

---

**Krzysztof Paschke**  
**Internes Kontrollsystem**  
**Umsetzung, Dokumentation und Prüfung**



Krzysztof Paschke ist geschäftsführender Gesellschafter der GRC Partner GmbH in Kiel. Er studierte Wirtschaftsinformatik an der Wirtschaftsakademie Schleswig-Holstein. Nach dem Studium war er als IT-Berater und leitender Angestellter tätig. Seit 2003 ist er maßgeblich an der Konzeption und Entwicklung der Compliance Management Software DocSetMinder® und GDPdU-Warehouse beteiligt. Der Schwerpunkt seiner Tätigkeit als Berater liegt in Bereichen der Compliance Management und IT-Governance.

Sein besonderes Interesse gilt hierbei den unterschiedlichen Facetten der Compliance-Dokumentation. Die Erfahrungen aus zahlreichen Projekten in unterschiedlichen Branchen setzt Herr Paschke bei der Optimierung der Einführungs- und Dokumentationsmethodik der Compliance Management Systeme sowie der genannten Softwarelösungen ein.

---

# **Internes Kontrollsystem**

## **Umsetzung, Dokumentation und Prüfung**

Praxisleitfaden für eine softwaregestützte  
Organisation der internen Kontrollen

**Krzysztof Paschke**

---

Weitere Informationen zum Thema Governance Risk und Compliance, Compliance Management Software DocSetMinder® finden Sie auf folgenden Internetseiten:

[www.docsetminder.de](http://www.docsetminder.de)

[www.grc-partner.de](http://www.grc-partner.de)

Alle Informationen und Anwendungen in dieser Publikation wurden nach bestem Wissen zusammengestellt und mit größter Sorgfalt kontrolliert. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Autor und Verlag können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Verwendete Bezeichnungen, Markennamen und Produktbezeichnungen unterliegen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz.

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN-978-3-84231-436-8

© 2011 Krzysztof Paschke

Herstellung und Verlag: Books on Demand GmbH, Norderstedt

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Verbreitung, ganz oder teilweise, ist verboten. Kein Teil der Dokumentation darf ohne schriftliche Genehmigung des Autors in irgendeiner Form durch Fotokopie, Mikrofilm oder andere Verfahren reproduziert oder in eine für Maschinen, insbesondere Datenverarbeitungsanlagen, verwendbare Sprache übertragen werden.

## **Vorwort**

Spektakuläre Unternehmenskrisen u.a. in den Vereinigten Staaten und in Europa haben im letzten Jahrzehnt sowohl die nationale als auch die internationale Diskussion über die Grundsätze einer Corporate Governance intensiviert. Die Einhaltung von geltenden nationalen und internationalen Gesetzen und Vorschriften (Compliance) durch die Gestaltung und Umsetzung einer effektiven Corporate Governance stellt eine wesentliche Herausforderung für die Führungskräfte, Aufsichtsgremien und Mitarbeiter in Unternehmen dar. Die aktuelle weltweite Finanz- und Wirtschaftskrise macht deutlich, wie wichtig das Thema unabhängig von Unternehmensgröße und Branche ist. Corporate Governance und Compliance Management spielen dabei eine sehr wichtige Rolle, um drohende Risiken frühzeitig zu erkennen und sie beherrschbar zu machen. Ein internes Kontrollsystem und eine Risikobeurteilung gehören zu den wichtigsten Bestandteilen einer wirksamen Corporate Governance im Unternehmen. Der vorliegende Praxisleitfaden beschreibt eine systematische Einführung und Dokumentation eines unternehmensweiten internen Kontrollsystems. Eine besondere Rolle spielt dabei die Dokumentation. Eine vollständige und sachgerechte Dokumentation stellt die Basis für eine erfolgreiche Umsetzung der Compliance dar und dient dem Nachweis sowie als Kommunikationsmedium der getroffenen organisatorischen und technischen Maßnahmen. Sie ist unabdingbar bei jeder Art von Audits, die durch interne oder externe Auditoren und Prüfer durchgeführt werden. Durch den Einsatz der Compliance Management Software DocSetMinder® kann die Etablierung, Dokumentation und Prüfung des internen Kontrollsystems sehr effizient und effektiv realisiert werden.

