WIRTSCHAFTS campus
Dr. Peemöller GmbH

Fachgebiet:

Compliance in der Organisation

Lehrbrief 1 – Leseprobe

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

Verfasser:
Prof. Dr. Volker H. Peemöller

© 2025 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

Stand: 2025

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. Hier haben sich einige Neuerungen ergeben durch das Finanzmarktintegritätsstärkungsgesetz (FISG), das in Folge des Wirecard-Skandals am 3. Juni 2021 verabschiedet wurde.

In diesem Lehrbrief haben nicht alle Funktionsbereiche Platz gefunden. So werden Kunden- und Lieferanten behandelt, Compliance-Aspekte von Forschung und Entwicklung thematisiert und Compliance im Akquisitionsprozess angesprochen. Im nächsten Lehrbrief finden Sie dann die relevanten Hinweise zur Führung und zum Rechnungswesen.

Viel Erfolg bei der Bearbeitung wünscht Ihnen

Ihr Wirtschaftscampus-Team

 © wirtschaftscampus

Abkürzungen

1. Abgrenzung der Prüfungs- und Überwachungsinstitutionen 1
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 Risikomanagement-systeme (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 6
1.2.5 Aufgabenverteilung im Gefüge der Überwachungsträger 8
1.3 Compliance 9
1.4 Corporate Governance 10
1.5 Risikomanagementsysteme 11
1.5.1 Begründung 11
1.5.2 Bestandteile eines Risikomanagementsystems 12
1.5.2.1 Risikofrüherkennungssystem 13
1.5.2.2 Risikosteuerungssystem 13
1.5.2.3 Internes Überwachungssystem 14
1.6 Zusammenhang zwischen den Elementen 14
1.7 Aufbau und Entwicklung eines Compliance-Management-Systems 17

2. Compliance von Lieferanten und Kunden 19

•
•
•

3. Compliance in Forschung und Entwicklung (FuE) 32

•
•
•

4. Compliance und Merger and Acquisition (M&A) 41

•
•
•

Lösungen zu den Kontrollfragen 50

Abkürzungen 1

ABC-Analyse	Analyseverfahren zur Abgrenzung von Sachverhalten nach ihrer Bedeutung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AktG	Aktiengesetz
AMD	Advanced Micro Services
AO	Abgabenordnung
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BGB	Bürgerliches Gesetzbuch
BPI	Bribe Payers Index
CMS	Compliance Management System
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPI	Corruption Perception Index
DAX	Deutscher Aktienindex
DBI	Deutsche Bahn international
DCGK	Deutscher Corporate Governance Kodex
DIN	Deutsche Industrie Norm
EMAS	Eco Management and Audit Scheme
ERM	Enterprise Risk Management
EuGH	Europäischer Gerichtshof
EU-RL	Europäische Union – Richtlinie
FCPA	Foreign Corrupt Practices Act
FISG	Finanzmarktintegritätsstärkungsgesetz
FuE	Forschung und Entwicklung
GKG	Gerichtskostengesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GRC	Governance-Risikomanagement und Compliance
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GWB	Gesetz gegen Wettbewerbsbeschränkungen
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer in Deutschland
IIA	Institute of Internal Auditors
IKS	Innerbetriebliches Kontrollsystem
ILO	Internationale Arbeitsorganisation

 © wirtschaftscampus

IR	Interne Revision
ISO	International Organization for Standardization
IT	Informationstechnologie
KMU	Klein- und Mittelunternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LkSG	Lieferkettensorgfaltspflichtengesetz
M&A	Merger and Acquisition
MaRisk	Mindestanforderungen an das Risikomanagement (BA)
MoMiG	Gesetz zur Modernisierung des GmbH-Rechts und zur Bekämpfung von Missbräuchen
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PS	Prüfungsstandard des IDW
RMS	Risikomanagementsystem
SOA	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
stopp	Strafprozessordnung
Tz	Textziffer
UKBA	United Kingdom Bribery Act
UstG	Umsatzsteuergesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
WpHG	Wertpapierhandelsgesetz
XYZ-Analyse	Analyseverfahren zur Abgrenzung von Sachverhalten nach ihrer ökologischen Relevanz

 © wirtschaftscampus

•
•
•

1.5 Risikomanagementsysteme

1.5.1 Begründung

Begriff Risiko

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 „verkraftet“ werden können.

Vorteile der Risikoorientierung

1.5.2 Bestandteile eines Risikomanagementsystems

Anforderungen des Gesetzgebers

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. Der § 91 AktG ist durch FISG um einen Absatz 3 erweitert worden:

„Der Vorstand einer Börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten."

