Oliver Bungartz

Handbuch Interne Kontrollsysteme (IKS)

Steuerung und Überwachung von Unternehmen

6., neu bearbeitete und erweiterte Auflage

ESV ERICH SCHMIDT VERLAG

ESV ERICH SCHMIDT VERLAG

Handbuch Interne Kontrollsysteme (IKS)

Steuerung und Überwachung von Unternehmen

Von
Dr. Oliver Bungartz

6., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978-3-503-19463-6

1. Auflage 2010
2. Auflage 2011
3. Auflage 2012
4. Auflage 2014
5. Auflage 2017
6. Auflage 2020

Gedrucktes Werk: ISBN 978-3-503-19462-9
eBook: ISBN 978-3-503-19463-6

Satz: multitext Berlin

Vorwort zur sechsten Auflage

„Interne Kontrollsysteme (IKS)“ sind als integraler Bestandteil der Corporate Governance allgemein akzeptiert und weit verbreitet. Insbesondere im Zusammenspiel mit dem Risikomanagement, der Internen Revision und der Compliance nimmt die Bedeutung von IKS noch weiter zu. Gerade erst wurde mit der Veröffentlichung des Referentenentwurfs zum Verbandssanktionengesetz (VerSanG) die Notwendigkeit von Compliance-Maßnahmen betont, welche interne Untersuchungen und Kontrollen sowie die systematische Identifizierung, Beurteilung, Steuerung und Überwachung von Risiken beinhalten. Auch angesichts der nicht mehr wegzudenkenden Rolle von IT und Digitalisierung in der Unternehmenspraxis sind Risiken und Kontrollen in diesen Bereichen untrennbar mit dem operativen Tagesgeschäft und den strategischen Zielen einer jeden Organisation verbunden.

Das „Handbuch Interne Kontrollsysteme (IKS) – Steuerung und Überwachung von Unternehmen“ ist mittlerweile als Standardwerk etabliert und die Nachfrage ist zu unserer großen Freude unvermindert hoch. Zehn Jahre nachdem das Handbuch erstmals erschienen ist, bietet nach Abverkauf der fünften Auflage eine Neuauflage die Möglichkeit, alle wichtigen Aktualisierungen und Ergänzungen aufzunehmen. Das gesamte Werk wurde wieder gründlich geprüft, wobei kleinere Fehler bereinigt, die Verzeichnisse und die Literaturhinweise aktualisiert sowie erweitert wurden. Die Bearbeitung und Erweiterung führte zu zahlreichen neuen Tabellen und Abbildungen.

Für die nun vorliegende sechste, neu bearbeitete und erweiterte Auflage wurde die bewährte Konzeption und Struktur der Vorauflagen beibehalten, da diese weiterhin die Zustimmung der Leser findet. Neben den Aktualisierungen aufgrund neuer Gesetze und Standards wurde die neue Auflage u.a. um folgende Aspekte und Abschnitte ergänzt:

- Ergänzung des „Kapitel I: Grundlagen eines Internen Kontrollsystems (IKS)“:
  - Richtlinien-Modell als Möglichkeit der organisatorischen Ausgestaltung
  - Übersicht und Abgrenzung zu den unterschiedlichen Typen von Prüfungen des dienstleistungsbezogenen IKS (System and Organization Controls – SOC) im internationalen Bereich
  - Darstellung des neuen Rahmenwerks „Control Objectives for Information and Related Technology (COBIT 2019®)“ sowie Überarbeitung des Prozessreferenzmodells nach COBIT und des COSO-COBIT-Mapping
- Ergänzung des „Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)“ um IT-Kennzahlen basierend auf den Zielen und IT-Prozessen nach COBIT

- Ergänzung des „Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)“ um ein Bewertungsverfahren basierend auf den COSO-Prinzipen sowie Integration mit dem Reifegrad-Modell zur Beurteilung der Wirksamkeit des IKS
- Ergänzung des „Kapitel IV: Enterprise Risk Management (ERM) als Modell zur Integration von Internen Kontrollsystemen (IKS), Interner Revision und Risikomanagement“:
  - Bewertungsverfahren basierend auf den ERM-Prinzipien sowie Integration mit ERM-Kennzahlen und dem Reifegrad-Modell zur Beurteilung der Wirksamkeit des Risikomanagementsystems
  - Darstellung des sog. „Three-Lines-of-Defense (TLoD)-Modell“ zur Einordnung u.a. von IKS, Interner Revision, Compliance und Risikomanagement innerhalb der Corporate Governance von Organisationen
  - Neuerungen durch den Referentenentwurf VerSanG mit Fokus auf interne Untersuchungen und Compliance-Maßnahmen
  - Fragenkatalog zur Erhebung des Umsetzungsstands und des Grads der Ausgestaltung eines Tax Compliance Management System (CMS)
  - Neuerungen des Deutschen Corporate Governance Kodex (DCGK) und der Grundsätze des Risikomanagements nach ISO 31000

Bei den Vorauflagen wurden bereits die jeweils notwendigen Ergänzungen und Aktualisierungen bei den rechtlichen Grundlagen und Standards berücksichtigt sowie das Werk mit der Hinzufügung relevanter Themen kontinuierlich ausgebaut.

Für ihre Hilfe bei der Realisierung der sechsten Auflage danke ich meinen Kollegen, die mich bei der bereits bei den Vorauflagen unterstützt haben. Auch für die gewohnt reibungslose Zusammenarbeit mit dem Erich Schmidt Verlag in Berlin möchte ich Frau Claudia Splittgerber und Herrn Dr. Joachim Schmidt ganz herzlich danken. Nicht zuletzt gilt besonderer Dank meinen Seminarteilnehmern und Studenten, die mir durch konstruktive Diskussionen und hilfreiche Anmerkungen geholfen haben, dieses Handbuch weiter zu verbessern.

Ich wünsche Ihnen eine anregende und hilfreiche Lektüre und freue mich weiterhin über jegliche Rückfragen und Anregungen. Hinweise und Verbesserungsvorschläge sind stets willkommen.

Hamburg, im Mai 2020 Dr. Oliver Bungartz

Vorwort zur ersten Auflage

Fehlende Kontrollen, mangelhaftes Risikomanagement, Wirtschaftskriminalität und Korruption werden in der Öffentlichkeit verstärkt diskutiert und scheinen in der Praxis an der Tagesordnung zu sein. Dabei lässt sich die Verpflichtung zur Einrichtung und Dokumentation eines Internen Kontrollsystems (IKS) als Verantwortlichkeit der Unternehmensleitung schon seit langer Zeit aus der deutschen Gesetzgebung herleiten. Das nationale Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sowie der Sarbanes-Oxley Act (SOX) auf internationaler Ebene sind nur zwei gesetzgeberische Meilensteine auf dem Weg zu einer weltweit neuen Überwachungskultur. In Deutschland ist dieser Trend zuletzt durch das Bilanzrechtsmodernisierungsgesetz (BilMoG) zur Transformation der 8. EU-Richtlinie ins nationale Recht verstärkt worden, in dem u. a. die Verpflichtung des Aufsichtsrats konkretisiert wurde, die Wirksamkeit des IKS, der Internen Revision und des Risikomanagementsystems zu beurteilen.

Vor diesem Hintergrund soll das hier vorliegende Handbuch eine geschlossene, ganzheitliche und praxisgerechte Konzeption für ein umfassendes und unternehmensweites IKS dienen, welches mit vertretbarem Aufwand zu realisieren ist und gleichzeitig nationalen sowie internationalen Standards genügt.

Kapitel I vermittelt die Grundlagen eines IKS in kompakter Form, um im folgenden Kapitel von Prozess zu Prozess an ein modernes und vollumfängliches IKS heranzuführen. Kapitel I enthält dabei alle Informationen zu einem IKS, die prozessübergreifend gültig sind, so dass sie in geschlossener Form der prozessorientierten Darstellung vorangestellt werden können. Das Rahmenwerk des Committee of Sponsoring Organizations of the Treadway Commission (COSO) dient dabei als Richtschnur für den Aufbau eines IKS und somit als Basis für das gesamte Handbuch.

Kapitel II enthält ausführliche Informationen zu wichtigen ausgewählten Prozessen:

- Beschaffung
- Produktion
- Absatz
- Anlagevermögen
- Personal
- Rechnungslegung
- Finanzen
- Steuern
- Informationstechnologie

Kapitel III gibt Hinweise für ein erfolgreiches Projektmanagement zur Prozessaufnahme, zur Implementierung, zu Prozessdurchlaufbeobachtungen und zur Optimierung eines IKS. Die Prüfung der Funktionsfähigkeit sowie die laufende Pflege eines IKS vervollständigen die Darstellung des Projektmanagements zur Implementierung. Aus der langjährigen Erfahrung im Aufbau von IKS in der Praxis werden abschließend zentrale Erfolgsfaktoren herausgearbeitet.

Kapitel IV gibt einen Ausblick auf die Erweiterung eines IKS von COSO I hin zu einem gesetzlich geforderten umfassenden Überwachungssystem (d.h. internes Kontroll-, Revisions- und Risikomanagementsystem). Als ganzheitliches Rahmenwerk zur Integration dieser drei Überwachungselemente wird das ERM-Modell (COSO II) für ein unternehmensweites Risikomanagement herangezogen.

Der Aufbau des Handbuchs ist im „Baukasten-Prinzip" gestaltet, d.h. jedes einzelne Kapitel ist für sich geschlossen dargestellt und kann isoliert gelesen werden. Darüber hinaus können auch einzelne Prozesse isoliert betrachtet werden, wobei für jeden dieser Prozesse die folgenden Aspekte behandelt werden:

- Allgemeine Informationen
- Risiko-Kontroll-Matrizen
- Fraud-Indikatoren
- Kennzahlen

Ein Werk wie das vorliegende ist stets in einem weiteren Sinn das Produkt einer Vielzahl von Personen, Quellen und Anregungen. Besonderer Dank gilt meinen Kollegen Maik Wellenbrock und Marco Michelsen von „RSM Altavis" in Hamburg, die mich mit wertvollen Anregungen, fachmännischem Rat und durch konstruktive Kritik unterstützt haben. Außerdem möchte ich mich bei den Herren Dr. Joachim Schmidt sowie Sebastian Engler vom Erich Schmidt Verlag in Berlin für die außergewöhnliche gute Zusammenarbeit und die schnelle Realisierung des Projekts bedanken. Nicht zuletzt gilt mein ganz besonderer Dank meiner Familie, der dieses Buch gewidmet ist.

Ich hoffe, Ihnen mit diesem Handbuch wertvolle Anregungen, Ideen und Hilfestellungen zum IKS geben zu können und wünsche Ihnen eine anregende und hilfreiche Lektüre. Für jegliche Rückfragen und Anregungen bin ich dankbar.

Hamburg, im Juli 2009 Dr. Oliver Bungartz

Inhaltsverzeichnis

Abkürzungsverzeichnis

A

Abb.	Abbildung
Abl.	Amtsblatt
Abs.	Absatz
ACFE	Association of Certified Fraud Examiners
AEAO	Anwendungserlass zur Abgabenordnung
AICPA	American Institute of Certified Public Accountants (CPAs)
AKEIÜ	Arbeitskreis „Externe und Interne Überwachung der Unternehmung“ der Schmalenbach-Gesellschaft für Betriebswirtschaftslehre e.V.
AktG	Aktiengesetz
AO	Abgabenordnung
APA	Advanced Pricing Agreements
APO	Align, Plan and Organise (Anpassung, Planung und Organisation)
Art.	Artikel
AStG	Außensteuergesetz
ATZ	Altersteilzeit
Aufl.	Auflage
AV	Anlagevermögen
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

B

BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAI	Build, Acquire and Implement (Aufbau, Beschaffung und Implementierung)
BCP	Business Continuity Plan
BDSG	Bundesdatenschutzgesetz
BewG	Bewertungsgesetz
BilMoG	Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz)
BMF	Bundesministerium der Finanzen
BMJ	Bundesministerium der Justiz
BörseG	Börsegesetz
BpO	Betriebsprüfungsordnung
BStBl.	Bundessteuerblatt
BT-Drucks.	Bundestags-Drucksache
Buchst.	Buchstabe
bzw.	beziehungsweise

C

CCSA	Certification in Control Self-Assessment
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFROI	Cash-Flow-Return On Investment
CIM	Computer Integrated Manufacturing
CMMI	Capability Maturity Model Integrated
CMS	Compliance Management System
COBIT	Control Objectives for Information and Related Technology
COO	Chief of Operations

COSO	The Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountant
CPO	Chief Purchasing Officer
CSA	Control Self-Assessment
C-SOX	China SOX

D

DBA	Doppelbesteuerungsabkommen
DCGK	Deutscher Corporate Governance Kodex
DD	Due Diligence
d.h.	das heißt
DIH	Days Inventory Held
DIIR	Deutsches Institut für Interne Revision e.V.
DOJ	Department of Justice
DPO	Days Payable Outstanding
DRP	Disaster Recovery Plan
DRS	Deutscher Rechnungslegungs Standard
DRSC	Deutsches Rechnungslegungs Standards Committee e. V.
DSGVO	Datenschutz-Grundverordnung
DSO	Days Sales Outstanding
DSS	Deliver, Service and Support (Bereitstellung, Betrieb und Unterstützung)

E

EBIT	Earnings Before Interest and Taxes
EBITDA	Earnings Before Interest, Taxes, Depreciation and Amortisation
EDI	Electronic Data Interchange
EDM	Evaluate, Direct and Monitor (Evaluierung, Vorgabe und Überwachung)
EGIT	Enterprise Governance of Information and Technology
EPS	Entwurf Prüfungsstandard
ERM	Enterprise Risk Management
ERP	Enterprise Ressource Planning
EStDV	Einkommensteuer-Durchführungsverordnung
EStG	Einkommensteuergesetz
et al.	et alii (und andere)
etc.	et cetera (und so weiter)
EU	Europäische Union
e.V.	eingetragener Verein
EWG	Europäische Wirtschaftsgemeinschaft

F

FAIT	Fachausschuss für Informationstechnologie
FCPA	U.S. Foreign Corrupt Practice Act
FGO	Finanzgerichtsordnung
FTE	Full Time Employee

G

GCC	Gerneral Computer Controls
GDPdU	Grundsätze zum Datenzugriff und zur Prüfung digitaler Unterlagen
GewStDV	Gewerbesteuer-Durchführungsverordnung
GewStG	Gewerbesteuergesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoB	Grundsätze ordnungsmäßiger Buchführung

GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GrStG	Grundsteuergesetz
GrEStG	Grunderwerbsteuergesetz
GuV	Gewinn- und Verlustrechnung

H

HGB	Handelsgesetzbuch
Hrsg.	Herausgeber(in)

I

IAASB	International Auditing and Assurance Standards Board
ICB	IPMA Competence Baseline
ID	Identifikation
i.d.R.	in der Regel
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IEC	International Electrotechnical Commission
i.e.S.	im engeren Sinne
IFAC	International Federation of Accountants
IfM	Institut für Mittelstandsforschung
IFRS	International Financial Reporting Standards
i.H.	in Hundert
IIA	Institute of Internal Auditors
IKS	Internes Kontrollsystem
inkl.	inklusive
insb.	insbesondere
IPMA	International Project Management Association
IRS	Internes Revisionssystem
i.S.d.	im Sinne des
i.S.v.	im Sinne von
ISA	International Standard on Auditing
ISACA	Information Systems Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management System oder Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITAC	IT Application Control
ITGC	IT General Control
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library

J

JIT	Just-In-Time

K

kg	Kilogramm
KMU	Kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KStG	Körperschaftsteuergesetz
KWG	Kreditwesengesetz

L

LG	Landesgericht
LStDV	Lohnsteuer-Durchführungsverordnung
lt.	laut

M

MaRisk	Mindestanforderungen an das Risikomanagement
MEA	Monitor, Evaluate and Assess (Überwachung, Evaluierung und Beurteilung)

N

N/A	Nicht Anwendbar
N.F.	Neue Fassung
No.	Number
Nr.	Nummer

O

o.O.	ohne Ort
OR	Obligationenrecht
ÖCGK	Österreichischer Corporate Governance Kodex
ÖNORM	Österreichische Norm(en)
ONR	Österreichische Regelwerke
OWiG	Ordnungswidrigkeitengesetz