# Inhaltsverzeichnis

<b>1</b>	<b>Ziel und Aufbau des Buches</b> .....	<b>13</b>
<b>2</b>	<b>Gesetzliche Grundlagen</b> .....	<b>17</b>
2.1	IKS Definition .....	17
2.2	IKS in der EU .....	20
2.3	IKS in Deutschland .....	20
2.4	IKS in der Schweiz.....	21
2.5	Sarbanes-Oxley Act (SOX).....	23
<b>3</b>	<b>Standards</b> .....	<b>25</b>
3.1	COSO.....	25
3.1.1	IKS-Kategorien (Dimension I).....	25
3.1.2	IKS-Komponenten (Dimension II) .....	26
3.1.3	Unternehmensorganisation (Dimension III).....	27
3.2	IDW PS 261 .....	28
3.2.1	IKS-Ziele .....	28
3.2.2	IKS-Komponenten.....	29
3.2.3	Unternehmensorganisation .....	30
3.3	IDW PS 330 .....	30
3.4	IT-Governance .....	34
3.4.1	CobiT.....	35
3.4.2	ITIL .....	37
<b>4</b>	<b>Dokumentation</b> .....	<b>39</b>
4.1	Unternehmensweite Dokumentationslösung .....	39
4.2	Aspekte der Dokumentation .....	41
4.3	Eigenschaften einer Compliance Management Software .....	43
4.4	Dokumentationsrichtlinie im Unternehmen .....	46
4.4.1	Redaktion.....	47
4.4.2	Detaillierungsgrad und Tiefe der Dokumentation.....	49
4.4.3	Fortführung der Dokumentation.....	51

---

<b>4.4.4</b>	Systematik der Dokumentation.....	52
<b>4.4.5</b>	Namenskonventionen .....	54
<b>4.5</b>	Lebenszyklus der Dokumentation und verwendete Methoden.....	55
<b>4.5.1</b>	S.M.A.R.T. ....	56
<b>4.5.2</b>	Magisches Dreieck .....	57
<b>4.5.3</b>	Deming-Kreis .....	58
<b>5</b>	<b>IKS-Projekt .....</b>	<b>61</b>
5.1	Projektmethodik und Softwareunterstützung .....	61
5.2	Wind Seeker AG.....	61
5.3	Meilenstein 1 „Projektmanagement“ .....	63
<b>5.3.1</b>	Ziel .....	63
<b>5.3.2</b>	Beschreibung und Definitionen .....	63
5.3.2.1	Initialisierung .....	64
5.3.2.2	Definition .....	64
5.3.2.3	Planung .....	65
5.3.2.4	Steuerung .....	65
5.3.2.5	Abschluss .....	66
<b>5.3.3</b>	Umsetzung mit DocSetMinder® .....	66
5.3.3.1	Projektorganisation .....	68
5.3.3.2	Meilensteine des IKS-Projektes .....	69
5.3.3.3	Dokumentationsrichtlinie .....	71
5.4	Unternehmensorganisation (Zusammenfassung) .....	77
5.5	Meilenstein 2 „Aufbauorganisation“ .....	79
<b>5.5.1</b>	Ziel .....	79
<b>5.5.2</b>	Beschreibung und Definitionen .....	80
<b>5.5.3</b>	Inhalt der Dokumentation .....	82
<b>5.5.4</b>	Umsetzung mit DocSetMinder® .....	83
5.5.4.1	Schritt 1: Modellierung.....	85
5.5.4.2	Schritt 2: Organigramme .....	86
5.5.4.3	Schritt 3: Unternehmensstammdaten.....	88

---

5.5.4.4	Schritt 4: Betriebsstätten und Repräsentanzen .....	89
5.5.4.5	Schritt 5: Abteilungen.....	90
5.5.4.6	Schritt 6: Stellenbeschreibungen .....	92
5.5.4.7	Schritt 7: Mitarbeiter.....	93
5.5.4.8	Schritt 8: Beauftragte .....	95
5.5.4.9	Schritt 9: Fremde Dritte.....	96
5.5.4.10	Schritt 10: Prüfer .....	96
5.5.4.11	Dokumentationshinweis.....	97
5.6	Meilenstein 3 „Ablauforganisation“ .....	102
5.6.1	Ziel .....	102
5.6.2	Beschreibung und Definitionen.....	102
5.6.3	Inhalt der Dokumentation.....	105
5.6.4	Umsetzung mit DocSetMinder® .....	106
5.6.4.1	Schritt 1: Dokumentation der Prozesslandkarte .....	110
5.6.4.2	Schritt 2: Dokumentation der Prozesse Ebene 1.....	111
5.6.4.3	Schritt 3: Dokumentation der Prozesse Ebene n.....	112
5.6.4.4	Schritt 4: Dokumentation der Arbeitsanweisungen.....	114
5.6.4.5	Wertschöpfungskette .....	115
5.6.4.6	Dokumentationshinweis.....	122
5.7	Meilenstein 4 „Richtlinien“ .....	125
5.7.1	Ziel .....	125
5.7.2	Beschreibung und Definitionen.....	125
5.7.3	Inhalt der Dokumentation.....	126
5.7.4	Umsetzung mit DocSetMinder® .....	127
5.7.4.1	Dokumentationshinweis.....	131
5.8	Internes Kontrollsystem (Zusammenfassung).....	131
5.9	Meilenstein 5 „Kontrollumfeld“ .....	133
5.9.1	Ziel .....	133
5.9.2	Beschreibung und Definitionen.....	134
5.9.3	Umsetzung mit DocSetMinder® .....	135



