

Handbuch Interne Kontrollsysteme (IKS)

Steuerung und Überwachung
von Unternehmen

Von
Dr. Oliver Bungartz

7., völlig 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/978-3-503-24078-4

1. Auflage 2010
2. Auflage 2011
3. Auflage 2012
4. Auflage 2014
5. Auflage 2017
6. Auflage 2020
7. Auflage 2026

Gedrucktes Werk: ISBN 978-3-503-24078-4

eBook: ISBN 978-3-503-24079-1

Alle Rechte vorbehalten.

© 2026 Erich Schmidt Verlag GmbH & Co. KG

Genthiner Straße 30 G, 10785 Berlin

info@ESVmedien.de, www.ESV.info

Die Nutzung für das Text und Data Mining ist ausschließlich dem Erich Schmidt Verlag GmbH & Co. KG vorbehalten.

Der Verlag untersagt eine Vervielfältigung gemäß § 44b UrhG ausdrücklich.

Satz: PER MEDIEN & MARKETING GmbH

Druck und Bindung: Beltz Grafische Betriebe, Bad Langensalza

Vorwort zur siebten 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 des IKS stetig zu. Dies gilt umso mehr vor dem Hintergrund aktueller Entwicklungen im Bereich der nicht-finanziellen Berichterstattung. Die zunehmenden Anforderungen an Transparenz und Nachvollziehbarkeit im Rahmen der Nachhaltigkeitsberichterstattung sowie das gestiegene öffentliche und regulatorische Interesse rücken den Aufbau und die Wirksamkeit von internen Kontrollen und Risikomanagement erneut in den Fokus. So gewinnt das IKS nicht nur für die klassische Finanzberichterstattung, sondern auch zur Sicherstellung der Verlässlichkeit und Integrität nicht-finanzieller Informationen zunehmend an Bedeutung. Auch angesichts der IT und Digitalisierung (z.B. Robotic Process Automation – RPA) in der Unternehmenspraxis sind Risiken und Kontrollen in diesen Bereich untrennbar mit dem operativen Tagesgeschäft und den strategischen Zielen einer jeden Organisation verbunden.

Das „Handbuch Interne Kontrollsysteme (IKS) – Steuerung und Überwachung von Unternehmen“ ist als Standardwerk etabliert und die Nachfrage ist zu unserer großen Freude unvermindert hoch. Fast 15 Jahre nachdem das Handbuch erstmals erschienen ist, bietet – nach Abverkauf der sechsten 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 Literaturhinweise aktualisiert sowie erweitert wurden. Die Bearbeitung und Erweiterung führten zu zahlreichen neuen Tabellen und Abbildungen.

Für die siebte, neu bearbeitete und erweiterte Auflage wurde die bewährte Konzeption und Struktur der Voraufgaben 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)“:
 - Aufnahme relevanter gesetzlicher Regelungen mit Bezug zum IKS aus dem Finanzmarktstabilitätsstärkungsgesetz (FISG) und dem „Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG)“
 - Hervorhebung der Nachhaltigkeit als Ziel des COSO-Reports zum IKS als Beispiel der nicht-finanziellen Berichterstattung

- Darstellung der Governance-Bereiche eines Rahmenwerks für Robotic Process Automation (RPA) sowie die Integration in die COSO-Komponenten anhand von RPA-Kontrollanforderungen und beispielhaften Kontrollaktivitäten (sog. integrierter COSO-IKS-RPA-Governance-Ansatz)
- Aktualisierung des „Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)“ und des „Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)“ um notwendige Änderungen und strukturelle Anpassungen
- Hinzufügung des „Kapitel IV: Erweiterung des Internen Kontrollsystems (IKS) im Hinblick auf die Nachhaltigkeitsberichterstattung“ unter Berücksichtigung der Anforderungen, Ausgestaltung und Komponenten eines IKS sowie beispielhaften Risiko-Kontroll-Matrizen (RKM) und Kennzahlen für wesentliche Prozesse (insb. Environmental, Social, Governance – ESG)
- Ergänzung des „Kapitel V: Enterprise Risk Management (ERM) als Modell zur Integration von Internen Kontrollsystemen (IKS), Interner Revision und Risikomanagement“:
 - Aufnahme relevanter gesetzlicher Regelungen mit Bezug zum Risikomanagement aus dem FISG und Aktualisierung der Anforderungen aus dem Deutschen Corporate Governance Kodex (DCGK)
 - Berücksichtigung der Änderungen durch die neuen Global Internal Audit Standards (GIAS) des „The Institute of Internal Auditors (IIA)“ in Bezug auf die Prüfung des Risikomanagements durch die Interne Revision
 - Integration der Aktualisierungen des Standards „ISO 31000 – Risk management“
 - Hinzufügung eines Exkurses zur Integration von Nachhaltigkeitsrisiken im ESG-Bereich auf Basis des ERM-Frameworks