P

PC	Personal Computer
PCAOB	Public Company Accounting Oversight Board
PH	Prüfungshinweis
PIR	Post-Implementation Review
PMBoK	Project Management Body of Knowledge
PRINCE2	Projects IN Controlled Environments 2
PS	Prüfungsstandard

Q

QA	Quality Assessment
QMS	Qualitätsmanagementsystem

R

RFID	Radio Frequency Identification
RKM	Risiko-Kontroll-Matrix
RMS	Risikomanagementsystem
ROCE	Return On Capital Employed
RONA	Return On Net Assets
ROS	Return On Sales
RS	Stellungnahme zur Rechnungslegung
RSA	Risk Self-Assessment

S

S.	Seite
SAS	Statement on Auditing Standard
SDLC	Software Development Life Cycle
SEC	Securities and Exchange Commission
Sec.	Section
SLA	Service Level Agreement
SOC	System and Organization Controls
sog.	sogenannte(r)
SolvV	Solvabilitätsverordnung
SOX	Sarbanes-Oxley Act
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

T

t	Tonne(n)
Tab.	Tabelle
TDSV	Telekommunikations-Datenschutzverordnung
TLoD	Three-Lines-of-Defense
TOGAF	The Open Group Architecture Framework
TQM	Total Quality Management
Tz.	Teilziffer

U

u.a.	unter anderem
UGB	Unternehmensgesetzbuch
UK	United Kingdom
UKBA	UK Bribery Act
URÄG	Unternehmensrechts-Änderungsgesetz
US(A)	United States (of America)
U.S.C.	United States Code
UStG	Umsatzsteuergesetz
UStR	Umsatzsteuer-Richtlinie
USV	Unterbrechungsfreie Stromversorgung

V

VAG	Versicherungsaufsichtsgesetz
Val IT	Value from IT Investments Framework
VerSanG	Gesetz zur Sanktionierung von verbandsbezogenen Straftaten (Verbandssanktionengesetz)
vgl.	vergleiche

W

WpHG	Wertpapierhandelsgesetz

Z

z.B.	zum Beispiel
Ziff.	Ziffer

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel I: Grundlagen eines Internen Kontrollsystems (IKS)

1 Einführung in ein Internes Kontrollsystem (IKS)

Ein allgemein **einheitliches Konzept** hinsichtlich der Strukturierung und Gestaltung eines Internen Kontrollsystems (IKS) ist erstmalig in den USA entwickelt worden. Dieses Konzept ist in Deutschland übernommen worden bzw. in nationale Standards und Empfehlungen eingeflossen, so dass auch die Definition von Begriff und Aufgaben eines IKS letztlich auf US-amerikanischen Vorgaben beruht.

1.1 Begriff und Aufgaben eines IKS

Nach dem IDW Prüfungsstandard „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (**IDW PS 261**)“[1] werden unter einem IKS die vom Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements

- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der Schutz des Vermögens, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),
- zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
- zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften.

---

[1] Zu einer tiefer gehenden Analyse hinsichtlich des Begriffs, den Aufgaben und Regelungsbereichen des IKS vgl. Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) (Hrsg.): Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261). In: Die Wirtschaftsprüfung 2006, S. 1433–1445. Gegenüber der alten Verlautbarung ergeben sich bei der Neufassung folgende Änderungen:

- Bedeutsame Schwächen des rechnungslegungsbezogenen IKS sind dem Aufsichtsorgan sowie den gesetzlichen Vertretern und ggf. anderen Führungskräften auf entsprechender Zuständigkeitsebene in angemessener Zeit und schriftlich vom Abschlussprüfer mitzuteilen
- Schriftliche Mitteilung des Abschlussprüfers hat eine Beschreibung der Schwächen, eine Erläuterung ihrer möglichen Auswirkungen sowie ausreichende Informationen aufzunehmen, um die Mitteilung richtig einordnen zu können
- Erfordernis der Berichterstattung in angemessener Zeit führt ggf. dazu, dass neben der Berichterstattung im Prüfungsbericht vorab gesondert schriftlich zu berichten ist

Vgl. Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) (Hrsg.): IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n. F.). In: IDW-Fachnachrichten 2012, S. 239–255.

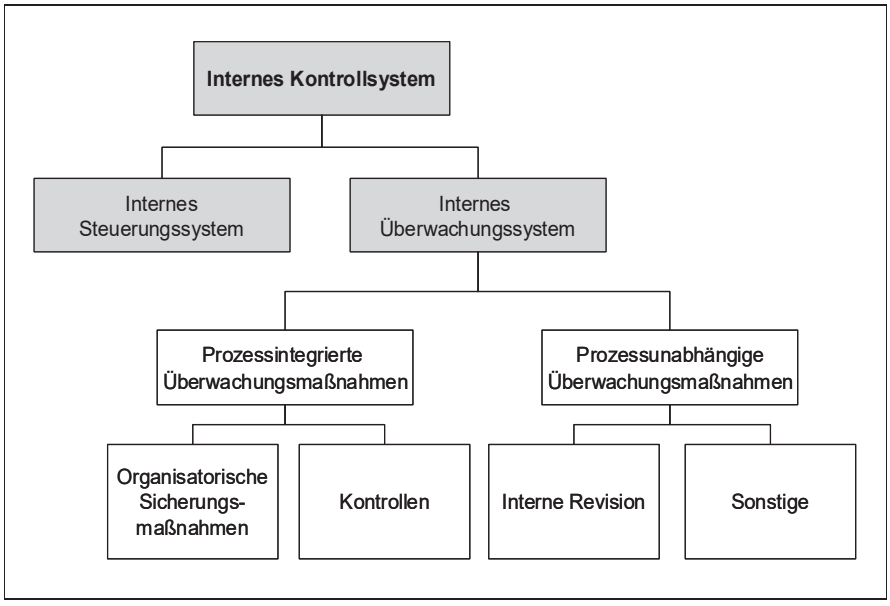
Ein IKS sollte nicht nur auf die Rechnungslegung beschränkt sein. Vielmehr sind **alle wesentlichen Geschäftsprozesse** in die Betrachtung einzubeziehen, um die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit sicherzustellen. Diese Forderung ergibt sich unter anderem aus der Begriffsdefinition des IKS, denn die „organisatorische Umsetzung von Entscheidungen der Unternehmensleitung" betrifft nicht nur den Bereich der Rechnungslegung, sondern alle wichtigen Entscheidungsfelder des Unternehmens.

Ein IKS hat die folgenden **Bestandteile**:

- Regelungen zur Steuerung der Unternehmensaktivitäten (internes Steuerungssystem) und
- Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem).

Das **interne Überwachungssystem** beinhaltet prozessintegrierte (organisatorische Sicherungsmaßnahmen, Kontrollen) und prozessunabhängige Überwachungsmaßnahmen (vor allem durch die Interne Revision):

Abb. 1: Regelungsbereiche eines IKS



Quelle: Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) (Hrsg.): IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n. F.). In: IDW-Fachnachrichten 2012, Tz. 20.

Organisatorische Sicherungsmaßnahmen werden durch laufende, automatische Einrichtungen wahrgenommen und umfassen fehlerverhindernde Maßnahmen, die sowohl in die Aufbau- als auch in die Ablauforganisation eines Unternehmens integriert sind und ein bestimmtes Sicherheitsniveau gewährleisten sollen (z. B. Funktionstrennung, Zugriffsbeschränkungen im IT-Bereich und Zahlungsrichtlinien).

Kontrollen erfolgen durch Maßnahmen, die in den Arbeitsablauf integriert sind. Erfolgen die Kontrollen durch Überwachungsträger, so können diese sowohl für das Ergebnis des überwachten Prozesses als auch für das Ergebnis der Überwachung verantwortlich sein. Kontrollen sollen vor allem die Wahrscheinlichkeit für das Auftreten von Fehlern in den Arbeitsabläufen vermindern bzw. aufgetretene Fehler aufdecken (z. B. Überprüfung der Vollständigkeit und Richtigkeit von empfangenen und weitergereichten Daten, manuelle Soll-Ist-Vergleiche und programmierte Plausibilitätsprüfungen).

Die **Interne Revision** ist eine prozessunabhängige Institution, die innerhalb eines Unternehmens Strukturen und Aktivitäten prüft und beurteilt. Dieser unternehmensinterne Überwachungsträger darf weder in den Arbeitsablauf integriert noch für das Ergebnis des überwachten Prozesses verantwortlich sein.

Daneben können **sonstige prozessunabhängige Überwachungsmaßnahmen** festgelegt sein, z. B. in Form von übergreifenden Kontrollen auf oberster Ebene (sog. High Level Controls), die im besonderen Auftrag der gesetzlichen Vertreter oder durch diese selbst vorgenommen werden.[2]

1.2 Internationale Anforderungen an ein IKS

Internationale Anforderungen (wie z. B. auch die Definition von Begriff und Aufgaben) an ein IKS sind ursprünglich in den USA entstanden. **Erfahrungswerte** zeigen, dass US-amerikanische Vorgaben mit einer gewissen zeitlichen Verzögerung auch Einfluss auf europarechtliche Entwicklungen haben.

US-amerikanische Vorgaben

Die wohl bekannteste Vorschrift hinsichtlich einer gesetzlichen Notwendigkeit zur Implementierung von detaillierten Maßnahmen zur Einrichtung, Dokumentation und

[2] Zu einer tiefer gehenden Analyse hinsichtlich des Begriffs, den Aufgaben und Regelungsbreichen des IKS vgl. Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) (Hrsg.): IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n. F.). In: IDW-Fachnachrichten 2012, Tz. 20.

Überprüfung von IKS resultiert aus dem am 30. Juli 2002 in Kraft getretenen **Sarbanes-Oxley Act (SOX)**, konkret aus der Section 404 „Management Assessment of Internal Controls".[3]

Mit der Verabschiedung des gesamten SOX-Regelwerks sollte vor allem das **Vertrauen der Investoren in die Kapitalmärkte** nach zahlreichen Bilanzskandalen bei US-amerikanischen Unternehmen wiederhergestellt werden. Hierzu wurden neben der Erweiterung der Offenlegungspflichten von Finanzinformationen der Unternehmen durch einen Bericht über das IKS zur Rechnungslegung und Finanzberichterstattung des Unternehmens auch zahlreiche weitere Vorschriften modifiziert sowie erstmalig gesetzlich verankert, die im Folgenden jedoch im Einzelnen nicht näher analysiert werden sollen.

Die **SOX Section 404**, die unbestritten den wohl größten Umsetzungsaufwand (sowohl zeit- als auch kostenmäßig) für Unternehmen im Rahmen aller SOX-Vorschriften verkörpert, weist als oberstes Ziel die Vermeidung von Fehlinformationen der Finanzberichterstattung aufgrund mangelhafter interner Kontrollen des Unternehmens aus:

Sarbanes-Oxley Section 404: Management Assessment of Internal Controls

(a) RULES REQUIRED. The Commission shall prescribe rules requiring each annual report required by section 78m(a) or 78o(d) of this title to contain an internal control report, which shall -
(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING. With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer, other than an issuer that is an emerging growth company (as defined in section 78c of this title), shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

[3] Vgl. Kongress der Vereinigten Staaten von Amerika (Hrsg.): The Sarbanes-Oxley Act of 2002 vom 30. Juli 2002.

> (c) EXEMPTION FOR SMALLER ISSUERS. Subsection (b) shall not apply with respect to any audit report prepared for an issuer that is neither a "large accelerated filer" nor an "accelerated filer" as those terms are defined in Rule 12b-2 of the Commission (17 C.F.R. 240.12b-2).

Konkret wird die Unternehmensleitung verpflichtet, ein **wirksames IKS** einzurichten und umfassend dessen Wirksamkeit zu dokumentieren. Gegenstand der Regelung sind hierbei sämtliche interne Kontrollen, die im Zusammenhang mit der Rechnungslegung stehen. Neben der Berichterstattung ist auch eine jährliche Einschätzung und Bewertung der Effektivität des IKS durch die Unternehmensleitung zu veröffentlichen. Diese Erklärung hat der Abschlussprüfer abschließend zu testieren und selbst eine eigene Stellungnahme über die Zuverlässigkeit des IKS abzugeben.

Der „Chief Executive Officer (CEO)" und der „Chief Financial Officer (CFO)" übernehmen zusätzlich auch die **persönliche Verantwortung** für die bei der U.S. Securities and Exchange Commission (SEC) eingereichten Berichte, da die Bestätigung der Vollständigkeit und Richtigkeit der im Rahmen der Finanzberichterstattung veröffentlichten Unterlagen auch Aussagen über das eingerichtete IKS umfasst. Bei fehlerhafter oder unrichtiger Bestätigung droht nach amerikanischem Recht dem CEO und dem CFO nach SOX Section 302 bzw. 906 eine verschärfte zivilrechtliche bzw. strafrechtliche Verfolgung.

Der Begriff des IKS sowie die konkrete Einrichtung und Dokumentation werden in SOX Section 404 nicht präzisiert. Als ein **mögliches Rahmenkonzept** wird u.a. der Bericht des Committee of Sponsoring Organizations of the Treadway Commission (COSO) empfohlen (sog. COSO-Report). Hinsichtlich des Dokumentations- und Bewertungsprozesses wird in der Praxis vor allem auf den speziellen Prüfungsstandard für die Prüfung des IKS vom Public Company Accounting Oversight Board (PCAOB) zurückgegriffen. Dieser ist zwar verbindlich nur für die Abschlussprüfer zu berücksichtigen, stellt jedoch aufgrund der Testatsvergabe auch Anforderungen an das Management dar.[4]

Section 404 des SOX Act und die dazu erlassenen Verordnungen der SEC verlangen, dass jeder bei der SEC eingereichte Jahresbericht eines Emittenten einen **Bericht über die Wirksamkeit des IKS zur finanziellen Berichterstattung** beinhaltet. Die

[4] Vgl. „Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements" der Securities and Exchange Commission (SEC) vom 17.06.2004, der inzwischen ersetzt wurde durch „Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements" (verabschiedet durch die SEC am 25.07.2007 und gültig für Abschlussprüfungen von Jahren, die am oder nach dem 15.11.2007 enden). Für allgemeine Informationen rund um das Public Company Accounting Oversight Board (PCAOB) und die U.S. Securities and Exchange Commission (SEC) wird auf die folgenden Internetadressen: www.pcaob.org und www.sec.gov verwiesen.

Regelung ist verpflichtend für alle Unternehmen, die den öffentlichen Kapitalmarkt in den USA in Anspruch nehmen (d.h. Handel an einer nationalen Börse, außerbörslicher Handel oder öffentliches Angebot von Wertpapieren), sowie die Tochtergesellschaften der Emittenten.[5]

In diesem Zusammenhang mag es auf den ersten Blick verwundern, dass gerade die neuesten regulatorischen Trends in Bezug auf SOX an **kleine und mittelständische Unternehmen** adressiert sind. So haben das PCAOB im Auditing Standard No. 5 als auch die SEC und COSO Standards und Entwürfe veröffentlicht, die Erleichterungen für kleine und mittelständische Unternehmen beinhalten.[6]

Die Standards und Entwürfe zielen darauf ab, die Einhaltung der Vorschriften der Section 404 auch für kleine und mittlere Unternehmen in einem **vertretbaren Zeit- und Kostenaufwand** zu erfüllen. Angesprochen sind in diesem Zusammenhang vor allem die Tochterunternehmen, die aufgrund einer Inanspruchnahme des US-Kapitalmarkts durch ihre Muttergesellschaft und Wesentlichkeitsbetrachtungen innerhalb des Konzerns ebenfalls unter die Bestimmungen der Section 404 fallen. Die letzten Jahre haben gezeigt, dass die Regelungen für große Aktiengesellschaften nicht einfach auf kleine und mittelständische Unternehmen übertragen werden können.

Die folgenden Standards und Entwürfe enthalten beispielsweise **Erleichterungen für kleine und mittelständische Unternehmen**:

- Committee of Sponsoring Organizations of the Treadway Commission (COSO): The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition, June 2013.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Guidance on Monitoring Internal Control Systems. February 4th, 2009.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control over Financial Reporting – Guidance for Smaller Public Companies. July 11th, 2006.
- Advisory Committee on Smaller Public Companies to the U.S. Securities and Exchange Commission (SEC): Final Report of the Advisory Committee on Smaller Public Companies to the U.S. Securities and Exchange Commission. April 4th, 2006.

