

*Fachgebiet:*

**Compliance in der Organisation**

## **Lehrbrief 1**

- ↗ **Abgrenzung der Prüfungs- und Überwachungsinstitutionen**
- ↗ **Compliance von Lieferanten und Kunden**
- ↗ **Compliance in Forschung und Entwicklung**
- ↗ **Compliance und M&A**
- ↗ **Compliance und IT**

**Verfasser:**

Prof. Dr. Volker H. Peemöller  
Oliver Gschwender

© 2020 WIRTSCHAFTScampus

Dr. Peemöller GmbH  
Austraße 42  
97299 Zell

Alle Rechte vorbehalten. Die Schulungsunterlagen der WIRTSCHAFTScampus Dr. Peemöller GmbH sind ausschließlich für Teilnehmer zum persönlichen Gebrauch bestimmt. Ohne ausdrückliche schriftliche Genehmigung der WIRTSCHAFTScampus Dr. Peemöller GmbH ist jede Reproduktion/Digitalisierung/Vervielfältigung/Verbreitung von Schulungsunterlagen – auch auszugsweise – in jedweder Form sowie die Weitergabe an Dritte unzulässig und berechtigt zum Schadensersatz. Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

**Certified Chief Compliance Officer**

**Lernziel:**

In diesem Lehrbrief werden Sie mit den verschiedenen Bereichen der Unternehmen unter Compliance-Aspekten vertraut gemacht. Als Einstieg – quasi als Wiederholung – wird die Abgrenzung der relevanten Begriffe Risikomanagementsystem, Kontrollsystem, Interne Revision und Prüfungsausschuss sowie Compliance und Corporate Governance vorgenommen.

In diesem Lehrbrief haben nicht alle Funktionsbereiche Platz gefunden. So werden Kunden- und Lieferanten behandelt, Compliance-Aspekte von FuE thematisiert und Compliance im Akquisitionsprozess angesprochen. Im nächsten Lehrbrief finden Sie dann die relevanten Hinweise zur Führung und zum Rechnungswesen. Sehr ausführlich wird der IT-Bereich auf Compliance-Sachverhalte analysiert.

Viel Erfolg bei der Bearbeitung wünscht Ihnen

Ihr Wirtschaftscampus-Team

## Abkürzungen

<b>1.</b>	<b>Abgrenzung der Prüfungs- und Überwachungsinstitutionen .....</b>	<b>1</b>
1.1	Interne Revision .....	1
1.1.1	Begriffliche Abgrenzung.....	1
1.1.2	Inhalt der Prüfung .....	1
1.1.2.1	Die Interne Revision bewertet und verbessert Risikomanagementsysteme (RMS) .....	1
1.1.2.2	Die Interne Revision bewertet und verbessert Kontrollsysteme (IKS) .....	2
1.1.2.3	Die Interne Revision bewertet und verbessert Governance .....	2
1.1.3	Zweck der Tätigkeit.....	3
1.2	Aufsichtsrat, Prüfungsausschüsse und Audit Committee .....	3
1.2.1	Aufsichtsrat .....	3
1.2.2	Prüfungsausschuss.....	4
1.2.3	Audit Committee .....	5
1.2.4	Übertragbarkeit des Audit Committees auf deutsche Verhältnisse.....	5
1.2.5	Aufgabenverteilung im Gefüge der Überwachungsträger .....	7
1.3	Compliance .....	8
1.4	Corporate Governance .....	9
1.5	Risikomanagementsysteme.....	10
1.5.1	Begründung.....	10
1.5.2	Bestandteile eines Risikomanagementsystems .....	11
1.5.2.1	Risikofrüherkennungssystem.....	11
1.5.2.2	Risikosteuerungssystem.....	12
1.5.2.3	Internes Überwachungssystem .....	12
1.6	Zusammenhang zwischen den Elementen .....	13
<b>2.</b>	<b>Compliance von Lieferanten und Kunden .....</b>	<b>15</b>
•		
•		
•		
<b>3.</b>	<b>Compliance in Forschung und Entwicklung (FuE) .....</b>	<b>21</b>
•		
•		
•		

