und Organisationsstrukturen wird eine Basis geschaffen, mögliche Haftungsrisiken im Schadensfall besser zu steuern.

Aber: Ohne eine nachhaltige Informations- und Trainingspolitik gilt seitens der Behörden die Vermutung, dass es sich nur um „Papiertiger“ handelt.

Gerne stehen wir Ihnen für weitere Fragen zur Verfügung

Gabriele Bornemann
geschäftsführende Gesellschafterin
Management Alliance GmbH

Tel: +49 201 50 77 20 91
bornemann@managementalliance.de

www.managementalliance.de

Sabine Schneider
operative Betreuung Risikomanagement

Tel: +49 201 50 77 20 91
Home Office: +49 271 38 29 468
sabine.schneider@managementalliance.de

www.managementalliance.de

Disclaimer - Haftungsausschluss

Alle Informationen in diesem Vortrag sind nach bestem Wissen und Gewissen zusammengestellt.

Wir weisen jedoch daraufhin, dass wir keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit übernehmen. Insbesondere ersetzt dieser Vortrag keine rechtliche Beratung im Einzelfall.

Herzlichen Dank für Ihre Aufmerksamkeit