5 Vgl. auch Menzies, Christof (Hrsg.): Sarbanes-Oxley Act. Professionelles Management interner Kontrollen. Stuttgart 2004, S. 13–14.

6 Vgl. Bungartz, Oliver und Marc Szackamer: Interne Kontrollsysteme in kleinen und mittelständischen Unternehmen. In: Zeitschrift für Corporate Governance 2007, S. 123–130 sowie Bungartz, Oliver und Marc Szackamer: Notwendigkeit und Aufbau von Internen Kontrollsystemen in Unternehmen. In: Steuer-Journal 2007, S. 45–50.

Chinesische Vorgaben

Nach den im Jahre 2008 durch das chinesische Finanzministerium in Zusammenarbeit mit weiteren Behörden und Einrichtungen verabschiedeten **„Basic Standards for Enterprise Internal Control“** (häufig auch bezeichnet als China-SOX oder C-SOX), müssen an der Börse (insb. Shanghai Stock Exchange und Shenzen Stock Exchange) notierte sowie mittelgroße und große nicht notierte Unternehmen ein IKS nachweisen können (vgl. Art. 2 der Basic Standards for Enterprise Internal Control).[7]

Die Basic Standards bestehen aus sieben Kapiteln, in denen die generellen Regelungen sowie **fünf Komponenten** beschrieben werden, die weitgehend mit dem COSO-Rahmenwerk übereinstimmen:[8]

- Internes Umfeld
- Risikobeurteilung
- Kontrollaktivitäten
- Information und Kommunikation
- Interne Überwachung

Die „Basic Standards for Enterprise Control“ wurden im Jahr 2010 um die von Finanzministerium, Börsenaufsicht, Revisionskommission, Bankenaufsicht und Versicherungsaufsicht verabschiedeten **„Guidelines for the Internal Control of Companies“** ergänzt, die sich aus den folgenden drei Bestandteilen zusammensetzen:[9]

- „Application Guidelines for the Internal Control of Companies“
- „Evaluation Guidelines for the Internal Control of Companies“
- „Auditing Guidelines for the Internal Control of Companies“

Im Gegensatz zu vielen anderen nationalen Gesetzgebungen zielen die chinesischen Vorgaben nicht nur auf Kontrollen im Bereich der Rechnungslegung und der finanziellen Berichterstattung ab, sondern fordern explizit auch Kontrollen über das **operative Geschäft, Korruption und allgemeine Compliance-Themen**.

---

7 Vgl. Takahiro, Sato und Pan Jia: Comparison of Internal Control Systems in Japan and China. In: International Journal of Business Administration. Januar 2012, S. 72; da die originalen Gesetzestexte nur in chinesischer Sprache verfügbar sind, wird in dieser Übersicht auf direkte Zitate aus dem Gesetz verzichtet.

8 Vgl. Strasser, Anne-Katrin: How to tackle C-SOX? – The success formula for the implementation of the Basic Standard for Enterprise Internal Control – the Chinese answer to the Sarbanes-Oxley-Act. Norderstedt 2009, S. 9.

9 Vgl. Takahiro, Sato und Pan Jia: Comparison of Internal Control Systems in Japan and China. In: International Journal of Business Administration. Januar 2012, S. 67.

Die **Verantwortung** für die Implementierung und jährliche Selbstbeurteilung des IKS liegt nach Art. 12 der Basic Standards bei der Unternehmensleitung, wobei in die Beurteilung ein durch das Unternehmen einzurichtender Prüfungsausschuss einbezogen werden muss. Der Prüfungsausschuss – als unabhängige Instanz – soll für die Durchführung der Selbstbeurteilung sorgen und diese überwachen (vgl. Art. 62 der Basic Standards).[10]

Die **Selbstbeurteilung** wird weiter konkretisiert in Art. 46 der Basic Standards, in dem die Durchführung der Selbstbeurteilung in Bezug auf die Funktionsweise der internen Kontrollen vorgeschrieben wird. Das Unternehmen hat darüber zu berichten. Ähnlich wird dies auch in den „Evaluation of Internal Control Guidelines" gefordert, wo diese Beurteilung als ein Prozess zur Prüfung der Funktionsfähigkeit des IKS inkl. anschließender Berichterstattung durch die Unternehmensleitung und das Management beschrieben wird.[11]

Das **primäre Ziel** der verabschiedeten Standards und Verlautbarungen ist – wie in anderen Ländern auch – die Erhöhung der Effektivität interner Kontrollen und die damit verbundene Reduzierung des Risikos für die betroffenen Unternehmen sowie insb. die Shareholder und Stakeholder der Unternehmen.[12]

In den oben beschriebenen Richtlinien ist die Frage nach der Notwendigkeit sowie Art und Weise einer **Bestätigung durch einen externen Prüfer** (Abschlussprüfer) nicht eindeutig beantwortet. Lediglich aus z. B. den „Internal Control Guidelines for Listed Companies on the Shanghai Stock Exchange" kann abgeleitet werden, dass zeitgleich mit der Veröffentlichung des jährlichen Berichts zur Funktionsfähigkeit der internen Kontrollen durch die Unternehmensleitung das Testat eines Wirtschaftsprüfers zu veröffentlichen ist (vgl. Art. 32). Nach Art. 32 muss der Abschlussprüfer die Berichte über die Selbstbeurteilung prüfen und verifizieren. Art. 10 der Basic Standards besagt, dass der vom Unternehmen beauftragte Abschlussprüfer selbst die Funktionsfähigkeit zu prüfen hat, erwähnt jedoch keine Form der Bestätigung. Im Art. 66 der „Internal Control Guidelines for Listed Companies on the Shenzhen Stock Exchange" wird darüber hinaus verlangt, dass das Unternehmen seinen Bericht über die Selbstbeurteilung zusammen mit der Bestätigung des Abschlussprüfers innerhalb von vier Monaten nach Abschluss des Geschäftsjahres zu übermitteln und diesen gemeinsam mit dem Jahresabschluss zu veröffentlichen hat.[13]

---

10 Vgl. Takahiro, Sato und Pan Jia: Comparison of Internal Control Systems in Japan and China. In: International Journal of Business Administration. Januar 2012, S. 72.

11 Vgl. Takahiro, Sato und Pan Jia: Comparison of Internal Control Systems in Japan and China. In: International Journal of Business Administration. Januar 2012, S. 72.

12 Vgl. Strasser, Anne-Katrin: How to tackle C-SOX? – The success formula for the implementation of the Basic Standard for Enterprise Internal Control – the Chinese answer to the Sarbanes-Oxley-Act. Norderstedt 2009, S. 9.

13 Vgl. Takahiro, Sato und Pan Jia: Comparison of Internal Control Systems in Japan and China. In: International Journal of Business Administration. Januar 2012, S. 72–73.

Europarechtliche Vorgaben

Die bisher noch weitestgehend abgrenzbare Anzahl von Unternehmen, die sich explizit verpflichtend mit der Ausgestaltung von IKS beschäftigen müssen, wird sich zukünftig aufgrund europarechtlicher Vorgaben deutlich erhöhen. Maßnahmen zur Regulierung des US-amerikanischen Kapitalmarkts waren in der Vergangenheit häufig Anstoß für vergleichbare rechtliche Veränderungen in Europa und somit nachfolgend auch in Deutschland. Auch bei der vollzogenen **Änderung der 4., der 7. und der 8. EU-Richtlinie** sind einzelne Elemente der SOX Section 404 in modifizierter, wenn auch abgeschwächter Form, berücksichtigt worden. Die geänderte 4. und 7. EU-Richtlinie ist ebenso wie die Umsetzung der 8. EU-Richtlinie durch den deutschen Gesetzgeber in nationales Recht zu transformieren:

– **Verbale Darstellung im (Konzern-) Lagebericht**: Die hier relevanten Änderungen und Erweiterungen ergeben sich bei der geänderten 4. und 7. EU-Richtlinie vor allem durch die Einfügung von Art. 46a[14], der von allen Unternehmen, deren Wertpapiere zum Handel an einem geregelten Markt im Sinne der Europäischen Union zugelassen sind, eine Beschreibung der wichtigsten Merkmale des internen Kontroll- und des Risikomanagementsystems der Gesellschaft im Hinblick auf den Rechnungslegungsprozess fordert. Diese Beschreibung, als Bestandteil des jährlich zu veröffentlichenden „Corporate Governance Statement", kann entweder als gesonderter Abschnitt im Lagebericht oder in einem gesonderten Bericht erfolgen, der zusammen mit dem Lagebericht offen gelegt wird oder auch nur durch eine Bezugnahme im Lagebericht, falls dieses Dokument auf der Internetseite der Gesellschaft öffentlich zugänglich ist (wahlweise durch die Mitgliedstaaten in nationales Gesetz transformierbar). In jedem Fall hat jedoch der Abschlussprüfer eine Einklangsprüfung dieser Beschreibung vorzunehmen, d.h. es ist zu überprüfen, ob die Angaben mit dem Jahresabschluss in Einklang stehen. Diese Einklangsprüfung ist jedoch nicht vergleichbar mit den umfassenden SOX-Anforderungen bezüglich der Prüfungstätigkeit des Abschlussprüfers.[15]

[14] Vgl. für die sog. „Abänderungs-Richtlinie": Europäisches Parlament und Rat (Hrsg.): Richtlinie 2006/46/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 zur Änderung der Richtlinien des Rates 78/660/EWG über den Jahresabschluss von Gesellschaften bestimmter Rechtsformen, 83/349/EWG über den konsolidierten Abschluss, 86/635/EWG über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten und 91/674/EWG über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen. In: Abl. L224 vom 16.08.2006.

[15] Hier sei nur kurz darauf hingewiesen, dass eine Effizienzüberprüfung der internen Kontrollen durch den Abschlussprüfer nicht Bestandteil der Regelung ist.

– **Konkretisierung der Überwachungspflicht:** Entsprechend Art. 41[16] hat zunächst jedes Unternehmen von öffentlichem Interesse grundsätzlich einen Prüfungsausschuss (sog. Audit Committee) zu bilden. Die Aufgabe dieses Prüfungsausschusses besteht dabei unabhängig von der Verantwortung der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des geprüften Unternehmens u. a. auch darin, den Rechnungslegungsprozess und die Wirksamkeit des IKS, ggf. des internen Revisionssystems und des Risikomanagementsystems des Unternehmens zu überwachen, wobei insb. das Kriterium der Wirksamkeit den Prüfungsausschuss vor eine nicht zu unterschätzende Herausforderung stellen dürfte. Entsprechend den Ausnahmemöglichkeiten im Sinne der EU-Mitgliedstaatenwahlrechte des Art. 41 ist es hierbei auch möglich, dass bei kleinen und mittleren Unternehmen von öffentlichem Interesse die Funktion des Audit Committee durch den Aufsichtsrat insgesamt ausgeübt oder auch auf einen Ausschuss eines bereits gesetzlich vorgesehenen Unternehmensorgans zurückgegriffen werden kann.

Eine gesetzliche Konkretisierung von Sorgfaltspflichten hinsichtlich der Überwachung der Wirksamkeit des IKS wird eine neue Stufe der Überwachungskultur einleiten, die dazu führen kann, dass ein Verstoß gegen die Sorgfaltspflichten eher festgestellt wird. Die beabsichtigte Konkretisierung schafft somit mittelbar einen Anreiz für die Mitglieder des Aufsichtratsausschusses **stringentere Kontrollsysteme und Informationsabläufe** zu installieren, um mögliche Überwachungsdefizite von vornherein zu minimieren. Aber auch die übrigen Mitglieder des Aufsichtsrats werden sich aufgrund ihrer allgemeinen Überwachungspflicht verstärkt um die ordnungsmäßige Überwachung des IKS bemühen, denn eine Befreiung von der allgemeinen Sorgfaltspflicht hat die Bildung von Ausschüssen nach geltender Rechtslage nicht zur Folge.

Letztendlich werden auch die **Anforderungen an die Ausgestaltung und Überwachung des IKS durch die gesetzlichen Vertreter** erhöht. Die gesetzlichen Vertreter und nicht der Aufsichtsrat oder ein Aufsichtsratsausschuss tragen die primäre Verantwortung für die Aufstellung von Jahres- und Konzernabschlüssen, aber auch für das IKS, die Interne Revision und das Risikomanagementsystem. Diese konkrete Verantwortung kann (auch indirekt) nicht einem Aufsichtsratsausschuss übertragen werden.

Diese Betrachtungsweise ist insb. auch durch eine Änderung der 4. und 7. EU-Richtlinie nochmals klargestellt worden. Es wurde verdeutlicht, dass zwar eine gemeinsame Verantwortlichkeit der Verwaltungs-, Leitungs- und Aufsichtsorgane der Gesellschaft für die Rechnungslegung und das Corporate Governance Statement

[16] Vgl. zur sog. „Abschlussprüfer-Richtlinie“: Europäisches Parlament und Rat (Hrsg.): Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates. In: Abl. L 157 vom 9.06.2006.

besteht, die jeweiligen Organe aber im Rahmen der ihnen durch innerstaatliches Recht zugewiesenen Zuständigkeiten handeln. Die kollektive Gesamtverantwortung von Vorstand und Aufsichtsrat für die Erstellung des Jahresabschlusses wird abgelehnt. Es wird vermutet, dass auch hinsichtlich der Überwachungstätigkeit des IKS nur die **wesentlichen Geschäftsprozesse des Unternehmens** mit einzubeziehen sind. Diese sind unter Berücksichtigung einer risikoorientierten Vorgehensweise nach US-amerikanischem Vorbild zu ermitteln. Die Überwachung aller Geschäftsprozesse würde zu einem nicht vertretbaren finanziellen, personellen und zeitlichen Aufwand führen.

Die Analyse der europarechtlichen Vorgaben zeigt, dass nicht nur die Beschreibung der wichtigsten Merkmale des IKS und des Risikomanagementsystems des Unternehmens im Hinblick auf den Rechnungslegungsprozess durch die gesetzlichen Vertreter vorzunehmen ist, sondern zusätzlich auch gewährleistet sein muss, dass die Wirksamkeit des IKS, ggf. des internen Revisionssystems, und des Risikomanagementsystems des Unternehmens **adäquat überwacht** werden kann.

Der Gesetzgeber hat darauf verzichtet, konkrete und explizite Anforderungen an ein IKS zu stellen bzw. dessen regelmäßige Effektivitätsmessung im Gesetz zu kodifizieren. Der Aufsichtsrat bzw. ein Prüfungsausschuss des Aufsichtsrats muss allerdings entsprechende **Effektivitätstests** durchführen und dokumentieren lassen, wenn die Wirksamkeit des IKS überwacht werden soll. Ob sich durch die Formulierung der EU-Richtlinien implizit vielleicht doch noch die gesetzliche Pflicht zur Durchführung von Effektivitätsmessungen analog der SOX-Vorschriften ergeben kann, ist von der Durchsetzung des geltenden Rechts und der Rechtsprechung in diesem Zusammenhang abhängig.

Die **Umsetzung der europarechtlichen Vorgaben** hat ebenfalls Auswirkungen auf die österreichische Gesetzgebung. Dabei wurden die Anforderungen an ein IKS zwar vom Gesetzgeber in neuen Gesetzen definiert, die Ausgestaltung wurde jedoch nicht näher präzisiert.

Österreichische Vorgaben

Der österreichische Gesetzgeber hat mit dem **Unternehmensrechts-Änderungsgesetz 2008 (URÄG)** versucht, eine Verbesserung der Transparenz der Finanzberichterstattung herbeizuführen. Neben der Stärkung des Vertrauens in die Tätigkeiten des Abschlussprüfers hat das Gesetz eine Konkretisierung der Anforderung an ein IKS zum Ziel.[17]

[17] Vgl. für den Wortlaut des URÄG 2008: Bundesministerium für Justiz (BMJ): Unternehmensrechts-Änderungsgesetz – URÄG 2008 vom 7. Mai 2008. In: BGBl. I Nr. 70/2008. Abrufbar unter: www.ris.bka.gv.at.