<b>4.</b>	<b>Compliance und Merger and Acquisition (M&amp;A).....</b>	<b>28</b>
	•	
	•	
	•	
<b>5.</b>	<b>Compliance und IT .....</b>	<b>35</b>
	•	
	•	
	•	
	<b>Lösungen zu den Kontrollfragen .....</b>	<b>70</b>

**Abkürzungen 1**

ABC-Analyse	Analyseverfahren zur Abgrenzung von Sachverhalten nach ihrer Bedeutung
AG	Aktiengesellschaft
AktG	Aktiengesetz
AO	Abgabenordnung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BIOS	Basic Input/Output System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CD-ROM	Compakt-Disc
CPI	Corruption Perception Index
DBI	Deutsche Bahn international
DCGK	Deutscher Corporate Governance Kodex
DIN	Deutsche Industrie Norm
DVD	Digital Versatile Disc
EDV	Elektronische Datenverarbeitung
EMAS	Eco Management and Audit Scheme
ERM	Enterprise Risk Management
EU-RL	Europäische Union - Richtlinie
FuE	Forschung und Entwicklung
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GRC	Governance-Risikomanagement und Compliance
Hash-Wert	Ergebnis einer kryptologischen Hashfunktion
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer in Deutschland
IIA	Institute of Internal Auditors
IKS	Innerbetriebliches Kontrollsystem
IR	Interne Revision
ISO	International Organization for Standardization
IT	Informationstechnologie
KMU	Klein- und Mittelunternehmen
M&A	Merger and Acquisition
MaRisk	Mindestanforderungen an das Risikomanagement (BA)

**Abkürzungen 2**

MoMiG	Gesetz zur Modernisierung des GmbH-Rechts und zur Bekämpfung von Missbräuchen
PC	Personal Computer
PS	Prüfungsstandard des IDW
RAID	Redundant Array of Independent Disks
RMS	Risikomanagementsystem
SaaS	Software as a Service
SOA	Sarbanes-Oxley Act
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
Tz	Textziffer
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
USB	Universal Serial Bus
UStG	Umsatzsteuergesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VMware	ist ein US-amerikanisches Unternehmen, das Software im Bereich der Virtualisierung entwickelt
VPN	Virtual Private Network
WpHG	Wertpapierhandelsgesetz
XYZ-Analyse	Analyseverfahren zur Abgrenzung von Sachverhalten nach ihrer ökologischen Relevanz

- 
- 
- 

## 1.5 Risikomanagementsysteme

### 1.5.1 Begründung

Generell wird Risiko als Mehrwertigkeit der zukünftig möglichen Entwicklung verstanden, denen eine Entscheidung unter Unsicherheit zugrunde liegt. Im allgemeinen Sprachgebrauch wird der Begriff Risiko im Sinne einer möglichen nachteiligen wirtschaftlichen Entwicklung benutzt. Jeder wirtschaftliche und unternehmerische Entscheidungsprozess ist mit Risiken verbunden, die sich wirtschaftlich in Verlusten oder Schäden niederschlagen und den Fortbestand des Unternehmens nachhaltig gefährden können. Der Vorteil der Risikoorientierung ergibt sich daraus, dass man sich nicht mit eingetretenen Verlusten und Schäden beschäftigt, sondern mit zukünftigen Verlustgefahren, deren Eintritt nach Möglichkeit verhindert werden soll. Außerdem soll damit erreicht werden, dass vom Unternehmen nur Risiken übernommen werden, die auch „verkräftet“ werden können.

