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

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/978-3-503-19462-9

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

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.

Satz: multitext Berlin
Druck und Bindung: Hubert & Co., Göttingen

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