Primär handelt es sich dabei um neue **Offenlegungspflichten zum IKS** und Risikomanagementsystem im Lagebericht von kapitalmarktorientierten Unternehmen. Die Beschreibung der Ausgestaltung und Merkmale des vorhanden IKS und Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess[18] hat dabei sowohl für den Konzern- als auch für den Jahresabschluss zu erfolgen. Neben börsennotierten Gesellschaften sind nun auch jene Unternehmen verpflichtet, die börsennotierte Wertpapiere emittiert haben. Die neu geregelten Offenlegungspflichten sind mit 1. Januar 2009 in Kraft getreten und auf alle Geschäftsjahre anzuwenden, die nach dem 31. Dezember 2008 beginnen:

„Eine Gesellschaft nach § 189a Z 1 lit. a hat im Lagebericht darüber hinaus die wichtigsten Merkmale des internen Kontroll- und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess zu beschreiben." **(§ 243a Abs. 2 UGB)**

Neben der Aufnahme einer Stellungnahme zum IKS und zum Risikomanagement des Unternehmens im Lagebericht, hat der Gesetzgeber auch die Überwachung der Wirksamkeit des IKS durch den **Aufsichtsrat** bzw. einen ggf. einzurichtenden Prüfungsausschuss durch das URÄG 2008 gesetzlich neu geregelt:

Zu den Aufgaben des Aufsichtsrats bzw. Prüfungsausschusses gehört die Überwachung der Wirksamkeit des internen Kontrollsystems, ggf. des internen Revisionssystems und des Risikomanagementsystems der Gesellschaft (vgl. **§ 92 Abs. 4a Nr. 4b) AktG**).[19]

Die **Bestätigung des Abschlussprüfers**, dass die Aussagen zum IKS im Lagebericht hinsichtlich des Rechnungslegungsprozesses im Einklang mit dem Jahresabschluss stehen und die Angaben des § 243a UGB zutreffen, wurden im § 274 Abs. 5 UGB neu geregelt. Ebenso wurde eine Rede- und Warnpflicht des Abschlussprüfers bei der Feststellung von wesentlichen Schwächen der internen Kontrollen des Rechnungslegungsprozesses in § 273 Abs. 2 UGB neu aufgenommen:

„Der Bestätigungsvermerk umfasst ferner
1. ein Urteil darüber, ob der Lagebericht oder Konzernlagebericht
   a. mit dem Jahresabschluss beziehungsweise Konzernabschluss des betreffenden Geschäftsjahres in Einklang steht,
   b. nach den geltenden rechtlichen Anforderungen aufgestellt wurde und
   c. gegebenenfalls zutreffende Angaben nach § 243a enthält sowie

[18] Der Prozess der Rechnungslegung beschränkt sich nicht nur auf die Rechnungslegung, sondern bezieht die buchmäßige Erfassung aller relevanten unternehmensspezifischen Daten mit ein.

[19] Für ähnliche Regelungen in Bezug auf Unternehmen anderer Rechtsform vgl. beispielsweise § 30g Abs. 4a GmbHG und § 24c Abs. 6 GenG.

2. eine Erklärung, ob angesichts der bei der Prüfung gewonnenen Erkenntnisse und des gewonnenen Verständnisses über das Unternehmen und sein Umfeld wesentliche fehlerhafte Angaben im Lagebericht beziehungsweise Konzernlagebericht festgestellt wurden, wobei auf die Art dieser fehlerhaften Angaben einzugehen ist.“ **(§ 274 Abs. 5 UGB)**

„Stellt der Abschlussprüfer bei Wahrnehmung seiner Aufgaben Tatsachen fest, die den Bestand des geprüften Unternehmens oder Konzerns gefährden oder seine Entwicklung wesentlich beeinträchtigen können oder die schwerwiegende Verstöße der gesetzlichen Vertreter oder von Arbeitnehmern gegen Gesetz, Gesellschaftsvertrag oder Satzung erkennen lassen, so hat er darüber unverzüglich zu berichten. Darüber hinaus hat er unverzüglich über wesentliche Schwächen bei der internen Kontrolle des Rechnungslegungsprozesses zu berichten.“ **(§ 273 Abs. 2 UGB)**

Gesetzliche Verpflichtungen zur **Führung eines IKS**, das den Anforderungen des Unternehmens entspricht, ergeben sich außerdem aus dem § 82 AktG und dem § 22 GmbHG:

„Der Vorstand hat dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“ **(§ 82 AktG)**

„Die Geschäftsführer haben dafür zu sorgen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.“ **(§ 22 Abs. 1 GmbHG)**

Neben den gesetzlichen Verpflichtungen ergeben sich für Unternehmen zusätzlich auch Regelungen zum IKS aus dem **Österreichischen Corporate Governance Kodex (ÖCGK)**.[20]

„… Der Prüfungsausschuss ist insbesondere für die Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontroll- und Risikomanagementsystems … zuständig.“ **(Regel 40, ÖCGK 2020)**

„Die Gesellschaft legt im Konzernlagebericht eine angemessene Analyse des Geschäftsverlaufes vor und beschreibt darin ihre wesentlichen Risiken und Ungewissheiten sowie die wichtigsten Merkmale des internen Kontrollsystems und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess …“ **(Regel 69, ÖCGK 2020)**

[20] Österreichischer Arbeitskreis für Corporate Governance (Hrsg.): Österreichischer Corporate Governance Kodex in der Fassung vom Jänner 2020. Abrufbar unter: www.corporate-governance.at.

Schweizerische Vorgaben

Ähnlich der Regelungen in Österreich wurden auch in der Schweiz **gesetzliche Änderungen in Bezug auf das IKS** eingeführt. Mit dem Ziel die Corporate Governance zu verbessern und die schweizerische Gesetzgebung an internationale Entwicklungen anzupassen, wurden verschiedene Änderungen des Gesellschaftsrechts sowie des Revisionsaufsichtsrechts eingeführt. Wie schon in Österreich war das Ziel in der Schweiz, eine Verbesserung der Transparenz und ein ausgewogenes Verhältnis zwischen Führung und Kontrolle zu schaffen.[21]

Ausgelöst durch die am 1. Januar 2008 in Kraft getretenen Änderungen des Obligationenrechts (OR)[22], müssen Unternehmen, unabhängig von ihrer Rechtsform, ein **IKS nachweisen, sofern sie der ordentlichen Revision unterliegen** (vgl. Art. 728a Abs. 1 Ziff. 3 OR).

Unternehmen, die der ordentlichen Revision unterliegen, sind im OR wie folgt definiert:

„1) Folgende Gesellschaften müssen ihre Jahresrechnung und gegebenenfalls ihre Konzernrechnung durch eine Revisionsstelle ordentlich prüfen lassen

1. Publikumsgesellschaften; als solche gelten Gesellschaften, die:
   a. Beteiligungspapiere an einer Börse kotiert haben,
   b. Anleihensobligationen ausstehend haben,
   c. mindestens 20 Prozent der Aktiven oder des Umsatzes zur Konzernrechnung einer Gesellschaft nach Buchstabe a oder b beitragen;
2. Gesellschaften, die zwei der nachstehenden Größen in zwei aufeinander folgenden Geschäftsjahren überschreiten:
   a. Bilanzsumme von 20 Millionen Franken,
   b. Umsatzerlös von 40 Millionen Franken,
   c. 250 Vollzeitstellen im Jahresdurchschnitt;

[21] Vgl. Pfaff, Dieter: IKS-Leitfaden. Empfehlungen des veb.ch zum internen Kontrollsystem IKS und zu den Angaben über die Risikobeurteilung im Anhang. Zürich 2008. Abrufbar unter: www.veb.ch sowie Schweizerischer Bundesrat: Botschaft zur Änderung des Obligationenrechts (Aktienrecht und Rechnungslegungsrecht sowie Anpassungen im Recht der Kollektiv- und der Kommanditgesellschaft, im GmbH-Recht, Genossenschafts-, Handelsregister- sowie Firmenrecht) vom 21. Dezember 2007, S. 1606–1607 (abrufbar unter: www.admin.ch) wonach die Corporate Governance durch eine effiziente unternehmensinterne Kontrolle wirtschaftliche Fehlentwicklungen im volkswirtschaftlichen Interesse so weit wie möglich vermieden werden sollen.

[22] Vgl. Bundesversammlung der Schweizerischen Eidgenossenschaft: Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Stand am 1. Januar 2017). Abrufbar unter: www.admin.ch.

3. Gesellschaften, die zur Erstellung einer Konzernrechnung verpflichtet sind.

2) Eine ordentliche Revision muss auch dann vorgenommen werden, wenn Aktionäre, die zusammen mindestens 10 Prozent des Aktienkapitals vertreten, dies verlangen.

3) Verlangt das Gesetz keine ordentliche Revision der Jahresrechnung, so können die Statuten vorsehen oder kann die Generalversammlung beschließen, dass die Jahresrechnung ordentlich geprüft wird." (**Art. 727 OR**)

Die Revisionsstelle prüft **nach Art. 728a Abs. 1 OR**, ob

1. die Jahresrechnung und ggf. die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;
2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinns den gesetzlichen Vorschriften und den Statuten entspricht;
3. **ein IKS existiert („Existenzprüfung")**.

Nach **Art. 728a Abs. 2 OR** berücksichtigt die Revisionsstelle bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das IKS.

Neben der Überprüfung der Existenz eines IKS, hat die Revisionsstelle zu prüfen, ob der Verwaltungsrat **Maßnahmen zur Sicherstellung einer ordnungsgemäßen Buchführung und Rechnungslegung** getroffen hat und ob diese Maßnahmen eingehalten werden. Stellt die Revisionsstelle dabei fest, dass das IKS Mängel aufweist, so kompensiert sie diese durch eigene Prüfungshandlungen. Andererseits berücksichtigt die Revisionsstelle das IKS bei der Festlegung des Umfangs ihrer Prüfungen. Über die Feststellungen hat sie der Generalversammlung summarisch und dem Verwaltungsrat umfassend Bericht erstatten:

„Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision." (**Art. 728b Abs. 1 OR**)

Der Gesetzgeber hat **konkrete Hinweise unterlassen**, wie die Ausgestaltung eines IKS, die Dokumentation und Anhangsangaben sowie die Existenzprüfung zu erfolgen haben. Hinsichtlich des Art. 728a OR hat der Bundesrat präzisiert, dass das IKS im Sinne dieses Artikels lediglich die Buchführung und Rechnungslegung betrifft. Operative Prozesse und Compliance (Regeleinhaltung) sind – sofern keine Auswirkungen auf die Jahresrechnung bestehen – nicht betroffen.[23]

[23] Vgl. auch Treuhand-Kammer – Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems vom 17. Dezember 2007, Ziff. I, Buchst. c.

Bei Prüfung der Existenz eines IKS kann der **Schweizer Prüfungsstandard „Prüfung der Existenz des internen Kontrollsystems (PS 890)**[24] eine Hilfestellung leisten. Demnach kann nach Auffassung der Treuhand-Kammer von der Existenz eines IKS insb. dann ausgegangen werden, wenn

– das IKS vorhanden und überprüfbar (d.h. dokumentiert) ist;
– das IKS den Geschäftsrisiken und der Geschäftstätigkeit angepasst ist;
– das IKS den zuständigen Mitarbeitenden bekannt ist;
– das definierte IKS angewendet wird;
– ein Kontrollbewusstsein im Unternehmen vorhanden ist.[25]

Das **IKS ist nach Auffassung der Treuhandkammer derart zu dokumentieren**, dass wesentliche Vorgänge nachvollzogen werden können. Auf Unternehmensebene muss die Dokumentation darlegen,

– was der Verwaltungsrat mit dem IKS erreichen will;
– wie die Unternehmensleitung das IKS umsetzt;
– wie die Risiken einer wesentlichen falschen Angabe in der Buchführung und Rechnungslegung eingeschätzt werden und
– wie das IKS solche Risiken verhindern oder vermindern soll.[26]

Des Weiteren bezieht sich die Schweizer Treuhandkammer in ihrem Prüfungsstandard PS 890 bei der Ausgestaltung und des Umfangs eines IKS auf die **Größe des Unternehmens, die Komplexität der Geschäftstätigkeit und die Art der Finanzierung**.

Für größere, insb. auch international tätige Unternehmen scheint unter diesen Umständen die Anwendung eines **international anerkannten Rahmenwerks** sinnvoll zu sein, um den gesetzlichen Anforderungen gerecht zu werden (z.B. COSO). Gerade für kleine und mittlere Unternehmen kann diese Gesetzesnovelle des Jahres 2008 von großer Bedeutung sein und einen erheblichen Mehraufwand im Sinne

[24] Vgl. Treuhand-Kammer – Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems vom 17. Dezember 2007. Der Prüfungsstandard gilt für Prüfungen der Existenz des internen Kontrollsystems für Perioden, die am 1. Januar 2008 oder danach beginnen. Abrufbar unter: www.treuhand-kammer.ch.

[25] Vgl. Treuhand-Kammer – Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems vom 17. Dezember 2007, Ziff. VII, Buchst. a und b.

[26] Vgl. Treuhand-Kammer – Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems vom 17. Dezember 2007, Ziff. VII, Buchst. c.

eines erhöhten Dokumentationsaufwands bedeuten, da der Gesetzgeber in der Ausgestaltung der Gesetzestexte auf eine Beschränkung hinsichtlich der Unternehmensgröße verzichtet hat.

Die Treuhandkammer fasst zusammen, dass i.S.d. schweizerischen Gesetzes (Art. 716a Abs. 1 Ziff. 3 i.V.m. Art. 662a sowie Art. 957ff. OR) der Verwaltungsrat für die **Ausgestaltung, Implementierung und Aufrechterhaltung eines geeigneten und angemessenen IKS** verantwortlich ist. Nach Art. 728a Abs. 1 Ziff. 3 OR bestätigt die Revisionsstelle einmal jährlich die Existenz dieses vom Verwaltungsrat definierten IKS. Die Revisionsstelle wird die Existenz i.S.v. Art. 728a Abs. 1 Ziff. 3 OR gegenüber der Generalversammlung positiv bestätigen können, sofern das vom Verwaltungsrat definierte IKS den minimalen Anforderungen aufgrund der Größe, Komplexität und dem Risikoprofil des Unternehmens entspricht. Voraussetzung dieser Existenzbestätigung ist jedoch, dass das vom Verwaltungsrat definierte IKS schriftlich dokumentiert ist und im Tagesgeschäft des Unternehmens angewendet wird. Die Dokumentation der Ausgestaltung und die Umsetzung des IKS sind von der Revisionsstelle im Rahmen der Jahresabschlussprüfung zu prüfen („Implementierung" und „Aufbau"). Nicht Bestandteil der „Existenzprüfung" des IKS nach Art. 728a Abs. 1 Ziff. 3 OR ist hingegen die Prüfung des dauerhaften und mängelfreien Funktionierens des IKS („Funktionsprüfung").[27]

1.3 Nationale Anforderungen an ein IKS

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG[28]) von 1998 auf nationaler Ebene sowie der Sarbanes-Oxley Act von 2002 (insb. Section 404) auf internationaler Ebene sind nur zwei wichtige Beispiele einer Reihe von Vorschriften mit Relevanz für ein IKS. Jedoch ergab sich bereits vor Einführung des KonTraG eine in der Praxis weitestgehend verkannte **Verpflichtung der gesetzlichen Vertreter** von Kapitalgesellschaften zur Einführung eines wirksamen und funktionsfähigen IKS, die zudem nicht auf die Inanspruchnahme eines geregelten Marktes durch das Unternehmen beschränkt ist.[29]

---

27 Treuhand-Kammer – Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems vom 17. Dezember 2007, Ziff. I, Buchst. c. Die Treuhandkammer betont, dass das Parlament durch das Streichen des Wortes „funktionierend" bewusst von einer Wirksamkeits- und Funktionsprüfung abgesehen hat.

28 Vgl. Bundesministerium der Justiz (BMJ): Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 28.01.1998. In: BT-Drucks. 13/9712.