Bei den Voraufgaben 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 siebten Auflage danke ich meinen Kollegen Herrn Kogan und Herrn Saveliev, die mich bereits bei den Voraufgaben unterstützt haben. Auch für die gewohnt reibungslose Zusammenarbeit mit dem Erich Schmidt Verlag (ESV) in Berlin möchte ich Frau Claudia Splittgerber, Herrn Fabarius und Herrn Dr. Joachim Schmidt ganz herzlich danken. Nicht zuletzt gilt besonderer Dank meinen Seminarteilnehmern, Kunden 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 November 2025

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 siebten Auflage	5
Vorwort zur ersten Auflage	7
Abkürzungsverzeichnis	11
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	37
1.4 Mehrwert und Grenzen eines IKS	43
1.5 Zusammenfassung: Definition und Anforderungen an ein IKS	45
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)“	47
2 Ausgestaltung eines Internen Kontrollsystems (IKS) nach den Empfehlungen des Committee of Sponsoring Organizations of the Treadway Commission (COSO)	50
2.1 Aufbau eines IKS nach COSO	50
2.2 „Kontrollumfeld“ als Komponente eines IKS	53
2.3 „Risikobeurteilung“ als Komponente eines IKS	62
2.4 „Kontrollaktivitäten“ als Komponente eines IKS	66
2.5 „Information und Kommunikation“ als Komponente eines IKS	71
2.6 „Überwachungsaktivitäten“ als Komponente eines IKS	74
2.7 Grundlegende Prinzipien und Attribute der COSO-Komponenten	85
2.8 Kontrollaktivitäten auf Unternehmensebene zur Überwachung der COSO-Komponenten	93
2.9 Zusammenfassung: IKS nach COSO	112
2.10 Exkurs: COSO und die Control Objectives for Information and Related Technology (COBIT)	113
2.11 Exkurs: COSO und Robotic Process Automation (RPA)	134
3 Dokumentation eines Internen Kontrollsystems (IKS)	145
3.1 Allgemeine Anforderungen an die Dokumentation eines IKS	145
3.2 Verbale Prozessbeschreibung als Möglichkeit der Dokumentation von Prozessabläufen im IKS	147
3.3 Flussdiagramm als Möglichkeit zur Dokumentation von Prozessabläufen im IKS	147
3.4 Risiko-Kontroll-Matrix (RKM) als Möglichkeit zur Dokumentation des Aufbaus und der Funktion eines IKS	150
3.5 Testblatt als Möglichkeit zur Dokumentation von Funktionsprüfungen im IKS	151