---

5.10	Meilenstein 6 „Risikobewertung“ .....	136
<b>5.10.1</b>	Ziel .....	136
<b>5.10.2</b>	Beschreibung und Definitionen .....	137
5.10.2.1	Risikoidentifikation .....	140
5.10.2.2	Risikoanalyse und -bewertung.....	146
<b>5.10.3</b>	Umsetzung mit DocSetMinder® .....	147
5.10.3.1	Dokumentationshinweis.....	151
5.11	Meilenstein 7 „Kontrollziele und Kontrollen“ .....	154
<b>5.11.1</b>	Ziel .....	154
<b>5.11.2</b>	Beschreibung und Definitionen .....	155
<b>5.11.3</b>	Inhalt der Dokumentation .....	155
<b>5.11.4</b>	Umsetzung mit DocSetMinder® .....	162
5.11.4.1	Dokumentationshinweis.....	169
5.12	Meilenstein 8 „Bilanz-, Gewinn- und Verlust-Positionen“ .....	173
<b>5.12.1</b>	Ziel .....	173
<b>5.12.2</b>	Beschreibung und Definitionen .....	173
<b>5.12.3</b>	Inhalt der Dokumentation .....	174
<b>5.12.4</b>	Umsetzung mit DocSetMinder® .....	175
5.12.4.1	Dokumentationshinweis.....	175
5.13	Meilenstein 9 „Risiko-Kontroll-Matrix“ .....	176
<b>5.13.1</b>	Ziel .....	176
<b>5.13.2</b>	Beschreibung und Definitionen .....	176
<b>5.13.3</b>	Inhalt der Dokumentation .....	178
<b>5.13.4</b>	Umsetzung mit DocSetMinder® .....	180
5.13.4.1	Dokumentationshinweis.....	185
5.14	Meilenstein 10 „Monitoring“ .....	190
<b>5.14.1</b>	Ziel .....	190
<b>5.14.2</b>	Beschreibung und Definitionen .....	190
5.14.2.1	Prüfungsplanung.....	191
5.14.2.2	Prüfungshandlung.....	191

---

<b>5.14.3</b>	Inhalt der Dokumentation.....	195
5.14.3.1	Prüfungsplanung .....	195
5.14.3.2	Prüfungsdurchführung .....	195
5.14.3.3	Bewertung der prozessbezogenen Kontrollen .....	201
<b>5.14.4</b>	Umsetzung mit DocSetMinder® .....	204
5.14.4.1	Planung der Prüfung.....	205
5.14.4.2	Prüfungskatalog.....	208
5.14.4.3	Walkthrough-Prozess .....	208
5.14.4.4	Test der Kontrollen.....	211
5.14.4.5	Gesamtbewertung der prozessbezogenen Kontrollen....	214
5.14.4.6	Dokumentationshinweis.....	217
5.15	Meilenstein 11 „Korrekturmaßnahmen“ .....	218
<b>5.15.1</b>	Ziel .....	218
<b>5.15.2</b>	Beschreibung und Definitionen .....	218
<b>5.15.3</b>	Inhalt der Dokumentation.....	218
<b>5.15.4</b>	Umsetzung mit DocSetMinder® .....	219
5.16	Meilenstein 12 „Information und Kommunikation“ .....	221
<b>5.16.1</b>	Ziel .....	221
<b>5.16.2</b>	Beschreibung und Definitionen.....	222
<b>5.16.3</b>	Umsetzung mit DocSetMinder® .....	222
<b>6</b>	<b>Produktbeschreibung DSM.....</b>	<b>227</b>
6.1	Compliance Management Software.....	227
6.2	Modularer Aufbau .....	227
6.3	Strukturaufbau der Dokumentation.....	228
6.4	Module - Zusammenfassung der Modulinhalte .....	229
<b>6.4.1</b>	Modul „Unternehmensorganisation“ .....	229
<b>6.4.2</b>	Modul „Internes Kontrollsystem“ .....	230
<b>6.4.3</b>	Modul „Verrechnungspreisdokumentation“ .....	230
<b>6.4.4</b>	Modul „Verfahrensdokumentation“ .....	233
<b>6.4.5</b>	Modul „CobIT“ .....	235

