

Handbuch Interne Kontrollsysteme (IKS)

Steuerung und Überwachung
von Unternehmen

Von

Dr. Oliver Bungartz

5., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 17145 3

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

Gedrucktes Werk: ISBN 978 3 503 17144 6
eBook: ISBN 978 3 503 17145 3

Alle Rechte vorbehalten
© Erich Schmidt Verlag GmbH & Co. KG , Berlin 2017
www.ESV.info

Ergeben sich zwischen der Version dieses eBooks
und dem gedruckten Werk Abweichungen,
ist der Inhalt des gedruckten Werkes verbindlich.

Satz: multitext, Berlin

Vorwort zur fünften Auflage

Die Aktualität und Popularität des Themas „Interne Kontrollsysteme (IKS)“ nimmt weiterhin zu. Gerade erst hat das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) mit dem „IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)“ neue nationale Maßstäbe für die freiwillige Prüfung eines IKS gesetzt. Der IDW Prüfungsstandard ist dabei nur *eine* wesentliche Neuerung auf dem Gebiet des IKS.

Das „Handbuch Interne Kontrollsysteme (IKS) – Steuerung und Überwachung von Unternehmen“ ist mittlerweile als Standardwerk anerkannt. Die Nachfrage ist zu unserer großen Freude unvermindert hoch, so dass nach Abverkauf der 4. Auflage eine Neuauflage die Möglichkeit bietet, alle wichtigen Aktualisierungen und Ergänzungen aufzunehmen.

Für die nun vorliegende fünfte, neu bearbeitete und erweiterte Auflage wurden die bewährte Konzeption und Struktur der Voraufgaben beibehalten, da sie weiterhin die Zustimmung der Leser finden. Neben Änderungen und Erweiterungen aufgrund neuer Gesetze und Standards wurde die fünfte Auflage u.a. um folgende Aspekte und Abschnitte erweitert:

- Ergänzung des „Kapitel I: Grundlagen eines Internen Kontrollsystems (IKS)“ um die wesentlichen Inhalte des IDW Prüfungsstandards zur freiwilligen Prüfung des IKS (IDW PS 982)
- Integration und Darstellung einer Zuordnung von COSO-Komponenten und COSO-Prinzipien zu COBIT-Prozessen (COSO-COBIT-Mapping)
- Berücksichtigung der aktuellen Entwicklungen im Bereich der Dokumentation eines IKS durch die Darstellung von Auflistungen zu wesentlichen Tabellenkalkulationen, Berichten und ausgelagerten Dienstleistungen
- Ergänzung des „Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)“ um wesentliche Inhalte des „Fraud Risk Management Guide“ von COSO
- Ergänzung des „Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)“ um den Prozess zur Auswahl wesentlicher IT-Anwendungen (IT-Scoping) im Rahmen der Risikobeurteilung
- Ergänzung des „Kapitel IV: Enterprise Risk Management (ERM) als Modell zur Integration von Internen Kontrollsystemen (IKS), Interner Revision und Risikomanagement“ um die Änderungen aus der aktuellen Überarbeitung des ERM-Framework von COSO

- Integration und Darstellung der neuen IDW Prüfungsstandards zu der freiwilligen Prüfung von Risikomanagementsystemen (IDW PS 981) und Internen Revisions-systemen (IDW PS 983)
- Erweiterung des Kapitels IV.5 zu Compliance Management Systemen (CMS) um das Thema „Tax CMS“

Das gesamte Werk wurde wieder gründlich geprüft, wobei kleinere Fehler bereinigt und die Literaturhinweise aktualisiert wurden. Die Bearbeitung und Erweiterung für die fünfte Auflage führte zu zahlreichen neuen Tabellen und Abbildungen. Die Verzeichnisse wurden entsprechend aktualisiert und erweitert.

Bei den Voraufgaben wurden bereits die jeweils notwendigen Ergänzungen und Aktualisierungen bei den rechtlichen Grundlagen und Standards berücksichtigt. Die vierte, neu bearbeitete und erweiterte Auflage aus dem Jahr 2014 wurde u.a. um folgende Aspekte und Abschnitte ergänzt:

- Änderungen des COSO-Rahmenwerks von 2013 und Darstellung der 17 grundlegenden Prinzipien und 87 Attribute zur umfassenden Charakterisierung aller COSO-Komponenten
- Darstellung des völlig neu bearbeiteten Rahmenwerks der Information Systems Audit and Control Association (ISACA) – Control Objectives for Information and related Technology (COBIT 5)
- Überblick zu den chinesischen Regelungen und Verlautbarungen betreffend das IKS (C-SOX)
- Kapitel zur Auslagerung von (Teil-) Prozessen (Outsourcing) um Inhalte des „IDW-Prüfungsstandards: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n.F.)“
- Besonderheiten kleiner und mittelständischer Unternehmen sowie der wettbewerblichen Notwendigkeit eines IKS
- Internationale Vorschriften und Grundsätze im Kapitel CMS