Begriff Risiko

Vorteile der  
Risikoorientierung

## 1.5.2 Bestandteile eines Risikomanagementsystems

Nach § 91 Abs. 2 AktG ist der Vorstand einer AG verpflichtet, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“ Aus dieser Anforderung des Gesetzgebers resultiert für den Vorstand eine zweistufige Verpflichtung: Die Einrichtung eines Risikofrüherkennungssystems und eines darauf ausgerichteten Internen Überwachungssystems. Ein Risikomanagementsystem als Gesamtheit aller Regeln und Maßnahmen zum strukturierten Umgang mit Risiken erfordert aber drei Subsysteme: Risikofrüherkennungs-, Risikobewältigungs- und internes Überwachungssystem. Soll die Einhaltung dieser Vorgaben gesichert werden, kommt noch Compliance hinzu. Diese vier Bestandteile sollen nachfolgend betrachtet werden:

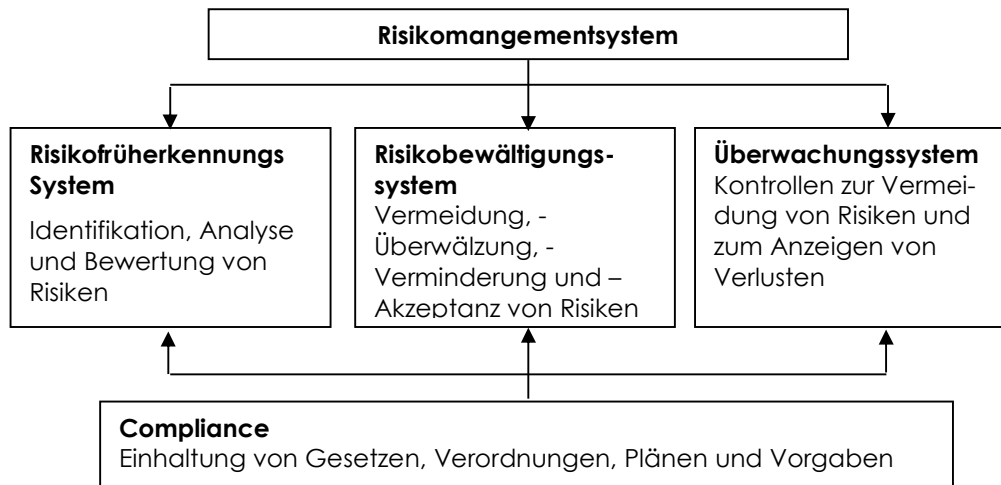


Abb. 1. Bestandteile eines Risikomanagementsystems

### 1.5.2.1 Risikofrüherkennungssystem

Eine systematische Vorgehensweise bei der Identifikation und Bewertung von Risiken ist die Voraussetzung für ein erfolgreiches Risikomanagement. Die Identifikation der Risiken dient der Aufdeckung von Verlustgefahren und der Lokalisierung von Problembereichen. Da die Risiken aus den betrieblichen Prozessen entstehen, bilden sie auch die Basis der Risikoanalyse. Die Prozesse werden in ihre Teilprozesse zergliedert, in denen die Risiken von den Prozessownern zu identifizieren sind.

Die identifizierten Risiken sind hinsichtlich des Ausmaßes ihres Einflusses auf die Zielerreichung zu bewerten. Diese Beurteilung erfolgt hinsichtlich der Wahrscheinlichkeit des Eintritts und der Auswirkung auf die Zielerreichung. Risiken können vielfach nicht isoliert bewertet werden, da einerseits Interdependenzen zwischen den Risiken innerhalb eines Prozesses bestehen und andererseits dasselbe Ereignis in mehreren Prozessen auftreten kann. Vermeintlich unbedeutende Einzelrisiken nehmen im Falle additiver oder kumulativer Wirkung in Verbindung mit anderen Risiken ein durchaus zielgefährdendes Ausmaß an. Zur Berücksichtigung dieser Zusammenhänge sind Risiken in eine Risiko-Portfolio-Betrachtung einzubeziehen und als inhärente Bruttoisiken zu bewerten, sodass an dieser Stelle noch nicht die Risikosteuerungsmaßnahmen zum Tragen kommen.