---

6.4.6	Modul „Qualitätsmanagement“ .....	235
6.4.7	Modul „IT-Dokumentation“ .....	235
6.4.8	Modul „IT-Notfallhandbuch“ .....	236
6.4.9	Modul „IT-Revision“ .....	236
6.4.10	Modul „Datenschutz“ .....	236
6.5	Aufbau und Umgebung .....	237
6.5.1	Funktionsbeschreibung .....	237
6.5.2	Revisionsicherheit .....	237
6.5.3	Versionskontrolle.....	238
6.5.4	Periodenabgrenzung/Jahresabschluss .....	239
6.5.5	Check-in/Check-out .....	240
6.5.6	Dokumentenentwürfe .....	240
6.5.7	Löschen von Dokumenten .....	240
6.5.8	Filter .....	241
6.5.9	Benutzer-Sichten .....	241
6.5.10	Volltextsuche .....	241
6.6	Ausgabe der Dokumentation.....	242
6.7	Dokumentationswerkzeuge.....	244
6.7.1	DocSetMinder® Texteditor .....	245
6.7.2	DocSetMinder® Designer.....	246
6.7.3	DocSetMinder® HTML-Publisher .....	246
6.7.4	Druckexport in Microsoft® Office Word .....	246
6.7.5	Import von externen Dateien .....	248
6.7.6	Standardvorlagen .....	248
6.7.7	Inhaltsklassen .....	249
6.8	Zugriffsschutzsystem .....	251
6.8.1	Rollenkonzept.....	252
6.8.2	Administrator.....	252
6.8.3	Manager.....	252
6.8.4	Bearbeiter .....	252

---

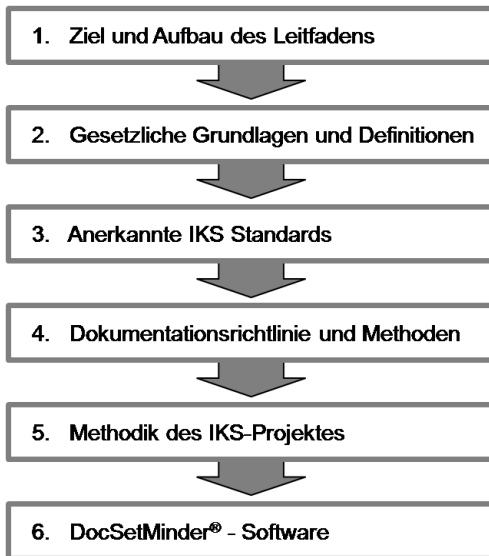
<b>6.8.5</b>	Leser .....	252
<b>6.8.6</b>	Prüfer .....	253
6.9	Active Directory und LDAP Integration .....	253
6.10	DocSetMinder® Clients.....	253
<b>6.10.1</b>	DocSetMinder® Voll-Client.....	254
<b>6.10.2</b>	DocSetMinder® Web Access-Client.....	256
<b>6.10.3</b>	DocSetMinder® Application Programming Interface .....	256
6.11	Reporting Services .....	257
6.12	Hilfe-Funktion.....	257
6.13	Prozessorientiertes Compliance-Management.....	257
6.14	Auszeichnung .....	258
<b>7</b>	<b>IKS-Projekt Checklisten .....</b>	<b>259</b>
7.1	Checklisten - Unternehmensorganisation.....	260
7.2	Checklisten – internes Kontrollsystem .....	263
<b>8</b>	<b>Abbildungen .....</b>	<b>267</b>
<b>9</b>	<b>Abkürzungsverzeichnis.....</b>	<b>273</b>
<b>10</b>	<b>Literatur .....</b>	<b>275</b>

