

Handbuch Interne Kontrollsysteme (IKS)

Steuerung und Überwachung
von Unternehmen

Von

Dr. Oliver Bungartz

2., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
[ESV.info/978 3 503 12632 3](http://ESV.info/9783503126323)

Gedrucktes Werk: ISBN 978 3 503 12632 3
eBook: ISBN 978 3 503 12989 8

Alle Rechte vorbehalten
© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2011
www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Druck und Bindung: Hubert & Co., Göttingen

Vorwort zur zweiten Auflage

Die Themen Interne Kontrollsysteme (IKS) und Risikomanagement sind nach wie vor brandaktuell und nehmen für die Praxis stetig an Bedeutung zu. Das ungebrochene Interesse an diesen Themen hat dazu geführt, dass die erste Auflage vom „Handbuch Interne Kontrollsysteme (IKS) – Steuerung und Überwachung von Unternehmen“ schnell vergriffen war. Aufgrund der positiven Resonanz und der starken Nachfrage nach einem praktischen Leitfaden, freue ich mich eine zweite, bearbeitete und erweiterte Auflage herauszubringen.

Über die notwendigen Aktualisierungen hinaus, sind die rechtlichen Grundlagen um relevante Regelungen zum IKS in Österreich und der Schweiz ausgeweitet worden. Dies ermöglicht einen umfassenden Vergleich der gesetzlichen Anforderungen zum IKS und steigert die Attraktivität des Werkes für den gesamten deutschsprachigen Raum.

Neben den Ergänzungen zu den rechtlichen Grundlagen ist das Handbuch u.a. um folgende Aspekte und Teile ergänzt worden:

- Praxisthesen zur Vorteilhaftigkeit von Kontrollen
- Praktische Beispiele zu den verschiedenen IKS-Komponenten
- Darstellung eines Ansatzes zur effektiven Überwachung
- Herausforderungen der Projektorganisation zur Implementierung eines IKS
- Darstellung des Capability Maturity Model Integration (CMMI) zur Bestimmung des Reifegrades eines IKS
- Kapitel zum Compliance Management System (CMS)

Die Bearbeitungen und Ergänzungen für die zweite Auflage führten zu zahlreichen neuen Tabellen und Abbildungen.

Ganz herzlich danken möchte ich allen Personen, die mich bei der Erstellung der zweiten Auflage unterstützt haben. Meinen Kollegen von der „RSM Altavis“ in Hamburg, insb. den Herren Marco Michelsen, Maik Wellenbrock und Gregor Strobl, bin ich Dank für wertvolle Hinweise und konstruktive Kritik schuldig. Auch für die gewohnt reibungslose Zusammenarbeit mit dem Erich Schmidt Verlag in Berlin möchte ich Dr. Joachim Schmidt und Sebastian Engler ganz herzlich danken. Nicht zuletzt gilt mein Dank den vielen Teilnehmern meiner Seminare, die mir durch konstruktive Diskussionen und hilfreiche Hinweise geholfen haben, dieses Handbuch zu optimieren.

Ich wünsche Ihnen eine anregende und hilfreiche Lektüre und freue mich weiterhin über jegliche Rückfragen und Anregungen.

Hamburg, im September 2010

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, fachmännischen 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

Vorwort zur zweiten Auflage	5
Vorwort zur ersten Auflage	7
Abkürzungsverzeichnis	13
Abbildungsverzeichnis	17
Tabellenverzeichnis	19
Kapitel I: Grundlagen eines Internen Kontrollsystems (IKS)	21
1 Einführung in ein Internes Kontrollsystem (IKS)	21
1.1 Begriff und Aufgaben eines IKS	21
1.2 Internationale Anforderungen an ein IKS	23
1.3 Nationale Anforderungen an ein IKS	35
1.4 Mehrwert und Grenzen eines IKS	41
1.5 Zusammenfassung: Definition und Anforderungen an ein IKS	43
2 Ausgestaltung eines Internen Kontrollsystems (IKS) nach den Empfehlungen des Committee of Sponsoring Organizations of the Treadway Commission (COSO)	45
2.1 Aufbau eines IKS nach COSO	45
2.2 „Kontrollumfeld“ als Komponente eines IKS	48
2.3 „Risikobeurteilung“ als Komponente eines IKS	54
2.4 „Kontrollaktivitäten“ als Komponente eines IKS	58
2.5 „Information und Kommunikation“ als Komponente eines IKS	63
2.6 „Überwachung“ als Komponente eines IKS	64
2.7 Grundlegende Konzepte der COSO-Komponenten	70
2.8 Kontrollaktivitäten auf Unternehmensebene zur Überwachung der COSO-Komponenten	72
2.9 Zusammenfassung: IKS nach COSO	90
2.10 Exkurs: COSO und die Control Objectives for Information and related Technology (CobiT)	91
3 Dokumentation eines Internen Kontrollsystems (IKS)	99
3.1 Allgemeine Anforderungen an die Dokumentation eines IKS	99
3.2 Verbale Prozessbeschreibung als Möglichkeit der Dokumentation von Prozessabläufen im IKS	101
3.3 Flussdiagramm als Möglichkeit zur Dokumentation von Prozessabläufen im IKS	102
3.4 Risiko-Kontroll-Matrix als Möglichkeit zur Dokumentation des Aufbaus und der Funktion eines IKS	104