3.6	Matrix als Möglichkeit zur Dokumentation der Funktionstrennung im IKS	154
3.7	Auflistung als Möglichkeit zur Dokumentation von Informationen zu wesentlichen Tabellenkalkulationen und Berichten	157
3.8	Auflistung als Möglichkeit zur Dokumentation von Informationen zu wesentlichen Dienstleistern für ausgelagerte Tätigkeiten	159
3.9	Maßnahmenplan als Möglichkeit zur Dokumentation von Schwachstellen und Überwachungstätigkeiten im IKS	160
3.10	Zusammenfassung: Dokumentationsmöglichkeiten eines IKS	162
Kapitel II: Prozesse eines Internen Kontrollsystems (IKS)		163
1	Grundlagen der Organisation von Prozessen im Internen Kontrollsystem (IKS)	163
1.1	Organisation von Prozessen im Unternehmen	163
1.2	Organisation „Beschaffung“	164
1.3	Organisation „Produktion“	169
1.4	Organisation „Absatz“	172
1.5	Organisation „Anlagevermögen“	174
1.6	Organisation „Personal“	176
1.7	Organisation „Rechnungslegung“	179
1.8	Organisation „Finanzen“	181
1.9	Organisation „Steuern“	186
1.10	Organisation „Informationstechnologie“	193
2	Risiko-Kontroll-Matrizen (RKM) für die Prozesse im Internen Kontrollsystem (IKS)	200
2.1	Grundlagen der Erstellung von Risiko-Kontroll-Matrizen (RKM)	200
2.2	Risiko-Kontroll-Matrix (RKM) „Beschaffung“	201
2.3	Risiko-Kontroll-Matrix (RKM) „Produktion“	216
2.4	Risiko-Kontroll-Matrix (RKM) „Absatz“	234
2.5	Risiko-Kontroll-Matrix (RKM) „Anlagevermögen“	247
2.6	Risiko-Kontroll-Matrix (RKM) „Personal“	256
2.7	Risiko-Kontroll-Matrix (RKM) „Rechnungslegung“	273
2.8	Risiko-Kontroll-Matrix (RKM) „Finanzen“	287
2.9	Risiko-Kontroll-Matrix (RKM) „Steuern“	308
2.10	Risiko-Kontroll-Matrix (RKM) „Informationstechnologie“	327
2.11	Funktionstrennungs-Matrix als Ergänzung der Risiko-Kontroll-Matrix (RKM)	350
3	Fraud-Indikatoren für die Prozesse im Internen Kontrollsystem (IKS)	356
3.1	Einführung in die Fraud-Thematik	356
3.2	Fraud-Indikatoren „Beschaffung“	375
3.3	Fraud-Indikatoren „Produktion“	379
3.4	Fraud-Indikatoren „Absatz“	381
3.5	Fraud-Indikatoren „Anlagevermögen“	384
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“	394
4	Kennzahlen für die Prozesse im Internen Kontrollsystem (IKS)	397
4.1	Begriff und Aufgaben von Kennzahlen	397
4.2	Kennzahlen „Beschaffung“	399
4.3	Kennzahlen „Produktion“	405
4.4	Kennzahlen „Absatz“	414
4.5	Kennzahlen „Anlagevermögen“	420
4.6	Kennzahlen „Personal“	422
4.7	Kennzahlen „Rechnungslegung“	426
4.8	Kennzahlen „Finanzen“	434
4.9	Kennzahlen „Steuern“	442
4.10	Kennzahlen „Informationstechnologie“	444
Kapitel III: Projektmanagement zur Einrichtung eines Internen Kontrollsystems (IKS)		459
1	Konzeption und Planung eines IKS	460
2	Implementierung und Dokumentation eines IKS	466
3	Überwachung und Pflege eines IKS	468
4	Besonderheiten von kleinen und mittelständischen Unternehmen in Bezug auf ein IKS	480
5	Erweiterung des IKS um Krisenindikatoren	487
6	Prüfung des Projekts zur Implementierung eines IKS	495
7	Zusammenfassung: Erfolgsfaktoren aus der Praxis bei der Einführung eines IKS	497
Kapitel IV: Erweiterung des Internen Kontrollsystems (IKS) im Hinblick auf die Nachhaltigkeitsberichterstattung		501
1	Einführung in das IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	501
2	Anforderungen, Ausgestaltung und Komponenten des IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	504
2.1	Anforderungen an das IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	504
2.2	Ausgestaltung des IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	508
2.3	Komponenten eines IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	510
3	Prozesse eines IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	515
3.1	Risiko-Kontroll-Matrix (RKM) „Themenübergreifend (TG)“	515
3.2	Risiko-Kontroll-Matrix (RKM) „Environmental (EN)“	520
3.3	Risiko-Kontroll-Matrix (RKM) „Social (SO)“	529
3.4	Risiko-Kontroll-Matrix (RKM) „Governance (GN)“	535

4	Kennzahlen für die Nachhaltigkeitsberichterstattung	541
4.1	Nachhaltigkeitskennzahlen „Themenübergreifend“	542
4.2	Nachhaltigkeitskennzahlen „Environmental“	542
4.3	Nachhaltigkeitskennzahlen „Social“	546
4.4	Nachhaltigkeitskennzahlen „Governance“	550
5	Zusammenfassung: Grundlagen, Anforderungen und Ausgestaltung der Erweiterung eines IKS im Hinblick auf die Nachhaltigkeitsberichterstattung	551

**Kapitel V: Enterprise Risk Management (ERM) als Modell zur Integration
von Internen Kontrollsystemen (IKS), Interner Revision und
Risikomanagement**

		553
1	Einführung in die gesetzlichen Grundlagen des Risikomanagements	553
2	Freiwillige Prüfung eines Risikomanagementsystems nach dem „IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)“	558
3	Weiterentwicklung des COSO-Report zum ERM-Framework	563
4	Aufbau des ERM-Frameworks für ein unternehmensweites Risiko- management	567
5	Rolle der Internen Revision im ERM-Framework	595
6	Compliance Management System (CMS) im ERM-Modell	606
7	Kompatibilität des ERM-Frameworks mit ISO Standards zum Risiko- management und Einordnung in ein integriertes Managementsystem	628
8	Zusammenfassung: IKS, Interne Revision und Risikomanagement als integrale Bestandteile des ERM	636
	Literaturverzeichnis	639
	Stichwortverzeichnis	653