# 1 Ziel und Aufbau des Buches

Die Umsetzung und Dokumentation eines unternehmensweiten internen Kontrollsystems wird in der Regel im Rahmen eines Projektes realisiert. Die vorliegende Publikation wendet sich an alle Projektmitarbeiter: An die Projektleitung wie an die Projektmitarbeiter aus den Fachabteilungen bis hin zu den externen Beratern, die mit der Aufgabe der Implementierung und Dokumentation eines internen Kontrollsystems im Unternehmen beauftragt worden sind. Sie beschreibt eine strukturierte Vorgehensweise bei der Umsetzung der gesetzlichen Anforderungen. Die geltenden Gesetze und Regelungen in Deutschland, in der Schweiz und in der Europäischen Union, welche die Existenz eines wirksamen internen Kontrollsystems begründen, werden nur am Rande erwähnt. Der Schwerpunkt dieses Leitfadens liegt auf der effizienten und effektiven Einführung und Dokumentation eines internen Kontrollsystems. Die Dokumentation stellt die Basis für eine permanente Verbesserung der bereits etablierten Kontrollmaßnahmen im Unternehmen dar. Die im folgenden beschriebene zentrale, datenbankbasierte Softwarelösung bietet viele technische und organisatorische Vorteile, nicht nur bei der Einführung, sondern insbesondere auch bei der systematischen Verbesserung der Kontrollmechanismen im Laufe der Zeit sowie bei der Pflege einer adäquaten Dokumentation. Der noch immer weit verbreitete Einsatz von Textverarbeitungsprogrammen und Tabellenkalkulationen bei derartigen Projekten stellt für diese Aufgaben keine echte Alternative dar. Die verwendete Projekt-Methodik ist unabhängig von der geplanten oder bereits eingesetzten Softwarelösung. Die **Abbildung 1** visualisiert die Struktur des Leitfadens.

In **Kapitel 2** werden die gesetzlichen Grundlagen in Deutschland, in der Schweiz, in der Europäischen Union und den USA am Rande skizziert. Darüber hinaus wird der Begriff des internen Kontrollsystems erläutert.

In **Kapitel 3** werden die wesentlichen Standards für die Etablierung eines internen Kontrollsystems vorgestellt. Der Einsatz eines anerkannten Standards trägt durch einheitliche Vorgaben und Vorgehensweise zu hoher Akzeptanz des implementierten internen Kontrollsystems bei den Mitarbeitern, sowie bei den internen und externen Prüfern bei.



**Abbildung 1:** Inhaltsstruktur des Leitfadens.

In **Kapitel 4** werden einige wichtige Aspekte der Dokumentationsrichtlinie und empfohlene Methoden skizziert, die bei der Erstellung und Pflege der IKS-Dokumentation zu berücksichtigen sind. Eine vollständige und sachgerechte Dokumentation stellt die Basis einer erfolgreichen Umsetzung der Compliance dar und dient dem Nachweis der getroffenen organisatorischen und technischen Maßnahmen im Unternehmen. Sie dient als sehr effektives, organisationsweites Kommunikationsmedium bei der Bekanntmachung und Verbreitung der getroffenen Compliance-Maßnahmen für alle Mitarbeiter. Sie ist unab-

dingbar bei jeder Art von Audits, die durch interne bzw. externe Auditoren und Prüfer durchgeführt werden können. Eine Dokumentationsrichtlinie trägt signifikant zur Erhöhung der Qualität der IKS-Dokumentation in ihrem gesamten Lebenszyklus bei.

In **Kapitel 5** ist die systematische Vorgehensweise der Einführung, der Dokumentation und der Prüfung eines internen Kontrollsystems im Unternehmen beschrieben. Am Beispiel einer fiktiven Firma, der Wind Seeker AG, wird das gesamte IKS-Projekt in mehreren Meilensteinen erläutert. Die hier beschriebene Projektmethodik kann auch ohne die vorgestellte Compliance Management Lösung DocSetMinder® bei der Einführung eines internen Kontrollsystems angewendet werden.

In **Kapitel 6** werden die Einsatzbereiche und der Funktionsumfang der Compliance Management Software DocSetMinder® vorgestellt. DocSetMinder® unterstützt die Unternehmensleitung und das IKS-Projektteam bei der Konzeption, Umsetzung, Dokumentation, Prüfung und Fortführung eines wirksamen internen Kontrollsystems. Durch den modularen Aufbau kann DocSetMinder® bei weiteren Compliance-Themen effektiv und effizient im Unternehmen eingesetzt werden (vgl. [www.docsetminder.de](http://www.docsetminder.de)).