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:

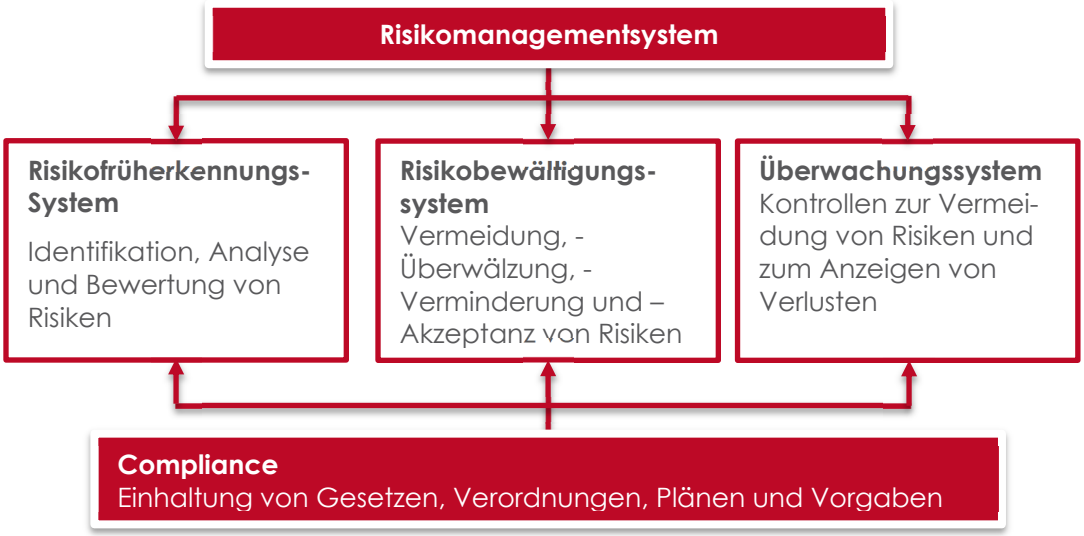

Abb. 1. Bestandteile eines Risikomanagementsystems

1.5.2.1 Risikofrüherkennungssystem

Identifizierung und Bewertung von Risiken

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 Prozess-Ownern zu identifizieren sind.

Eintrittswahrscheinlichkeit und Bedeutung des Risikos

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 meh-

reren 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 Bruttorisiken zu bewerten, sodass an dieser Stelle noch nicht die Risikosteuerungsmaßnahmen zum Tragen kommen.

einheitliche Behandlung von Unternehmen

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 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.

Formen der Risikohandhabung

Risikovermeidung	**Risikoüberwälzung**
Aufgabe risikobehafteter Aktivitäten	Reduzierung von Eintrittswahrscheinlichkeit und/oder Schadenshöhe
Beispiele: Aufgabe von Geschäftseinheiten, Abbruch von Projekten	Beispiele: Versicherungen, vertragliche Gestaltung, Hedging
Risikoverminderung	**Risikoakzeptanz**
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).

1.6 Zusammenhang zwischen den Elementen

3 Verteidigungslinien

Das Konzept 3 Lines of Defense des IIA wurde 2020 aktualisiert und wird nun als Drei-Linien-Modell des IIA bezeichnet [1]. Den 3 Linien übergeordnet ist das Management.

Drei-Linien-Modell

Das Management delegiert Verantwortung und stellt dem Management Ressourcen zur Verfügung, um die Ziele der Organisation zu erreichen (Aufgabe der 1. Linie: Business) und gleichzeitig sicherzustellen, dass rechtliche, regulatorische und ethische Erwartungen (Aufgabe der 2. Linie: Compliance) erfüllt werden. Das Leitungsorgan ist damit sowohl für die Rolle der ersten (Business) als auch der zweiten (Compliance) Linie bei der Erreichung der Organisationsziele verantwortlich. Hinsichtlich der 3. Linie etabliert und beaufsichtigt sie eine unabhängige, objektive und kompetente interne Revisionsfunktion, die Klarheit und Vertrauen bezüglich des Fortschritts bei der Erreichung der Ziele liefert.

Die Rolle der ersten Linie besteht in der Lieferung von Produkten und Leistungen an Kunden der Organisation, einschließlich der Unterstützungsfunktionen.