Wichtig sind eine einheitliche Identifizierung und Bewertung der Risiken und die Vermeidung von Tabuthemen. Das Ausklammern von Themen aus diesem Prozess mag auch mit ursächlich für die Finanzkrise gewesen sein. Einmalige oder seltene

Anforderungen  
des Gesetzgebers



Identifizierung  
und Bewertung  
von Risiken

Eintrittswahrscheinlichkeit  
und Bedeutung  
des Risikos



einheitliche  
Behandlung von  
Unternehmen



Ereignisse sind besonders zu würdigen, da für sie nur wenige Daten zu den Risiken der Vergangenheit vorliegen. Hier sollte für die Bewertung auf Vergleichsprozesse, andere Branchen oder zeitliche Vorläufer zurückgegriffen werden. Bei den Standardprozessen sollten auch externe Schocks berücksichtigt werden. Das Denken „in eingefahrenen Gleisen“ wird mit ein Grund dafür gewesen sein, dass die Risikomanagementsysteme bei der Finanzkrise nicht gegriffen haben.

### 1.5.2.2 Risikosteuerungssystem

Mithilfe des Risikosteuerungssystems soll den Risiken effektiv begegnet und diese auf ein definiertes Maß begrenzt werden. Grundsätzlich sind bei der Ableitung der entsprechenden Maßnahmen die Auswirkungen der Risiken in den Prozessen, die Konformität der Prozesse mit den Zielen und die bestehenden Risikosteuerungsmaßnahmen zu berücksichtigen. Grundsätzlich werden vier Möglichkeiten unterschieden.

<b>Risikovermeidung</b>	<b>Risikoüberwälzung</b>
Aufgabe risikobehafteter Aktivitäten	Reduzierung von Eintrittswahrscheinlichkeit und/oder Schadenshöhe
Beispiele: Aufgabe von Geschäftseinheiten, Abbruch von Projekten	Beispiele: Versicherungen, vertragliche Gestaltung, Hedging
<b>Risikoverminderung</b>	<b>Risikoakzeptanz</b>
Entwicklung von Steuerungsmaßnahmen	Bewusste Übernahme von Risiken
Beispiele: Verbesserung der Geschäftsprozesse, Diversifikation, Portfoliomanagement	Beispiele: Bildung von Rückstellungen, Stärkung des Eigenkapitals, Schulung der Mitarbeiter

Abb. 2: Möglichkeiten der Risikosteuerung

Durch eine Maßnahme kann sowohl die Schadenshöhe als auch die Eintrittswahrscheinlichkeit beeinflusst werden und mehr als ein Risiko betroffen sein. Zudem ist bei diesen Maßnahmen auch das Kosten-Nutzen-Verhältnis zu berücksichtigen. Die Reduktion von Risiken kann auch zu einem Verzicht auf Chancen und zu Imageverlusten führen, wenn angestammte Geschäftsfelder aufgegeben werden. Letztendlich ist diejenige Kombination von Maßnahmen auszuwählen, bei der die verbleibenden Restrisiken sowohl einzeln als auch in der Summe unterhalb der vom Management festgelegten Schadensgrenze bleiben.

### 1.5.2.3 Internes Überwachungssystem

Das interne Überwachungssystem enthält alle Regelungen und Maßnahmen, die Abweichungen verhindern bzw. aufgetretene Abweichungen rechtzeitig anzeigen sollen. Alle möglichen Arten prozessintegrierter Kontrollen kommen in Betracht, die in manuelle, IT- und Antifraud-Kontrollen unterschieden werden können. Für jede Kontrolle sind Kontrollziel, betroffenes Risiko, betroffener Jahresabschlussposten und Hinweise zur Überwachung anzugeben. Eine Kontrolle ist hinsichtlich der folgenden zwei Sachverhalte zu konzipieren:

1. Die Ausgestaltung der Kontrolle muss geeignet sein, die Risiken zu vermindern (control design).
2. Die Kontrolle muss durchgängig wirken (operative effectiveness).