29 Vgl. zur nachfolgenden Argumentation ausführlich z.B. Schoberth, Joerg et al.: Anforderungen an die Gestaltung von Internen Kontrollsystemen. In: Der Betriebs-Berater 2006, S. 2571–2577 sowie Schoberth, Joerg und Oliver Bungartz: Zusammenarbeit zwischen Interner Revision und Wirtschaftsprüfung. Lektion 4 des schriftlichen Management-Lehrgangs in 12 Lektionen „Interne Revision". Hrsg. Euroforum Verlag. 4. Aufl. Düsseldorf 2009.

Leitungsaufgabe und Sorgfaltspflicht der Unternehmensleitung

Die Geschäftsleitung eines nicht börsennotierten Unternehmens ist verpflichtet, durch organisatorische Sicherungsmaßnahmen und entsprechende Kontrollmechanismen einen geregelten Arbeitsablauf im Unternehmen zu gewährleisten, um Fehlentwicklungen zeitnah festzustellen und geeignete Gegenmaßnahmen ergreifen zu können. Nur so kann die Unternehmensleitung sicherstellen, dass sie die Risiken ihres unternehmerischen Handelns stets erkennen kann. Diese Verpflichtung ist Ausprägung der **allgemeinen GmbH-Geschäftsführerpflichten** nach § 43 Abs. 1 GmbHG, die sich mit dem Sorgfaltsmaßstab in § 93 Abs. 1 S. 1 AktG decken.

Auch aus Sichtweise der Wirtschaftsprüfung liegt die Verantwortung für die Ausgestaltung, d.h. die Konzeption, Implementierung, Überwachung, laufende Anpassung und Weiterentwicklung eines angemessenen und wirksamen IKS ausschließlich bei der Unternehmensleitung. Die durch das KonTraG eingeführte Regelung des § 91 Abs. 2 AktG hingegen, die vom Vorstand einer Aktiengesellschaft explizit fordert „geeignete Maßnahmen zu treffen, insb. ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“, ist letztlich als eine **gesetzliche Hervorhebung der allgemeinen Leitungsaufgabe** des Vorstandes nach § 76 AktG zu verstehen, mit der kein neuer Pflichtenkreis für Vorstandsmitglieder geschaffen wurde, sondern lediglich die bereits bestehenden Kontroll- und Überwachungspflichten des Geschäftsleiters einer Kapitalgesellschaft aufgrund seiner Organstellung konkretisiert wurden.

§ 91 Abs. 2 AktG ist hierbei auf GmbH-Geschäftsführer mittlerer und großer GmbH weitgehend der gesetzgeberischen Intention entsprechend anzuwenden (sog. **Ausstrahlungswirkung**). Der Gesetzgeber hat zwar keine (materielle) Verschärfung der Haftung der Organmitglieder angestrebt; dennoch ist Vorständen eines Unternehmens aufgrund der Hervorhebung in § 91 Abs. 2 AktG zu empfehlen, das bestehende IKS nochmals dahingehend zu überprüfen, ob die Kontroll- und Sicherungssysteme dem notwendigen Standard entsprechen und dies auch eingehend zu dokumentieren. Auch wenn mit der Konkretisierung in § 91 Abs. 2 AktG keine materielle Haftungsverschärfung einhergegangen ist, lassen sich zukünftig Sorgfaltspflichtverletzungen aufgrund dieser Konkretisierung mit Einführung des KonTraG leichter begründen. Dies kann aus praktischer Sicht dann doch zu einer verschärften Haftung der Geschäftsleiter führen.

Dokumentationspflichten der Unternehmensleitung

Eine **Verpflichtung zur Dokumentation** des IKS kann im Zusammenhang mit den Regelungen der Prüfung von Jahresabschlüssen durch Wirtschaftsprüfer hergeleitet werden. Demnach erstreckt sich der Umfang der Prüfung des Jahresabschlusses nach § 317 Abs. 1 S. 1 HGB durch den Abschlussprüfer auch auf das IKS. Hierzu hat der Abschlussprüfer im Rahmen der Prüfung des IKS (vgl. IDW PS 261 n.F.) und vor

dem Hintergrund des IDW PS 300 (Prüfungsnachweise im Rahmen der Abschlussprüfung) zur Beurteilung des rechnungslegungsbezogenen IKS, Prüfungshandlungen zur Risikobeurteilung (inkl. Aufbauprüfung) und Wirksamkeit (Funktionsprüfung) des auf die Rechnungslegung bezogenen IKS durchzuführen.

Der **Abschlussprüfer** muss nach den IDW Standards überprüfen, ob die Buchführung als Teil des IKS den gesetzlichen Anforderungen entspricht und das IKS während des zu prüfenden Geschäftsjahres kontinuierlich bestanden hat. Die dafür notwendigen Informationen und Unterlagen müssen dem Abschlussprüfer zur Verfügung gestellt werden, damit dieser seinem Prüfungsauftrag gerecht werden kann. Ohne eine entsprechende Dokumentation ist dies nur schwer feststellbar.[30]

Aus der Dokumentation sollten das generelle Vorgehen, Maßnahmen zur Risikoidentifikation, Risikomessung, Risikosteuerung, allgemeine Risikorichtlinien, festgelegte Verantwortlichkeiten sowie Schulungsmaßnahmen hervorgehen. Die Pflicht zur Verfügungstellung dieser Unterlagen, und damit auch die Verantwortung für deren Erstellung obliegen dem **Geschäftsführer**, der für die ordnungsgemäße Buchführung der Gesellschaft zu sorgen hat. Dieser kann einzelne Aufgabenbereiche zwar delegieren und zur Erfüllung seiner Pflichten Dritte einschalten; seine Verantwortlichkeit bleibt hiervon jedoch letztlich unberührt.

Pflichtverletzung und Haftung der Unternehmensleitung

Der gesetzliche Vertreter haftet der Gesellschaft nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG für den dadurch eingetretenen Schaden (d.h. für jeden vermögenswerten Nachteil der Gesellschaft, der bei pflichtgemäßem Verhalten der Geschäftsführung nicht eingetreten wäre), wenn er seine **Sorgfaltspflichten** in Bezug auf die angemessene Ausgestaltung eines IKS verletzt. Die Gesellschaft muss lediglich den Eintritt und die Höhe des Schadens, die Handlung des Vorstands bzw. des Geschäftsführers im Sinne eines pflichtwidrigen Unterlassens zur Einrichtung eines angemessenen IKS und die adäquate Kausalität zwischen Handlung und Schaden darlegen und ggf. beweisen. Ist die Gesellschaft ihrer Darlegungs- und gegebenenfalls Beweispflicht nachgekommen, obliegt es dem beklagten gesetzlichen Vertreter darzulegen und gegebenenfalls zu beweisen, dass er nicht pflichtwidrig und / oder schuldhaft gehandelt hat oder dass der Schaden auch bei pflichtgemäßem Verhalten eingetreten wäre. Dem gesetzlichen Vertreter obliegt somit im Rahmen der Anwendung des § 93 Abs. 2 S. 2 AktG nicht nur die Beweislast für fehlendes Verschulden, sondern auch für fehlende Pflichtwidrigkeit.

---

30 Vgl. z.B. aber auch die Entscheidung des Landgerichts München (LG München I vom 5.4.2007, 5 HK O 15964/06): Nach der Urteilsbegründung „gehört auch die Dokumentation des Früherkennungssystems zu den zentralen Aufgaben des Vorstandes im Anwendungsbereich von § 91 Abs. 2 AktG und der in dieser Vorschrift zum Ausdruck kommenden Bestandsverantwortung."

Ist aufgrund der Art des Schadens zudem anzunehmen, dass dieser vermutlich auf ein **Unterlassen des gesetzlichen Vertreters** zurückzuführen ist, wird die Gesellschaft von der Darlegung der Kausalität befreit (d.h. den gesetzlichen Vertreter trifft zusätzlich auch die Kausalitätsvermutung). Zur Abwendung einer Haftung muss der gesetzliche Vertreter neben der oben dargelegten Beweislast in diesem Fall zusätzlich die vermutete Kausalität zwischen Handlung und Schadenseintritt widerlegen. Diese Kausalitätsvermutung greift zusätzlich auch, wenn der Gesellschaft aufgrund unzureichend geführter Bücher der Nachweis der Kausalität erschwert oder unmöglich gemacht wird. Die schriftliche Niederlegung aller wesentlichen Geschäftsvorgänge und nicht nur der rechnungslegungsbezogenen Sachverhalte ist daher in der Praxis nicht nur üblich, sondern auch im Interesse des Geschäftsführers dringend anzuraten.

Die Untersuchung der Mindestanforderungen und Rechtsfolgen in Deutschland zeigt auf, dass die angemessene Ausgestaltung eines IKS zur **Leitungsaufgabe und gesetzlichen Sorgfaltspflicht** der gesetzlichen Vertreter gehört. Diese Ausgestaltung umfasst auch zwingend die Dokumentation, also die schriftliche Niederlegung aller wesentlichen Geschäftsprozesse. In den Fällen, in denen das Absehen von der schriftlichen Dokumentation nicht bereits für sich als Sorgfaltspflichtverletzung eingestuft wird, wird dem gesetzlichen Vertreter sonst eine Haftungsbefreiung aufgrund der Kausalitätsvermutung erschwert.

Nicht zuletzt sollte es aber im Interesse eines **jeden ordentlichen und gewissenhaften Kaufmanns** (vgl. beispielsweise § 93 Abs. 1 S. 1 AktG und § 43 Abs. 1 GmbHG) liegen, sein Unternehmen durch ein funktionsfähiges und auf die unternehmensspezifischen Bedürfnisse zugeschnittenes IKS basierend auf einem anerkannten Rahmenwerk zu schützen. Bei genauer Betrachtung sind in jedem Unternehmen Kontrollmechanismen zu finden, die – vielleicht nicht immer formalisiert, dokumentiert und auf Funktionalität getestet – aber schon immer Bestandteil der Unternehmensprozesse waren und es auch in Zukunft sein werden.

Transformation europarechtlicher Vorgaben in die nationale Gesetzgebung

Der deutsche Gesetzgeber hat mit dem Gesetz zur Modernisierung des Bilanzrechts (**Bilanzrechtsmodernisierungsgesetz – BilMoG**)[31] auf die europarechtlichen Vor-

[31] Vgl. Bundesministerium der Justiz (BMJ): Gesetz zur Modernisierung des Bilanzrechts (BilMoG) vom 27.03.2009. In: BT-Drucks. 270/09. Für eine vollständige Übersicht der Änderungen sowie der ausführlichen und wörtlichen Begründung des BilMoG vgl. Bundesministerium der Justiz (BMJ): Gesetzentwurf der Bundesregierung. Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz – BilMoG) vom 21.05.2008. In: BT-Drucks. 16/10067. Abrufbar unter: www.bmj.de.

gaben zur rechnungslegungsbezogenen Corporate Governance reagiert und somit die Tendenz zur Hervorhebung der Bedeutung des IKS noch verstärkt:[32]

> „Er (der Aufsichtsrat, Anmerkung des Verfassers) kann insbesondere einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung, hier insbesondere der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst." (**§ 107 Abs. 3 S. 2 AktG**)
>
> „Ist der Jahresabschluss oder der Konzernabschluss durch einen Abschlussprüfer zu prüfen, so hat dieser an den Verhandlungen des Aufsichtsrats oder des Prüfungsausschusses über diese Vorlagen teilzunehmen und über die wesentlichen Ergebnisse seiner Prüfung, insbesondere wesentliche Schwächen des internen Kontroll- und des Risikomanagementsystems bezogen auf den Rechnungslegungsprozess, zu berichten." (**§ 171 Abs. 1 S. 2 AktG**)

Nach der Begründung zum BilMoG ist dabei das Risikomanagementsystem umfassend als allgemeines Risikomanagementsystem zu verstehen und **nicht auf die Rechnungslegung beschränkt**.

Der Aufsichtsrat ist verpflichtet zu beurteilen, ob Ergänzungen, Erweiterungen oder Verbesserungen des allgemeinen Risikomanagementsystems notwendig sind. Fehlt es bislang an einem Risikomanagementsystem**,** ist die Notwendigkeit der Einrichtung eines solchen zu prüfen. Der Aufsichtsrat muss den Vorstand anhalten, **stringente interne Kontrollsysteme und Informationsabläufe** einzurichten, um mögliche Defizite im Risikomanagement zu minimieren und somit eigene Sorgfaltspflichtverletzungen auszuschließen. Die vorstehenden Überlegungen gelten entsprechend auch bezüglich der Überwachung des IKS. Die Überwachung des Rechnungslegungsprozesses dürfte i.d.R. mit der Überwachung des IKS und des Risikomanagementsystems einhergehen.[33]

Die **Berichterstattung im Lagebericht bzw. im Konzernlagebericht** wurde durch das BilMoG mit Bezug auf die Risikoberichterstattung wie folgt ergänzt:[34]

---

32 Vgl. auch Happ, Dominik und Christiane Pott: Auswirkungen des Sarbanes-Oxley Act Section 404: Kosten und Nutzen für europäische Unternehmen. In: Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung 2007, S. 672.

33 Vgl. für einen Leitfaden, wie der Aufsichtsrat die Existenz, den Aufbau und die Funktionsfähigkeit eines IKS effektiv überwachen kann, z.B. Bungartz, Oliver: Interne Kontrollsysteme (IKS) – Basiswissen für den Aufsichtsrat. Berlin 2017.

34 Die Änderung des BilMoG für den Lagebericht bzw. den Konzernlagebericht verfolgt die Umsetzung von Art. 46a Abs. 1 der Bilanzrichtlinie in der Fassung der Abänderungs-Richtlinie.

„Kapitalgesellschaften im Sinn des § 264d haben im Lagebericht die wesentlichen Merkmale des internen Kontroll- und Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess zu beschreiben." (**§ 289 Abs. 4 HGB**)

„Ist das Mutterunternehmen oder ein in den Konzernabschluss einbezogenes Tochterunternehmen kapitalmarktorientiert im Sinne des § 264d, ist im Konzernlagebericht auch auf die wesentlichen Merkmale des internen Kontroll- und Risikomanagementsystems im Hinblick auf den Konzernrechnungslegungsprozess einzugehen." (**§ 315 Abs. 4 HGB**)

In der **Begründung zu § 289 HGB** führt der Regierungsentwurf aus, dass mit der Vorschrift weder die Einrichtung noch die inhaltliche Ausgestaltung eines IKS im Hinblick auf den Rechnungslegungsprozess verpflichtend angegeben wird. Es bleibt den geschäftsführenden Organen überlassen, ein IKS nach den vorhandenen Bedürfnissen unter Berücksichtigung der Unternehmensstrategie, des Geschäftsumfangs und anderer wichtiger Wirtschaftlichkeits- und Effizienzgesichtspunkte einzurichten.

Die Vorschrift verpflichtet nur dazu, die wesentlichen Merkmale des vorhandenen IKS – mithin die Strukturen und Prozesse – im Hinblick auf den Rechnungslegungsprozess zu beschreiben. Das Maß an Beschreibungen ist von den individuellen Gegebenheiten eines jeden Unternehmens abhängig. Die Beschreibung muss aber so ausgestaltet sein, dass die Abschlussadressaten sich ein **Bild von den wesentlichen Merkmalen des IKS** machen können. Besteht kein IKS, ist dies anzugeben.

Ausführungen zur Einschätzung der Effektivität des IKS sind nach der Begründung zum BilMoG nicht erforderlich**.** Bereits die Beschreibung des IKS zwingt die Organe der Geschäftsführung zu einer Auseinandersetzung mit dem IKS und damit auch mit der **Frage nach dessen Effektivität**. Dies gilt umso mehr, als die unzureichende Einrichtung eines IKS die Möglichkeit einer Sorgfaltspflichtverletzung durch die Geschäftsführungsorgane bergen kann.

Der Vergleich der internationalen und nationalen Anforderungen an ein IKS kommt zu einem nicht vermuteten Ergebnis: Die lediglich impliziten deutschen gesetzlichen Vorschriften zur Implementierung eines IKS und deren haftungsrechtliche Folgen **gehen insoweit über die strengen Anforderungen nach internationalem Verständnis hinaus**, als auch die Verletzung nicht nur rechnungslegungsrelevanter Sorgfaltsvorschriften zu einer Haftung der gesetzlichen Vertreter nach deutschen Rechtsvorschriften führen kann.[35]

[35] Schoberth, Joerg et al.: Anforderungen an die Gestaltung von Internen Kontrollsystemen. In: Der Betriebs-Berater 2006, S. 2577.