3.5	Testblatt als Möglichkeit zur Dokumentation von Funktionsprüfungen im IKS	106
3.6	Matrix als Möglichkeit zur Dokumentation der Funktionstrennung im IKS.	110
3.7	Maßnahmeplan als Möglichkeit zur Dokumentation von Schwachstellen und Überwachungstätigkeiten im IKS	112
3.8	Zusammenfassung: Dokumentationsmöglichkeiten eines IKS	114
Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)		115
1	Grundlagen der Organisation von Prozessen im Internen Kontrollsystem (IKS)	115
1.1	Organisation von Prozessen im Unternehmen	115
1.2	Organisation „Beschaffung“	117
1.3	Organisation „Produktion“	122
1.4	Organisation „Absatz“	126
1.5	Organisation „Anlagevermögen“	128
1.6	Organisation „Personal“	130
1.7	Organisation „Rechnungslegung“	134
1.8	Organisation „Finanzen“	137
1.9	Organisation „Steuern“	143
1.10	Organisation „Informationstechnologie“	151
2	Risiko-Kontroll-Matrizen für die Prozesse im Internen Kontrollsystem (IKS)	159
2.1	Grundlagen der Erstellung von Risiko-Kontroll-Matrizen	160
2.2	Risiko-Kontroll-Matrix „Beschaffung“	161
2.3	Risiko-Kontroll-Matrix „Produktion“	176
2.4	Risiko-Kontroll-Matrix „Absatz“	195
2.5	Risiko-Kontroll-Matrix „Anlagevermögen“	208
2.6	Risiko-Kontroll-Matrix „Personal“	218
2.7	Risiko-Kontroll-Matrix „Rechnungslegung“	235
2.8	Risiko-Kontroll-Matrix „Finanzen“	248
2.9	Risiko-Kontroll-Matrix „Steuern“	269
2.10	Risiko-Kontroll-Matrix „Informationstechnologie“	289
2.11	Funktionstrennungs-Matrix als Ergänzung der Risiko-Kontroll-Matrix	313
3	Fraud-Indikatoren für die Prozesse im Internen Kontrollsystem (IKS) ..	319
3.1	Einführung in die Fraud-Thematik	319
3.2	Fraud-Indikatoren „Beschaffung“	335
3.3	Fraud-Indikatoren „Produktion“	339
3.4	Fraud-Indikatoren „Absatz“	342
3.5	Fraud-Indikatoren „Anlagevermögen“	346
3.6	Fraud-Indikatoren „Personal“	347
3.7	Fraud-Indikatoren „Rechnungslegung“	348

3.8	Fraud-Indikatoren „Finanzen“	350
3.9	Fraud-Indikatoren „Steuern“	353
3.10	Fraud-Indikatoren „Informationstechnologie“	356
4	Kennzahlen für die Prozesse im Internen Kontrollsystem (IKS)	359
4.1	Begriff und Aufgaben von Kennzahlen	359
4.2	Kennzahlen „Beschaffung“	361
4.3	Kennzahlen „Produktion“	368
4.4	Kennzahlen „Absatz“	378
4.5	Kennzahlen „Anlagevermögen“	385
4.6	Kennzahlen „Personal“	387
4.7	Kennzahlen „Rechnungslegung“	392
4.8	Kennzahlen „Finanzen“	402
4.9	Kennzahlen „Steuern“	409
4.10	Kennzahlen „Informationstechnologie“	411
Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)		419
1	Konzeption und Planung eines IKS	421
2	Implementierung und Dokumentation eines IKS	427
3	Überwachung und Pflege eines IKS	431
4	Besonderheiten von kleinen und mittelständischen Unternehmen in Bezug auf ein IKS	439
5	Prüfung des Projekts zur Implementierung eines IKS	443
6	Zusammenfassung: Erfolgsfaktoren aus der Praxis bei der Einführung eines IKS	445
Kapitel IV: Enterprise Risk Management (ERM) als Modell zur Integration von Internen Kontrollsystemen (IKS), Interner Revision und Risikomanagement		447
1	Einführung in die gesetzlichen Grundlagen des Risikomanagement ...	447
2	Weiterentwicklung des COSO-Report zum ERM-Framework	453
3	Aufbau des ERM-Framework für ein unternehmensweites Risikomanagement	457
4	Rolle der Internen Revision im ERM-Framework	465
5	Compliance Management System (CMS) im ERM-Modell	473
6	Zusammenfassung: IKS, Interne Revision und Risikomanagement als integrale Bestandteile des ERM	483
Literaturverzeichnis		485
Stichwortverzeichnis		493