Formen der  
Risikohand-  
habung

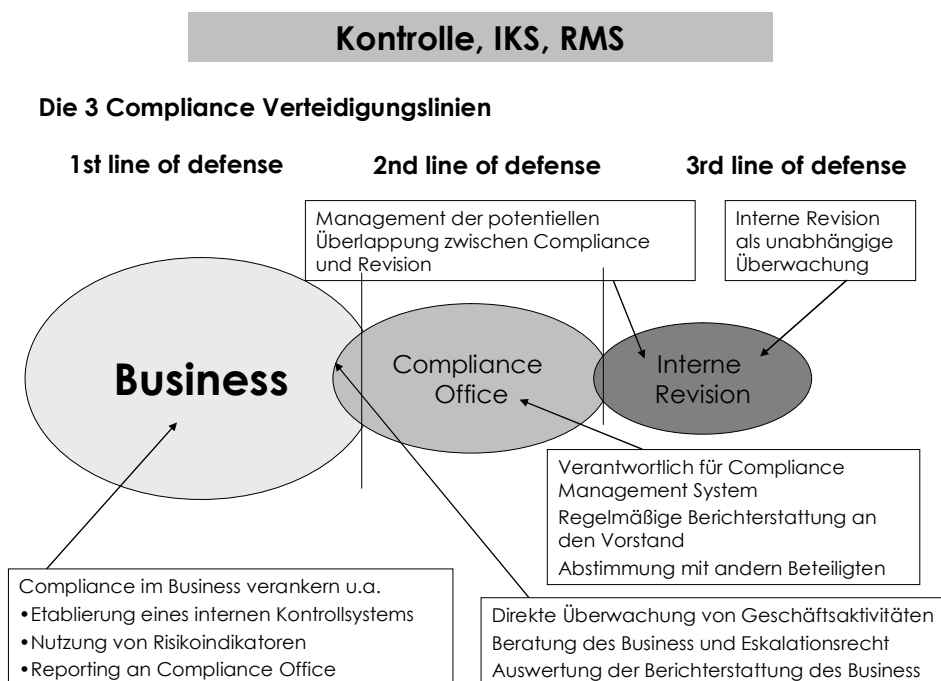


## 1.6 Zusammenhang zwischen den Elementen

Das Konzept 3 Lines of Defense des IIA gibt die Zusammenhänge zwischen den Instrumenten wieder. Danach besteht folgende Reihenfolge der Instrumente, um die Einhaltung der Vorgaben zu gewährleisten:

1. Geschäftsprozesse: Die einzelnen Führungskräfte für die operativen Abläufe sind für das Managen der Risiken verantwortlich. Sie haben für zuverlässige Kontrollen zu sorgen, die Behandlung der Risiken vorzunehmen und Kontrollverfahren einzuführen.
2. Compliance Funktionen: In einer idealen Welt würde eine Verteidigungslinie reichen. Es treten aber in der Praxis vielfältige Gefährdungen auf, so dass eine weitere Verteidigungslinie erforderlich wird. Zu ihr gehören finanzielle Kontrollen, Sicherheitsdienste, Risikomanagement, Qualitätssicherung, Überwachung und Compliance.
3. Interne Revision: Die Interne Revision als unabhängige Institution im Unternehmen mit umfassenden Prüfungsrechten ausgestattet, versorgt die Geschäftsführung mit umfassenden Prüfungsleistungen.

Daraus lässt sich folgende Abbildung gewinnen.



- 
- 
- 

3 Verteidigungslinien



Geschäftsprozesse

Compliance

Interne Revision



**Lösung zu den Kontrollfragen:**

- 
- 
-