1.4 Mehrwert und Grenzen eines IKS

Das IKS hilft einem Unternehmen, seine **Entwicklungs- und Profitabilitätsziele** zu erreichen und einen Verlust an Ressourcen zu vermeiden. Es unterstützt die Sicherstellung einer verlässlichen finanziellen Berichterstattung sowie die Einhaltung von Gesetzen und Vorschriften zur Vermeidung von Reputationsschäden und anderen Konsequenzen. Zusammengefasst hilft das IKS einem Unternehmen bei dem Erreichen seiner Ziele, indem es Stolpersteine und Überraschungen auf dem Weg dorthin aufdeckt und vermeidet.

Allerdings kann auch ein sachgerecht gestaltetes IKS **nicht in jedem Fall gewährleisten**, dass die vom Unternehmen verfolgten Ziele erreicht werden. Als Gründe hierfür kommen u.a. in Betracht:

- Menschliche Fehlleistungen, z.B. infolge von Nachlässigkeit, Ablenkung, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen
- Nicht routinemäßige Geschäftsvorfälle, die vom IKS nur bedingt, schwer oder überhaupt nicht erfasst werden können
- Umgehung oder Außerkraftsetzung des IKS durch das Management und andere Mitarbeiter oder durch das Zusammenwirken dieser Personen mit unternehmensexternen Personen
- Missbrauch oder die Vernachlässigung der Verantwortung durch für bestimmte Kontrollen verantwortliche Personen
- Zeitweise Unwirksamkeit des IKS aufgrund veränderter Unternehmens- und Umweltbedingungen
- Verzicht des Managements auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen

Das IKS hat neben den definierten Hauptzielen noch andere positive Nebeneffekte, die einen Mehrwert für das Unternehmen schaffen können. Der Mehrwert eines IKS ergibt sich zum einen aus den Ergebnissen der **Prozessoptimierung** und der Identifizierung von operativen Schwachstellen innerhalb der Prozesse und zum anderen aus dem Erreichen eines erhöhten Risikobewusstseins auf Mitarbeiterebene, das wiederum zur Aufdeckung und Vermeidung von Fehlerquellen im Unternehmen beiträgt.

Zusätzlich kann die im Rahmen der Einrichtung eines IKS entstandene Dokumentation der Prozesse bei Personalwechsel innerhalb des Unternehmens von großem Nutzen sein, da Einarbeitungszeiten verkürzt und eine **Kontinuität und Stabilität der Abläufe** erhalten werden können. Auch unternehmensexternen Interessenten wird durch die bestehende Dokumentation ermöglicht, sich in kürzester Zeit einen Überblick über die wesentlichen Prozesse des Unternehmens zu verschaffen.

Des Weiteren kann ein formalisiertes und dokumentiertes IKS gerade für kleine und mittlere Unternehmen vor dem Hintergrund der gesetzgeberischen Tendenzen und der Entwicklungen am Kapitalmarkt zukünftig die **Mittelbeschaffung** erleichtern. Entscheidungen im Rahmen des Kreditvergabeverfahrens werden unter dem

Gesichtspunkt der Risikoklassifizierung durch ein vorzeigbares IKS sicherlich begünstigt.

Auch im Hinblick auf eine spätere **Unternehmensveräußerung** sollte das Vorhandensein eines formalisierten und dokumentierten IKS positive Auswirkungen auf Verhandlungen und Kaufpreisfindung haben. Die Ergebnisse einer europäischen Studie unter Kapitalanlagegesellschaften, die sowohl die Käufer- als auch die Verkäuferseite bei Unternehmenstransaktionen betrachtet, belegen diese These:[36]

- Die Befragten schreiben einem **IKS einen klaren Mehrwert** zu. Konsequenterweise sind viele Unternehmensvertreter bereit, einen signifikanten Teil des Transaktionsvolumens in die Entwicklung eines funktionierenden IKS zu investieren. Die Zahlung eines Aufpreises für ein dokumentiertes und effektives IKS im Rahmen einer Unternehmenstransaktion wird von der Mehrheit der Unternehmen in Erwägung gezogen.
- Die Befragten sind fast einheitlich der Meinung, dass ein **IKS Mehrwert schafft**. Sowohl Käufer als auch Verkäufer von Unternehmen zeigen Bereitschaft, für die Implementierung eines IKS oder den Erwerb eines bereits bestehenden IKS einen Aufpreis von bis zu 15 % des Transaktionsvolumens zu zahlen.

Die **Ergebnisse der Studie** können durchschnittlich über Käufer- und Verkäuferseite in Bezug auf ein dokumentiertes und funktionsfähiges IKS wie folgt zusammengefasst werden:[37]

- 78 % der Unternehmen stimmen zu, dass ein funktionsfähiges IKS einen nachhaltigen Mehrwert schafft, wobei „weniger negative Überraschungen“ und „höhere Transparenz“ die wichtigsten Mehrwerttreiber sind.
- 66 % der Unternehmen stimmen zu, dass eine Spanne von 1 – 15% des Transaktionsvolumens für ein bereits implementiertes IKS gerechtfertigt ist.
- 73 % der Unternehmen stimmen zu, dass eine separate Beurteilung des IKS im Sinne einer „IKS Due Diligence (IKS DD)“ sinnvoll wäre, wobei 88% der Unternehmen zwischen 1 – 20% des gesamten DD-Volumens dafür investieren würden.
- 76 % der Unternehmen sind bereit, nachträglich in ein IKS zu investieren und beziffern die Investitionsbereitschaft auf bis zu 15 % des Investitionsvolumens.

Bei Fragen der Nachfolgeregelung kann ein formalisiertes und dokumentiertes IKS als wichtiges Instrument des **Know-how-Transfers** dienen.

[36] Vgl. Bungartz, Oliver und Gregor Strobl: Mehrwert durch Interne Kontrollsysteme (IKS) – Ergebnisse einer europäischen Studie. In: Zeitschrift Interne Revision 2012, S. 143.

[37] Vgl. Bungartz, Oliver und Gregor Strobl: Mehrwert durch Interne Kontrollsysteme (IKS) – Ergebnisse einer europäischen Studie. In: Zeitschrift Interne Revision 2012, S. 144.

Grundsätzlich werden viele Chancen vergeben, wenn ein angemessenes IKS nicht vorhanden ist. Die folgenden **Thesen aus der Praxis** beschreiben abschließend mögliche Vorteile von Kontrollen aus der Sicht von Führungskräften:[38]

- Kontrolle führt Mitarbeiter zu besseren Leistungen.
- Kontrolle fördert Entwicklung und lässt Chancen erkennen.
- Kontrolle unterstützt Freiheit, Autonomie und damit Kreativität.
- Kontrolle vermittelt Informationen und gibt Überblick und Sicherheit.
- Kontrolle als Dialog fördert Wissenstransfer, Verständnis und Orientierung.
- Kontrolle kann Katastrophen, Skandale und Fehler verhindern.
- Kontrolle nimmt den Mitarbeitern Angst und stärkt ihr Vertrauen.
- Kontrolle begleitet Vertrauen.
- Kontrolle demonstriert dem Mitarbeiter Interesse an seiner Arbeit.
- Kontrolle darf keine Fehlersuche sein.
- Kontrolle ist nicht eine Frage des Ob, sondern des Wie.

1.5 Zusammenfassung: Definition und Anforderungen an ein IKS

Unter einem IKS werden entsprechend dem **IDW PS 261 n.F.** allgemein die von der Unternehmensleitung im Unternehmen eingeführten Grundsätze, Verfahren und Regelungen verstanden, die auf die organisatorische Umsetzung von Entscheidungen der Unternehmensleitung gerichtet sind.

US-amerikanische Vorschriften nach dem **Sarbanes-Oxley Act (SOX)** sind die wohl weltweit bekanntesten rechtlichen Vorgaben zum IKS. Die Töchter von den SOX-Bestimmungen unterliegenden Mutterunternehmen sind aber nicht die einzigen Unternehmen, die für ein funktionierendes IKS sorgen müssen.

Auch in China wurden 2008 mit den „Basic Standards for Enterprise Internal Control“ (**C-SOX**) vergleichbare Anforderungen an ein IKS kodifiziert. Die „Basic Standards for Enterprise Control“ wurden im Jahr 2010 noch um die „Guidelines for the Internal Control of Companies“ ergänzt.

Die **Bestrebungen in der EU** gehen ebenfalls in Richtung einer Verschärfung der Regelungen zum IKS. Einzelne Elemente der SOX-Vorschriften sind bereits mit der 4., 7. und 8. EU-Richtlinie umgesetzt worden.

Auf **nationaler Ebene** lässt sich die Verpflichtung zur sorgfältigen und ordnungsgemäßen schriftlichen Dokumentation aller geschäftswesentlichen Vorgänge einschließlich des rechnungslegungsbezogenen IKS bereits aus der allgemeinen Sorgfaltspflicht und Verantwortlichkeit der gesetzlichen Vertreter nach § 93 Abs. 2 AktG

[38] Vgl. Brandes, Dieter: Unbeliebt und vernachlässigt – Mut zur Kontrolle. In: Management und Qualität 2010, S. 9.

bzw. § 43 Abs. 2 GmbHG herleiten, wobei es sich dabei noch nicht einmal um Neuerungen des KonTraG oder anderer aktueller Gesetzesreformen handelt. Die Tendenz zum IKS verstärkt sich weiter durch die Transformation von europarechtlichen Vorgaben wie zuletzt das Bilanzrechtsmodernisierungsgesetz (BilMoG).

Unter Berücksichtigung der naturgemäß immanenten Grenzen hat ein IKS viele Vorteile für ein Unternehmen. Der **Mehrwert**, den ein IKS schaffen kann, sollte alle Unternehmen dazu bewegen, frühzeitig darüber nachzudenken ein ordnungsmäßiges IKS auf Grundlage eines anerkannten Rahmenwerks einzuführen, selbst wenn momentan noch kein unmittelbarer regulatorischer Druck oder gesetzlicher Zwang besteht. In diesem Fall existiert für solche Unternehmen ein zeitlicher Vorsprung, der sinnvoll genutzt werden sollte.

1.6 Exkurs: Freiwillige Prüfung eines IKS nach dem „IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)“

Mit dem **„IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)“**[39] beschreibt das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) den Inhalt freiwilliger Prüfungen des IKS außerhalb der Abschlussprüfung. Der IDW PS 982 steht im Einklang mit dem International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“[40], geht insofern über die Prüfung eines IKS im Rahmen der Jahresabschlussprüfung nach IDW PS 261 n. F. hinaus und erfordert ein gesondertes Prüfungsurteil zum IKS.

Die Veröffentlichung des IDW PS 982 resultiert aus der gesetzlichen Anforderung, dass der Aufsichtsrat bzw. ein eingerichteter Prüfungsausschuss die Wirksamkeit des IKS beurteilen muss (vgl. § 107 Abs. 3 S. 2 AktG). Die **Überwachungsaufgabe in Bezug auf die Wirksamkeit des IKS** ist vom Aufsichtsrat bzw. dem Prüfungsausschuss höchstpersönlich wahrzunehmen. Hierbei kann es für den Aufsichtsrat bzw. den Prüfungsausschuss interessant sein, einen Wirtschaftsprüfer mit der Prüfung

[39] Vgl. für die nachfolgend zusammengefassten Inhalte der Verlautbarung das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) (Hrsg.): IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems der Unternehmensberichterstattung (IDW PS 982)“. In: IDW Life 2017, S. 415–448. Der Prüfungsstandard ist erstmalig anzuwenden bei freiwilligen Prüfungen des IKS der Unternehmensberichterstattung, die nach dem 30. 04. 2017 beauftragt werden.

[40] Vgl. The International Federation of Accountants (IFAC): International Standard on Assurance Engagements (ISAE) 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information. Stand Juni 2016. Abrufbar unter: www.ifac.org.

eines IKS zu beauftragen, um dieses Prüfungsergebnis als Grundlage seiner eigenen Beurteilung zu verwenden.[41]

Die Prüfung des **IKS der Unternehmensberichterstattung** umfasst nach IDW PS 982 Regelungen im Zusammenhang mit dem Berichtswesen. Der Informationsverarbeitungsprozess hat die Gewinnung, Verarbeitung, Weiterleitung und Darstellung von entscheidungsrelevanten Informationen in Form von Unternehmensberichterstattung zum Inhalt und erstreckt sich auf die zugrunde liegenden Kern- und Unterstützungsprozesse mit ihren Steuerungs- und Kontrollmaßnahmen.

Ziel einer Systemprüfung nach IDW PS 982 ist die Abgabe eines Prüfungsurteils mit hinreichender Sicherheit, ob – im Einklang mit den angewandten IKS-Grundsätzen – die Regelungen des IKS in der IKS-Beschreibung in allen wesentlichen Belangen geeignet und implementiert bzw. geeignet und wirksam waren.

Die **Verantwortung für das IKS** (d.h. Konzeption, Implementierung, Aufrechterhaltung und Überwachung) liegt bei den gesetzlichen Vertretern. Die Verantwortung der gesetzlichen Vertreter umfasst auch die Dokumentation eines IKS.

Die **IKS-Beschreibung** enthält explizite oder implizite Aussagen der gesetzlichen Vertreter zu den Grundelementen (inkl. Regelungen) des IKS und zur Angemessenheit, Implementierung und – sofern notwendig – Wirksamkeit des IKS in Übereinstimmung mit den angewandten IKS-Grundsätzen.

Die nach IDW PS 982 geforderten **Mindestinhalte einer IKS-Beschreibung** umfassen die folgenden Bestandteile für alle Grundelemente des IKS:

- Darstellung der bei der Ausgestaltung des IKS angewandten IKS-Grundsätze
- Benennung der Unternehmensberichterstattungen, auf die sich die IKS-Beschreibung bezieht
- Beschreibung des Kontrollumfelds
- Beschreibung der IKS-Ziele
- Beschreibung des Prozesses der Risikobeurteilungen
- Beschreibung der Kontrollaktivitäten unter Verweis auf auch außerhalb der IKS-Beschreibung dokumentierte sog. Risiko-Kontroll-Matrizen
- Beschreibung der Information und Kommunikation
- Beschreibung einer ggf. vorhandenen Einheit im Unternehmen, die mit unterstützenden organisatorischen Tätigkeiten der Einrichtung und Aufrechterhaltung des IKS befasst ist

[41] Vgl. für einen Leitfaden, wie der Aufsichtsrat die Existenz, den Aufbau und die Funktionsfähigkeit eines IKS effektiv überwachen kann, z.B. Bungartz, Oliver: Interne Kontrollsysteme (IKS) – Basiswissen für den Aufsichtsrat. Berlin 2017.

– Beschreibung der Verantwortlichkeiten, Prozesse und Maßnahmen zur Überwachung und Verbesserung des IKS

Das **Ziel der Prüfung** nach IDW PS 982 kann sich auf

1. die Angemessenheit und Implementierung des IKS und / oder
2. die Wirksamkeit des IKS beziehen.

1. Angemessenheit und Implementierung des IKS

Ziel der Angemessenheitsprüfung ist die Abgabe eines Prüfungsurteils mit hinreichender Sicherheit darüber, ob

– die zu einem bestimmten Zeitpunkt implementierten Regelungen des IKS in der IKS-Beschreibung in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind,
– die dargestellten Regelungen in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen
  – geeignet waren, mit hinreichender Sicherheit die IKS-Ziele für die Unternehmensberichterstattung zu erreichen, und
  – zu einem bestimmten Zeitpunkt implementiert waren.

2. Wirksamkeit des IKS

Ziel der Wirksamkeitsprüfung (die stets auch eine Angemessenheitsprüfung umfasst) ist die Abgabe eines Prüfungsurteils mit hinreichender Sicherheit darüber, ob

– die im geprüften Zeitraum implementierten Regelungen des IKS in der IKS-Beschreibung in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind,
– die dargestellten Regelungen in Übereinstimmung mit den angewandten IKS-Grundsätzen in allen wesentlichen Belangen
  – während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die IKS-Ziele für die Unternehmensberichterstattung zu erreichen, und
  – während des geprüften Zeitraums wirksam waren.