In der dritten Auflage 2012 sowie in der zweiten Auflage aus dem Jahr 2011 wurde das Handbuch u.a. um folgende Aspekte und Teile erweitert:

- Krisenindikatoren und Krisensymptome in den jeweiligen Prozessen eines IKS
- ISO Standard zum Risikomanagement und Einordnung des IKS in ein Integriertes Managementsystem
- Praxisthesen zur Vorteilhaftigkeit von Kontrollen und praktische Beispiele zu den verschiedenen IKS-Komponenten
- Darstellung eines Ansatzes zur effektiven Überwachung
- Herausforderungen der Projektorganisation zur Implementierung eines IKS
- Capability Maturity Model Integration (CMMI) zur Bestimmung des Reifegrads eines IKS
- Kapitel zum Compliance Management System (CMS)

Für ihre Hilfe bei der Realisierung der fünften Auflage danke ich meinen Kollegen, die mich bereits bei den Voraufgaben unterstützt haben. Besonders hervorzuheben sind wertvolle Hinweise meiner Kollegin und Kollegen Frau Sophia Hueber sowie den Herren Gregor Strobl und Stefan Boldorf bei RSM / BRL-Boege Rohde Luebbenhuesen in Hamburg. 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 2017

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

Vorwort zur fünften Auflage.....	5
Vorwort zur ersten Auflage.....	9
Abkürzungsverzeichnis.....	15
Abbildungsverzeichnis.....	21
Tabellenverzeichnis.....	23
Kapitel I: Grundlagen eines Internen Kontrollsystems (IKS)	25
1 Einführung in ein Internes Kontrollsystem (IKS)	25
1.1 Begriff und Aufgaben eines IKS	25
1.2 Internationale Anforderungen an ein IKS.....	27
1.3 Nationale Anforderungen an ein IKS.....	41
1.4 Mehrwert und Grenzen eines IKS	47
1.5 Zusammenfassung: Definition und Anforderungen an ein IKS.....	49
1.6 Exkurs: Freiwillige Prüfung eines IKS nach dem „IDW Prüfungs- standard: Grundsätze ordnungsmäßiger Prüfungen des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982)“.....	50
2 Ausgestaltung eines Internen Kontrollsystems (IKS) nach den Empfehlungen des Committee of Sponsoring Organizations of the Treadway Commission (COSO).....	55
2.1 Aufbau eines IKS nach COSO	55
2.2 „Kontrollumfeld“ als Komponente eines IKS	58
2.3 „Risikobeurteilung“ als Komponente eines IKS	66
2.4 „Kontrollaktivitäten“ als Komponente eines IKS	70
2.5 „Information und Kommunikation“ als Komponente eines IKS	76
2.6 „Überwachungsaktivitäten“ als Komponente eines IKS	79
2.7 Grundlegende Prinzipien und Attribute der COSO-Komponenten ...	88
2.8 Kontrollaktivitäten auf Unternehmensebene zur Überwachung der COSO-Komponenten	96
2.9 Zusammenfassung: IKS nach COSO	114
2.10 Exkurs: COSO und die Control Objectives for Information and Related Technology (COBIT)	115
3 Dokumentation eines Internen Kontrollsystems (IKS)	131
3.1 Allgemeine Anforderungen an die Dokumentation eines IKS.....	131
3.2 Verbale Prozessbeschreibung als Möglichkeit der Dokumentation von Prozessabläufen im IKS	133