Die Rolle der zweiten Linie (Compliance) besteht in der Unterstützung des Managements beim Handeln von Risiken. Sie bietet ergänzende Fachkenntnisse, Unterstützung, Überwachung und Aufgaben im Zusammenhang mit dem Risikomanagement:

- Entwicklung, Implementierung und kontinuierliche Verbesserung von Risikomanagementpraktiken auf Prozess-, System- und Unternehmensebene.
- Erreichen von Risikomanagement-Zielen, wie z. B. Einhaltung von Gesetzen, Regulierungen und akzeptablen ethischen Verhaltens, internen Kontrollen, Informations- und Technologiesicherheit, Nachhaltigkeit und Qualitätssicherung.

Die Bereitstellung von Analysen und Berichten über die Angemessenheit und Wirksamkeit des Risikomanagements (einschließlich interner Kontrollen), gehört ebenso zur Aufgabe der 2. Linie.

Die **Verantwortung** für das Management der Risiken liegt aber bei der ersten Linie und dem Management.

[1] vgl. IIA: Das Drei-Linien-Modell, deutsche Übersetzung vom DIIR Juli 2020

Die Rolle der dritten Linie bezieht sich auf die Interne Revision als unabhängige und objektive Prüfungs- und Beratungsinstanz im Unternehmen bezüglich der Angemessenheit und Wirksamkeit von Governance und RMS. Entscheidend für die Sicherstellung dieser Rolle ist die Unabhängigkeit der dritten Linie.

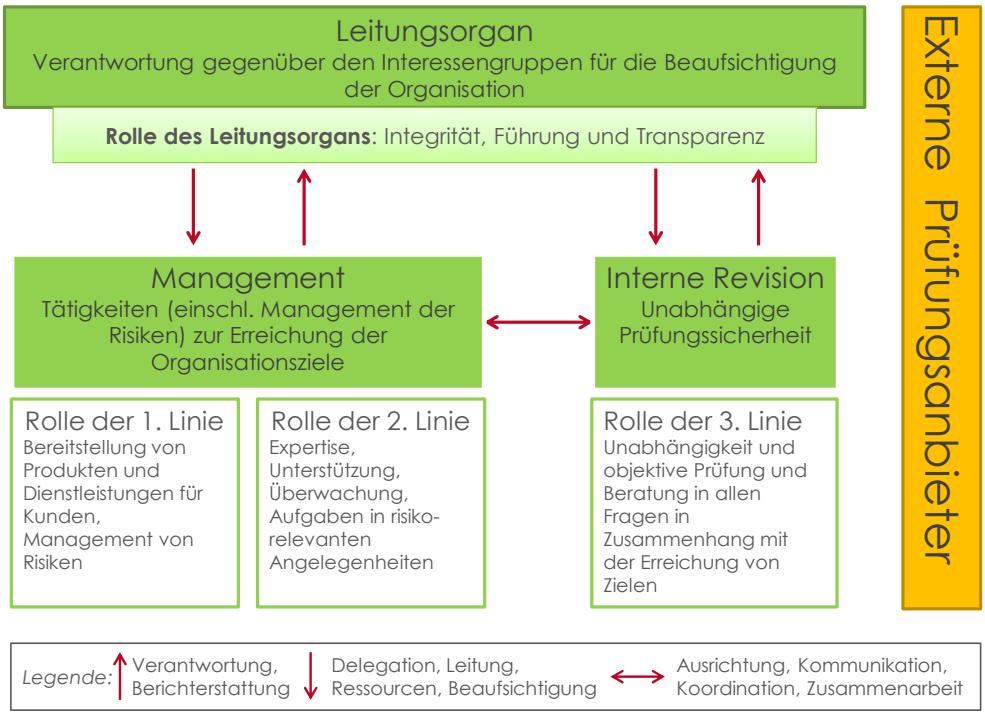

Abb. 3: Drei-Linien-Modell des IIA[2]

-
-
-

[2] Vgl. IIA: Das Drei-Linien-Modell, Übersetzung DIIR Frankfurt 2020, S. 4.

Kontrollfragen 1:

1. Was ist Gegenstand des Governance-Systems des Unternehmens?
2. Welche Anforderungen sind an die Identifizierung und Bewertung von Risiken zu stellen?
3. Welche Formen der Risikobehandlung können unterschieden werden?

Lösung:

zu 1.: _____

zu 2.: _____

zu 3.: _____

Lösungen zu den Kontrollfragen

Lösung zu Kontrollfragen 1:

zu 1.:
Zum Governance System eines Unternehmens gehören die Wertvorstellungen, die Ziele, die Zielerreichung, die Zuordnung der Verantwortlichkeit und die Sicherung des Vermögens. Daraus ergeben sich Vorgaben für das Compliance.

zu 2.:
-
-
-