Die Ausgestaltung des IKS hängt neben festgelegten Zielen auch vom Gegenstand der Unternehmensberichterstattung sowie der Art, dem Umfang und der Komplexität der Geschäftstätigkeit ab und beinhaltet nach IDW PS 982 die folgenden **in Wechselwirkung stehenden Grundelemente**, welche in die Geschäftsabläufe eingebunden sind:

- Kontrollumfeld
- IKS-Ziele
- Risikobeurteilung
- Kontrollaktivitäten
- Information und Kommunikation
- Überwachung des IKS

Die vorstehend beschriebenen Grundelemente und Anforderungen in Bezug auf ein IKS nach IDW PS 982 basieren – ebenso wie nach IDW PS 261 n.F. – auf **dem Rahmenwerk des Committee of Sponsoring Organizations of the Treadway Commission (COSO)**.[42]

[42] So verweist IDW PS 982 in seinen Anwendungshinweisen und sonstigen Erklärungen explizit auf die Rahmenkonzepte von COSO und COBIT als typische Beispiele für allgemein anerkannte IKS-Grundsätze für die Gestaltung von IKS bzw. IT-Prozessen.

2 Ausgestaltung eines Internen Kontrollsystems (IKS) nach den Empfehlungen des Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Die Studie mit dem Titel „Internal Control – Integrated Framework" (COSO-Report) wurde im September 1992 vom **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** veröffentlicht und versuchte erstmals bis dahin undefinierte Begriffe aus dem Corporate Governance Bereich zu präzisieren und strukturelle Zusammenhänge aufzuzeigen. Der COSO-Report bildet den zentralen Standard für den Aufbau und die Funktionsweise eines IKS und wurde 2013 überarbeitet und aktualisiert.[43]

2.1 Aufbau eines IKS nach COSO

Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) hat mit dem COSO-Report ein allgemein einsetzbares Konzept hinsichtlich der Gestaltung des „**Internal Control System**" vorgeschlagen.

Der Begriff des „Internal Control System" wurde im deutschsprachigen Raum mit „Internes Kontrollsystem (IKS)" übersetzt. Besser umschrieben wird „Internal Control"[44] jedoch durch die beiden **Teilbereiche des IKS:**

- Internes Steuerungssystem und
- Internes Überwachungssystem.

Es geht demnach um die Gestaltung eines Internen Steuerungs- und Überwachungssystems für alle wesentlichen Geschäftsprozesse eines Unternehmens. Welche Geschäftsprozesse als wesentlich einzuschätzen sind, ergibt sich aus dem jeweiligen Geschäftsmodell und seinen Möglichkeiten zur Nutzenstiftung für den Kunden

---

43 COSO wurde 1985 als freiwillige privatwirtschaftliche Organisation gegründet, mit der Mission „… to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations." Für allgemeine Informationen rund um COSO sowie dessen Verlautbarungen wird auf die folgende Internetadresse verwiesen: www.coso.org. Vgl. für die nachfolgende Darstellung des IKS nach dem COSO-Modell vor allem Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. September 1992 und Mai 2013 sowie die Verlautbarungen Internal Control – Integrated Framework. Guidance on Monitoring Internal Control Systems. Februar 2009; Internal Control over Financial Reporting – Guidance for Smaller Public Companies. Juli 2006; Enterprise Risk Management – Integrated Framework. September 2004.

44 Vgl. für den Begriff „Internal Control" im Wandel der Zeit sowie die Rolle der Internen Revision z. B. Bungartz, Oliver: Interne Revision und das Interne Kontrollsystem (IKS) – Von der „internen Kontrolle" zum „Internal Control". In: Zeitschrift Interne Revision Sonderheft 01/2015, S. 73–84.

sowie der wettbewerblichen Differenzierung. Aufgrund der Etablierung und allgemein weiten Verbreitung des Begriffs „**Internes Kontrollsystem (IKS)**“ wird dieser zur Vermeidung von Unklarheiten und aus Praktikabilitätsgründen auch weiterhin in diesem Buch verwendet.

Der **COSO-Report** besteht aus drei Teilen, wobei der erste Teil des Berichts (Executive Summary) eine Zusammenfassung über die Ergebnisse der Untersuchungen beinhaltet. Im zweiten Teil (Framework and Appendices) wird ein IKS definiert und seine Komponenten näher beschrieben sowie Anhänge u. a. mit Rollen / Verantwortlichkeiten, Überlegungen für kleinere Organisationen, Kommentierungen sowie Vergleiche mit dem COSO-Report 1992 und dem ERM-Rahmenwerk dargestellt. Im abschließenden dritten Teil (Illustrative Tools for Assessing Effectiveness of a System of Internal Controls) werden Werkzeuge und Beispiele dargestellt, anhand derer eine Bewertung des IKS ermöglicht werden soll.

Das COSO-Framework und das daraus entwickelte COSO-Modell (COSO I) fanden ihren Niederschlag im Wesentlichen inhaltsgleich in den berufsständischen Verlautbarungen der Wirtschaftsprüfer. Der **IDW PS 261 n. F.** gibt im Wesentlichen das Verständnis von Zielen und Komponenten eines IKS des COSO-Modells wieder. Ebenso basiert der Prüfungsstandard IDW PS 982 auf dem COSO-Modell und beschreibt dieselben Grundelemente eines IKS.

Die **Ausgestaltung** (d. h. die Konzeption, Implementierung, Aufrechterhaltung, Überwachung sowie die laufende Anpassung und Weiterentwicklung) eines angemessenen und wirksamen IKS liegt explizit im Verantwortungsbereich der Unternehmensleitung und muss anhand von unternehmensspezifischen Merkmalen (z. B. Größe, Komplexität, Rechtsform und Organisation des Unternehmens; Art, Komplexität und Diversifikation der Geschäftstätigkeit; Methoden der Erfassung, Verarbeitung, Aufbewahrung und Sicherung von Informationen sowie Art und Umfang der zu beachtenden rechtlichen Vorschriften) erfolgen. Eine unreflektierte und standardisierte Übernahme eines Standardmodells in jedes beliebige Unternehmen ist nicht möglich.

So wird z. B. das IKS in kleinen und mittelständischen Unternehmen, die von einem Gesellschafter-Geschäftsführer geleitet werden, übersichtlich sind, eine flache Hierarchie mit täglichen persönlichen Kontakten und einfache Geschäftsprozesse haben, i. d. R. **weniger formalisiert** sein als in großen Unternehmen mit mehreren hierarchischen Ebenen, örtlich getrennten Einheiten und komplexen Geschäftsprozessen.

COSO definiert „**Internal Control**“ als einen Prozess, der durch Überwachungs- und Leitungsorgane, das Management und andere Mitarbeiter einer Organisation ausgeführt wird, um hinreichende Sicherheit bezüglich des Erreichens der folgenden Zielkategorien zu gewährleisten (d. h. alle Mitarbeiter innerhalb einer Organisation sind in unterschiedlicher Art und Weise verantwortlich für das IKS):

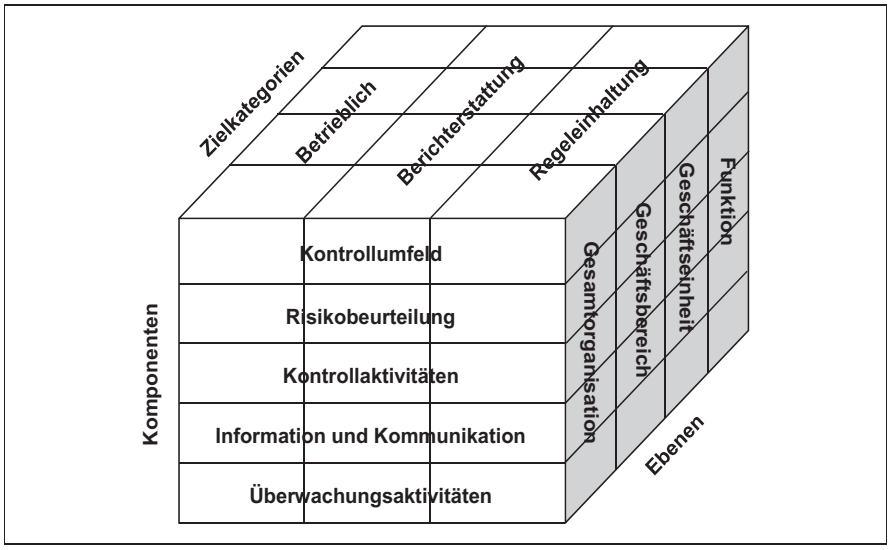
– Effektivität und Effizienz der Geschäftsprozesse (**Betrieblich**)
– Verlässlichkeit der Berichterstattung (**Berichterstattung**)
– Einhaltung der gültigen Gesetze und Vorschriften (**Regeleinhaltung**)

Grundsätzlich besteht das IKS aus **fünf Komponenten**, die zueinander in wechselseitiger Beziehung stehen:

– Kontrollumfeld
– Risikobeurteilung
– Kontrollaktivitäten
– Information und Kommunikation
– Überwachungsaktivitäten

Das IKS nach COSO kann als dreidimensionales Modell interpretiert werden. Die drei Zielkategorien (**erste Dimension**) und die fünf Komponenten (**zweite Dimension**) stehen im direkten Verhältnis zueinander. Jede der fünf Komponenten bezieht sich jeweils auf alle drei Zielkategorien. Ebenso gelten die drei Zielkategorien für jede Komponente des IKS. Das IKS ist sowohl für das gesamte Unternehmen oder den Konzern als auch für die einzelnen betrieblichen Einheiten und Funktionen relevant (**dritte Dimension**). Die Zusammenhänge zwischen den drei Dimensionen werden mit der folgenden Abbildung zusammengefasst:

Abb. 2: Drei Dimensionen eines IKS nach COSO



Quelle: Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Framework and Appendices. Mai 2013, S. 5.

In Ergänzung seines Rahmenkonzepts zur „Internal Control“ hat COSO 2004 ein „**Enterprise Risk Management (ERM) Framework**“ (**COSO II**)[45] zur Gestaltung eines unternehmensweiten Risikomanagement veröffentlicht, welches den COSO-Report (COSO I) erweitert und die zwischenzeitlich bedeutend gewordene Integration von Risikomanagementsystemen und IKS berücksichtigt.[46]

2.2 „Kontrollumfeld“ als Komponente eines IKS

Das Kontrollumfeld[47] dient allen weiteren Komponenten als **Fundament** und stellt den Rahmen dar, innerhalb dessen die Grundsätze, Verfahren und Maßnahmen eingeführt und angewendet werden. Es ist geprägt durch die Grundeinstellungen, das Problembewusstsein und das Verhalten des Managements in Bezug auf das IKS.

Die **wesentlichen Faktoren**, die das Kontrollumfeld in einer Organisation prägen, sind

1. die Bedeutung von Integrität und ethischen Werten im Unternehmen,
2. die Bedeutung der fachlichen Kompetenz im Unternehmen,
3. die Tätigkeit des Überwachungsorgans,
4. die Philosophie und das Geschäftsgebaren des Managements,
5. die Organisationsstruktur,
6. die Zuordnung von Weisungsrechten und Verantwortung sowie
7. die Grundsätze der Personalpolitik.

1. Integrität und ethische Werte

Integrität und ethische Werte sind ein Produkt der Unternehmenskultur und äußern sich häufig in einem **Verhaltens- und Ethikkodex**. Anreize und Versuchungen (wie z. B. Druck zur Erreichung unrealistischer Ziele, Prämien abhängig von außergewöhnlich hohen Leistungen, Möglichkeit unangemessene Aktivitäten leicht zu verbergen, unwesentliche Strafen und die fehlende Anleitung zur Durchführung richtiger Handlungen) beeinflussen die Integrität und die ethischen Werte in einem Unternehmen.

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf die Integrität und die ethischen Werte im Unternehmen können sein:

---

45 Vgl. für eine zusammenfassende Darstellung des Enterprise Risk Management (ERM) Framework, z. B. Bungartz, Oliver: Die Rolle der Internen Revision im Enterprise Risk Management (ERM) des Committee of Sponsoring Organizations of the Treadway Commission (COSO). In: Accounting, Auditing and Management. Festschrift für Wolfgang Lück. Hrsg. Michael Henke und Hilmar Siebert, S. 53–72 sowie Kapitel IV dieses Handbuchs.

46 Vgl. ausführlich zum Risikomanagement z. B. Bungartz, Oliver: Risikomanagement. Abschnitt 8. In: Bilanzrecht für die Praxis. Hrsg. Memento Verlag. Freiburg 2009 und Bungartz, Oliver: Risikomanagement für Aufsichtsräte. Anforderungen – Komponenten – Beurteilung. Berlin 2019 sowie Kapitel IV dieses Handbuchs.

47 Mit der Überarbeitung des COSO-Frameworks ist die Komponente „Kontrollumfeld“ durch 5 Prinzipien mit 20 zugehörigen Attributen charakterisiert worden. Vgl. dazu Abschnitt „2.7 Grundlegende Prinzipien und Attribute der COSO-Komponenten“ in diesem Kapitel.

– Existenz und Einführung eines Verhaltenskodex sowie anderer Vorschriften und Richtlinien in Bezug auf akzeptierte Geschäftspraktiken, Interessenkonflikte oder erwartete ethische Standards und moralisches Verhalten.
– Behandlung von Mitarbeitern, Lieferanten, Kunden, Investoren, Kreditgebern, Prüfern etc. (z.B. ob das Management bei Geschäften einem hohen ethischen Standard folgt und darauf besteht, dass dies auch andere tun oder ob das Management ethischen Aspekten wenig Beachtung schenkt).
– Druck zur Erreichung unrealistischer Leistungsziele – insb. für kurzfristige Ergebnisse – und das Ausmaß von dem die Vergütung auf der Erreichung dieser Zielvorgaben basiert.

Die folgende Tabelle enthält eine mögliche Strukturierung sowie potenzielle Inhalte eines Verhaltens- und Ethikkodex:[48]

Tab. 1: Inhalt eines Verhaltens- und Ethikkodex

Abschnitt	Inhalt
Brief der Geschäftsführung	– Präsentation der Einstellung der Geschäftsführung zur Wichtigkeit von Integrität und Ethik im Unternehmen – Einführung in den Verhaltens- und Ethikkodex (Zweck und Anwendung)
Ziele und Philosophie	Darstellung der – Kultur – Geschäftstätigkeit und Branche – Geographische Standorte (national und international) – Bekenntnis zu ethischem Führungsverhalten
Interessenskonflikte	– Adressierung von Verhaltenskonflikten und Arten der Selbstkontrahierung – Adressierung von Mitarbeitern und im Auftrag des Unternehmens handelnden Personen sowie Aktivitäten, Investitionen, oder Interessen, die Auswirkung auf die Unternehmensintegrität oder Unternehmensreputation haben
Geschenke und Zuwendungen	– Adressierung der Vergabe von Geschenken und Zuwendungen unter Betonung der Unternehmensrichtlinie, die über die nationale Gesetzgebung hinausgeht – Etablierung von Standards und Anweisungen zum Umgang mit Geschenken und Bewirtung sowie deren angemessene Berichterstattung
Transparenz	Berücksichtigung von Regelungen zur Sicherstellung der Unternehmensverpflichtung für eine vollständige und verständliche soziale, ökologische und ökonomische Berichterstattung
Unternehmensressourcen	Berücksichtigung von Regelungen im Umgang mit Unternehmensressourcen, einschließlich geistigen Eigentums und geschützte Informationen – wem diese gehören und wie sie gesichert werden

48 Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management – Integrated Framework. Application Techniques. Jersey City 2004, S. 9–10.

2. Bekenntnis zur fachlichen Kompetenz

Die Vorgehensweise des Unternehmens bei der Neueinstellung, Tätigkeitsbeurteilung, Beförderung, Vergütung und Kündigung von Mitarbeitern sowie die Identifikation von Kompetenzniveaus für jede Stelle im Unternehmen und die Ausgewogenheit vom Grad der Überwachung, der Befugnisse und das einem Mitarbeiter entgegen gebrachte Vertrauen sind **Ausdruck des Bekenntnisses** vom Management zur fachlichen Kompetenz. Das Bekenntnis zur fachlichen Kompetenz wird durch angemessene Disziplinarmaßnahmen im Unternehmen unterstützt.