3.3	Flussdiagramm als Möglichkeit zur Dokumentation von Prozessabläufen im IKS	134
3.4	Risiko-Kontroll-Matrix als Möglichkeit zur Dokumentation des Aufbaus und der Funktion eines IKS	136
3.5	Testblatt als Möglichkeit zur Dokumentation von Funktionsprüfungen im IKS	138
3.6	Matrix als Möglichkeit zur Dokumentation der Funktionstrennung im IKS	142
3.7	Auflistung als Möglichkeit zur Dokumentation von Informationen zu wesentlichen Tabellenkalkulationen und Berichten	144
3.8	Auflistung als Möglichkeit zur Dokumentation von Informationen zu wesentlichen Dienstleistern für ausgelagerte Tätigkeiten	147
3.9	Maßnahmeplan als Möglichkeit zur Dokumentation von Schwachstellen und Überwachungstätigkeiten im IKS	149
3.10	Zusammenfassung: Dokumentationsmöglichkeiten eines IKS	150
Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)		153
1	Grundlagen der Organisation von Prozessen im Internen Kontrollsystem (IKS)	153
1.1	Organisation von Prozessen im Unternehmen	153
1.2	Organisation „Beschaffung“	155
1.3	Organisation „Produktion“	160
1.4	Organisation „Absatz“	164
1.5	Organisation „Anlagevermögen“	166
1.6	Organisation „Personal“	168
1.7	Organisation „Rechnungslegung“	171
1.8	Organisation „Finanzen“	173
1.9	Organisation „Steuern“	179
1.10	Organisation „Informationstechnologie“	187
2	Risiko-Kontroll-Matrizen für die Prozesse im Internen Kontrollsystem (IKS)	195
2.1	Grundlagen der Erstellung von Risiko-Kontroll-Matrizen.	196
2.2	Risiko-Kontroll-Matrix „Beschaffung“	197
2.3	Risiko-Kontroll-Matrix „Produktion“	212
2.4	Risiko-Kontroll-Matrix „Absatz“	231
2.5	Risiko-Kontroll-Matrix „Anlagevermögen“	243
2.6	Risiko-Kontroll-Matrix „Personal“	253
2.7	Risiko-Kontroll-Matrix „Rechnungslegung“	270
2.8	Risiko-Kontroll-Matrix „Finanzen“	283
2.9	Risiko-Kontroll-Matrix „Steuern“	304
2.10	Risiko-Kontroll-Matrix „Informationstechnologie“	324
2.11	Funktionstrennungs-Matrix als Ergänzung der Risiko-Kontroll-Matrix.	348

3	Fraud-Indikatoren für die Prozesse im Internen Kontrollsystem (IKS) .	353
3.1	Einführung in die Fraud-Thematik	353
3.2	Fraud-Indikatoren „Beschaffung“	374
3.3	Fraud-Indikatoren „Produktion“	378
3.4	Fraud-Indikatoren „Absatz“	381
3.5	Fraud-Indikatoren „Anlagevermögen“	385
3.6	Fraud-Indikatoren „Personal“	386
3.7	Fraud-Indikatoren „Rechnungslegung“	387
3.8	Fraud-Indikatoren „Finanzen“	389
3.9	Fraud-Indikatoren „Steuern“	392
3.10	Fraud-Indikatoren „Informationstechnologie“	395
4	Kennzahlen für die Prozesse im Internen Kontrollsystem (IKS)	399
4.1	Begriff und Aufgaben von Kennzahlen	399
4.2	Kennzahlen „Beschaffung“	401
4.3	Kennzahlen „Produktion“	408
4.4	Kennzahlen „Absatz“	418
4.5	Kennzahlen „Anlagevermögen“	425
4.6	Kennzahlen „Personal“	427
4.7	Kennzahlen „Rechnungslegung“	432
4.8	Kennzahlen „Finanzen“	442
4.9	Kennzahlen „Steuern“	450
4.10	Kennzahlen „Informationstechnologie“	452
 Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)		
1	Konzeption und Planung eines IKS	461
2	Implementierung und Dokumentation eines IKS	469
3	Überwachung und Pflege eines IKS	473
4	Besonderheiten von kleinen und mittelständischen Unternehmen in Bezug auf ein IKS	481
5	Erweiterung des IKS um Krisenindikatoren	489
6	Prüfung des Projekts zur Implementierung eines IKS	497
7	Zusammenfassung: Erfolgsfaktoren aus der Praxis bei der Einführung eines IKS	499
 Kapitel IV: Enterprise Risk Management (ERM) als Modell zur Integration von Internen Kontrollsystemen (IKS), Internal Revision und Risikomanagement		
1	Einführung in die gesetzlichen Grundlagen des Risikomanagement . . .	503
2	Freiwillige Prüfung eines Risikomanagementsystems nach dem „IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)“	509
3	Weiterentwicklung des COSO-Report zum ERM-Framework	515
4	Aufbau des ERM-Framework für ein unternehmensweites Risikomanagement	519

5	Rolle der Internen Revision im ERM-Framework	535
6	Compliance Management System (CMS) im ERM-Modell	545
7	Kompatibilität des ERM-Framework mit ISO Standards zum Risiko- management und Einordnung in ein integriertes Managementsystem .	565
8	Zusammenfassung: IKS, Interne Revision und Risikomanagement als integrale Bestandteile des ERM	573
	Literaturverzeichnis	577
	Stichwortverzeichnis	587