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf das Bekenntnis zur fachlichen Kompetenz im Unternehmen können sein:

- Formelle oder informelle Stellenbeschreibungen oder andere Arten der Definition von Aufgaben, die bestimmte Stellen charakterisieren.
- Analyse des Wissens und der Fähigkeiten, um eine Tätigkeit angemessen ausführen zu können.

3. Tätigkeit des Überwachungsorgans

Das Überwachungsorgan, wie z.B. **Aufsichtsrat oder Beirat sowie ggf. ein Prüfungsausschuss** sollte unabhängig vom Management sein. Die Identifikation und Kontrolle von Risiken durch das Management sollte durch das Überwachungsorgan geprüft werden. Das Überwachungsorgan sollte eine gut informierte, wachsame und effektive Überwachungsfunktion im Unternehmen sein, die Finanzexperten in ihren Reihen hat. Aufsichtsrat, Beirat oder ggf. ein Prüfungsausschuss steht in direkter Verbindung mit den externen und internen Revisoren. Protokolle belegen und dokumentieren die Tätigkeit des Überwachungsorgans.[49]

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf die Überwachungstätigkeit des Aufsichtsrats bzw. der Gesellschafterversammlung können sein:

- Unabhängigkeit vom Management, so dass notwendige, wenn auch schwierige und bohrende Fragen, gestellt werden.
- Häufige und rechtzeitige Sitzungen mit Finanzleitern und/oder Rechnungswesenleitern, internen und externen Revisoren.
- Hinreichende und rechtzeitige Informationsversorgung des Überwachungsorgans, um die Überwachung der Ziele, der Strategien, der finanziellen Situation, der ope-

[49] Vgl. zur Tätigkeit des Überwachungsorgans i.V.m. den Verantwortlichkeiten innerhalb des IKS z.B. Bungartz, Oliver: Lücken im System – Verantwortlichkeiten einer wirksamen Unternehmensüberwachung. In: Lohn und Gehalt 2015, S. 34–41.

rativen Ergebnisse sowie wesentliche Vertragsvereinbarungen des Managements gewährleisten zu können.
– Hinreichende und rechtzeitige Unterrichtung des Überwachungsorgans über sensible Informationen, Untersuchungen und dolose Handlungen (z.B. Reisekosten des Top Managements, wesentliche Rechtsstreitigkeiten, Untersuchungen von Regulierungsbehörden, Unterschlagung, Betrug, Veruntreuungen, Missbrauch von Unternehmenseigentum, Insidergeschäfte sowie politisch motivierte oder illegale Zahlungen).

Das Überwachungsorgan sollte die Existenz und Wirksamkeit des IKS unter Berücksichtigung sämtlicher fünf COSO-Komponenten kontrollieren, wobei z.B. folgende **Überwachungsaktivitäten** zu berücksichtigen sind:[50]

Tab. 2: Aktivitäten zur Überwachung der IKS-Komponenten

IKS-Komponente	Überwachungsaktivitäten
Kontrollumfeld	– Überwachung der Definition und Anwendung von Verhaltensstandards – Etablierung der Erwartungen an sowie Beurteilung von Leistung, Integrität und ethischen Werten der Unternehmensführung – Etablierung der Überwachungsstrukturen und -prozesse im Einklang mit den Unternehmenszielen (z.B. Besetzung von Ausschüssen und Gremien mit der notwendigen Qualifikation und Expertise) – Überwachung von Wirksamkeitsprüfungen und Adressierung von Verbesserungsmöglichkeiten durch einen Lenkungsausschuss – Ausübung treuhänderischer Verantwortung gegenüber Anteilseignern oder anderen Eigentümern und Anwendung notwendiger Sorgfalt in der Überwachung (z.B. Vorbereitung von und Anwesenheit in Sitzungen, Prüfung der finanziellen Berichterstattung und anderen Unternehmenspublikationen) – Kritische Hinterfragung der Unternehmensführung im Hinblick auf die Erreichung der Unternehmensziele und die Geschäftsentwicklung sowie Forderung von Nachschauaktivitäten und Korrekturmaßnahmen (soweit erforderlich)
Risiko-beurteilung	– Berücksichtigung von internen und externen Faktoren, die wesentliche Risiken bei der Erreichung der Unternehmensziele darstellen können, und Identifizierung von Problemen und Trends – Kritische Hinterfragung der Beurteilung von Risiken der Zielerreichung durch das Management (inkl. potenzieller Auswirkungen von wesentlichen Veränderungen, dolosen Handlungen und Korruption) – Beurteilung der proaktiven Risikobeurteilung in Bezug auf Innovationen und Veränderungen, ausgelöst durch z.B. neue Technologien sowie ökonomische und geopolitische Verschiebungen
Kontroll-aktivitäten	– Befragung des Managements bezüglich der Auswahl, Entwicklung und Implementierung von Kontrollaktivitäten in wesentlichen Risikobereichen sowie der notwendigen Beseitigung von Kontrollschwächen – Überwachung der Unternehmensführung in der Durchführung von Kontrollaktivitäten

[50] Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework. Framework and Appendices. Mai 2013, S. 42–43.

IKS-Komponente	Überwachungsaktivitäten
Information & Kommunikation	– Kommunikation von Richtung und „Tone at the Top“ – Beschaffung, Durchsicht und Diskussion von Informationen in Bezug auf die Erreichung der Unternehmensziele – Hinterfragung der erhaltenen Informationen und Generierung von alternativen Standpunkten – Prüfung der Veröffentlichung an externe Parteien auf Vollständigkeit, Relevanz und Richtigkeit – Genehmigung und Adressierung der Eskalation von Problemen
Überwachungs-aktivitäten	– Beurteilung und Beaufsichtigung von Art und Umfang der Überwachungsaktivitäten, jeglicher Regelaussetzung sowie der Beurteilung und Beseitigung von Kontrollschwächen durch das Management – Zusammenarbeit mit dem Management, den internen und externen Revisoren und sonstigen Parteien zur Beurteilung des Bewusstseins in Bezug auf Unternehmensstrategien und -zielen sowie Kontrollauswirkungen im Zusammenhang mit der Entwicklung der Geschäftstätigkeit, der Infrastruktur, dem Regulieren und anderen Faktoren

4. Philosophie und Geschäftsgebaren des Managements

Der **Stil des Managements** beeinflusst das „akzeptierte“ Verhalten der Mitarbeiter im Unternehmen (z.B. in der Situation, wenn das Management versucht seine Ziele durch das Eingehen unverhältnismäßiger Risiken oder die Manipulation von Leistungskennzahlen zu erreichen, indem es beispielsweise Budgets abändert, um Abweichungen zu vermeiden).

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf die Philosophie und das Geschäftsgebaren des Managements können sein:

- Natur der vom Management akzeptierten Geschäftsrisiken (z.B. ob das Management häufiger unverhältnismäßig hohe Risiken eingeht oder extrem risikoavers ist).
- Häufigkeit der Interaktion zwischen dem Top Management und dem operativen Management, insb. bei geografisch auseinander liegenden Geschäftsaktivitäten.
- Einstellung zu und Aktionen der Finanzberichterstattung einschließlich der Diskussion von Bilanzierungspraktiken (z.B. konservative versus liberale Bilanzierungsrichtlinien, nicht angewendete Bilanzierungsgrundsätze, nicht offen gelegte wichtige finanzielle Angaben sowie manipulierte oder gefälschte Zahlen).

5. Organisationsstruktur

Die Organisationsstruktur legt den **Grad der Zentralisierung bzw. Dezentralisierung von Autoritäten** fest. Die Angemessenheit der Berichtsstrukturen, die Organi-

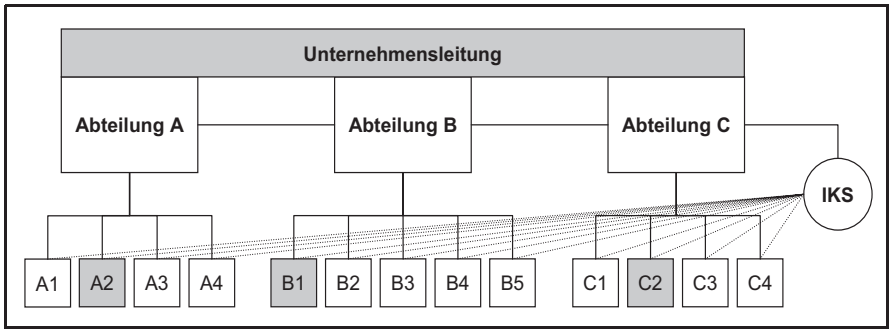
sation der Rechnungslegungsabteilung und die Interaktion mit anderen Gruppen sowie Funktionstrennung zwischen Initiierung und Verbuchung von Transaktionen sind Aspekte der Organisationsstruktur.

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf die Organisationsstruktur können sein:

- Angemessenheit der organisatorischen Struktur und die Möglichkeit den notwendigen Informationsfluss zur Steuerung der Aktivitäten zu ermöglichen.
- Angemessenheit der Definition von Verantwortlichkeiten von Schlüsselpositionen im Management und das Verständnis dieser Verantwortlichkeiten durch die betroffenen Personen.
- Angemessenheit von Wissen und Erfahrung von Managern in Schlüsselpositionen unter Beachtung ihrer Verantwortlichkeiten.

Die folgende Abbildung gibt eine mögliche organisatorische Einbindung im Sinne eines „**Stabs-Modells**“ wieder.

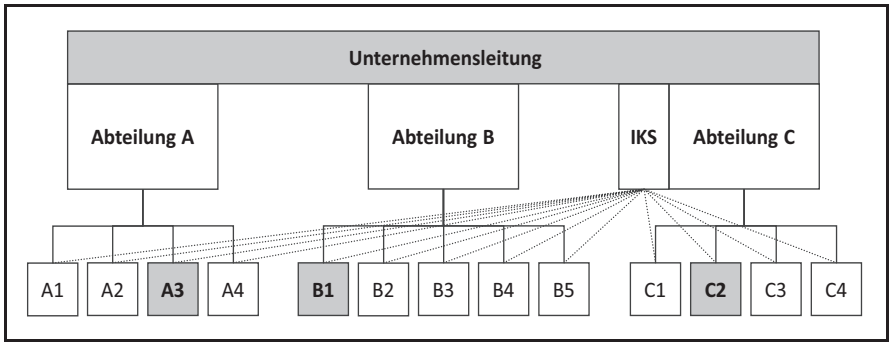
Abb. 3: Organisatorische Einbindung als „Stabs-Modell“



Anmerkung: Die grau schattierten Teilbereichsleiter sind zugleich IKS-Beauftragte der Abteilungen A, B und C. Beim Stabsmodell nimmt der IKS-Stab die Aufgaben der Entscheidungsvorbereitung wahr und dient der informationellen und methodischen Unterstützung der Unternehmensbereiche. Die getroffenen IKS-Entscheidungen beruhen bei dieser Lösung auf bereichsinternen und vom Stab erarbeiteten Daten und Kenntnissen. Die Stabseinheit kann als „Informationsdrehscheibe“ Fachwissen bündeln, das dann für die bereichsübergreifende Konsolidierung und Integration genutzt werden kann. Eine zentrale Analyse von Informationen aus den verschiedensten Bereichen bietet insb. die Chance, Informationssynergien zu realisieren, da z.B. große Datenbestände zuverlässig ausgewertet werden können und sich die Bedeutung von Einzelinformationen im Zusammenspiel mit weiterem (Hintergrund-) Wissen erschließt.

Die folgende Abbildung gibt die mögliche organisatorische Einbindung im Sinne eines „**Richtlinien-Modells**“ wieder.

Abb. 4: Organisatorische Einbindung im Sinne eines „Richtlinien-Modells“



Anmerkung: Die grau schattierten Teilbereichsleiter sind zugleich IKS-Beauftragte der Bereiche A, B und C. Das Richtlinien-Modell sieht vor, dass die betrachteten Aufgaben in mehreren Einheiten (zentral und auf operativer Ebene) verankert werden. Der Richtlinienbereich ist dabei für die Grundsatzentscheidungen der betreffenden Aufgabe allein entscheidungsbefugt und gegenüber den operativen Einheiten, welche die Aufgabe ausführen, weisungsberechtigt (Richtlinienkompetenz). Das Richtlinien-Modell baut auf einem hierarchischen Prinzip auf, bei dem die nach gelagerten Geschäftsbereiche für die Umsetzung der Entscheidungen des Richtlinienbereichs zuständig sind und nur im Rahmen der Vorgaben eigene Entscheidungen treffen können. Aufgrund seiner Struktur ist das Richtlinien-Modell in der Lage, eine übergreifende, unternehmenszielorientierte Perspektive zu verfolgen. Im Hinblick auf das IKS scheint das Richtlinien-Modell geeignet, die spezifischen Anforderungen erfüllen zu können. Eine unternehmensweite Integration der Risikoperspektive ist durch klare Vorgaben gesichert. Gleichzeitig wird das Fachwissen der operativen Einheiten sinnvoll genutzt und integriert.

6. Zuordnung von Weisungsrechten und Verantwortung

Mögliche Beispiele für **Ausprägungen und Einflussfaktoren** auf die Zuordnung von Weisungsrechten und Verantwortung können sein:

- Zuordnung von Weisungsrechten und Verantwortung, um Ziele der Organisation, der operativen Funktionen zu erreichen und regulatorische Anforderungen zu erfüllen (einschließlich Verantwortung für das Informationssystem und das Autorisieren von Änderungen).
- Angemessenheit von Kontrollstandards und Kontrollverfahren unter Berücksichtigung von Stellenbeschreibungen der Mitarbeiter.

– Angemessenheit der Mitarbeiterzahl, insb. mit Bezug zur elektronischen Datenverarbeitung und Bilanzierungsfunktionen sowie den dazu notwendigen Qualifikationen in Relation zur Größe des Unternehmens bzw. der Unternehmenseinheit sowie der Art und Komplexität der Aktivitäten und des Systems.

In der nachfolgenden Abbildung sind beispielhaft die **Verantwortlichkeiten** für die einzelnen Komponenten des IKS nach COSO den Unternehmensfunktionen – in einer zu Anschaulichkeitszwecken stark vereinfachten Verantwortlichkeitsmatrix – zugeordnet:

Abb. 5: Verantwortlichkeitsmatrix

	Aufsichtsrat / Beirat	Vorstand / Geschäftsführung	Risikocontrolling	Bereichsleiter	Operative Einheiten
Kontrollumfeld	x	x	(x)	(x)	
Risikobeurteilung		x	(x)	x	(x)
Kontrollaktivitäten		x	(x)	x	(x)
Information & Kommunikation	(x)	x	x	x	(x)
Überwachungsaktivitäten	x	x	x	(x)	

Legende:
x: Volle Aufgabenwahrnehmung
(x): Eingeschränkte Aufgabenwahrnehmung

7. Grundsätze der Personalpolitik

Richtlinien für Einstellungen, Aus- und Fortbildung, Beurteilungen, Beförderungen, Vergütung und Entlassungen sind Bestandteile von Grundsätzen der Personalpolitik (z.B. Einstellung der am besten qualifizierten Mitarbeiter mit Nachweis von Integrität und ethischem Verhalten, sog. Background Checks, kontinuierliche und individuelle Aus- und Fortbildung, Beförderungen basierend auf regelmäßigen Beurteilungen, klare Regelungen für Prämien und Boni, um ethisches Verhalten zu motivieren sowie angemessene disziplinarische Maßnahmen bei Nichteinhaltung von Richtlinien).

Die **Leistung des Personals** wird stark dadurch beeinflusst, wie konsequent Mitarbeiter zur Rechenschaft gezogen oder belohnt werden. Kennzahlen zur Leistungsmessung, Anreize und Belohnungen unterstützen ein wirksames IKS wenn sie den Unternehmenszielen angepasst sind und sich mit den Änderungen der Anforderungen dynamisch entwickeln.