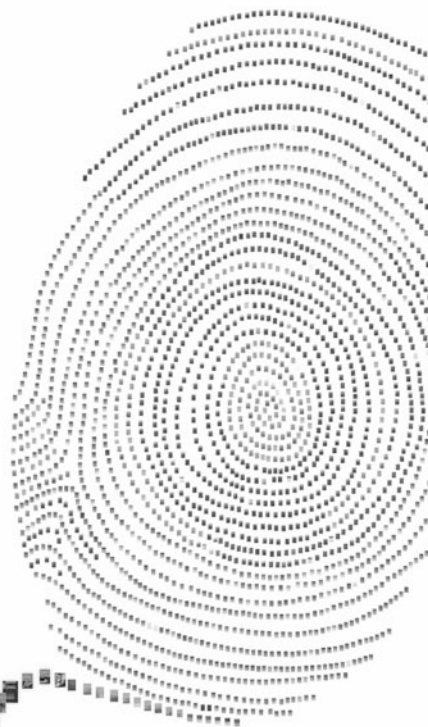

IT-Revision, IT-Audit und IT-Compliance

Lizenz zum Wissen.




Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf www.springerprofessional.de/buchaktion/



**Jetzt
30 Tage
testen!**

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

-  Zugriff auf tausende von Fachbüchern und Fachzeitschriften
-  Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
-  Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

 Springer

Aleksandra Sowa • Peter Duscha
Sebastian Schreiber

IT-Revision, IT-Audit und IT-Compliance

Neue Ansätze für die IT-Prüfung

Aleksandra Sowa
Bonn, Deutschland

Peter Duscha
Frankfurt, Deutschland

Sebastian Schreiber
Syss GmbH
Tübingen, Deutschland

ISBN 978-3-658-02807-7 ISBN 978-3-658-02808-4 (eBook)
DOI 10.1007/978-3-658-02808-4

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

Springer Vieweg

© Springer Fachmedien Wiesbaden 2015

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Fachmedien Wiesbaden GmbH ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Inhalt

1	Einleitung	1
1.1	Buchinhalte	3
1.2	Historisches	4
2	Audit, Continuous Audit, Monitoring und Revision	7
2.1	Allgemeine gesetzliche Grundlagen zur Internen Revision	8
2.2	3LoD: Three Lines of Defence	9
2.3	Rolle der Internen Revision	10
2.4	Monitoring	10
2.5	Exkurs: Jahresabschlussprüfung	12
2.6	Continuous Auditing	13
2.7	Audit	14
	Literatur	15
3	Methodik der IT-Prüfung	17
3.1	Ausgangslage	17
3.2	Standards für die Revision	18
3.2.1	IT-Prüfungsstandards und Richtlinien des ISACA	18
3.2.2	Internationale Standards für die Interne Revision des IIA	19
3.2.3	Gegenüberstellung relevanter Standards für IT-Revision	20
3.3	Prüfungsmanagement	22
3.3.1	Ablauf einer Prüfung	22
3.3.2	Projektmanagement	26
3.3.3	Prüfziele	28
3.3.4	Beauftragung und Planung einer Prüfung (Phase 1)	30
3.3.5	Durchführung der Prüfung (Phase 2)	36
3.3.6	Berichtschreibung (Phase 3)	40
3.3.7	Nachschau (Phase 4)	44

3.4	Hypothesenbasiertes Prüfen	45
3.4.1	Prüferfehler	46
3.4.2	Hypothesen	47
3.5	Tests	50
3.5.1	Erwartungen	51
3.5.2	Testformen	54
3.5.3	Annahme oder Ablehnung von Hypothesen	69
3.6	Kommunikation in der Prüfung	70
3.6.1	Ziele der Kommunikation	71
3.6.2	Prüferkommunikation und Vertrauen	73
3.6.3	Kommunikationssituationen in einer Prüfung	75
3.7	Prüfungsdokumentation	81
3.7.1	Anforderungen	81
3.7.2	Dokumentation der Arbeit	90
3.7.3	Dokumentation der Ergebnisse	92
3.7.4	Aufbewahrung der Dokumentation	94
4	Datenschutzaudit gemäß § 9 und Anlage zu § 9 BDSG	95
4.1	Ausgangslage	96
4.2	Datenschutzaudit: Begriffsabgrenzung	96
4.3	Risikoorientierter Prüfungsansatz	97
4.4	Prüfungskontext	99
4.4.1	Datenschutzkontrollen im Kontext der Informationssicherheit	100
4.4.2	Eingrenzung des Prüfungsuniversums	104
4.5	Datenschutzrisiken identifizieren	105
4.6	Datenschutzrisiken analysieren	106
4.7	Datenschutzrisiken evaluieren	107
4.8	Datenschutzrisiken managen	107
4.8.1	Verhältnismäßigkeit und Erforderlichkeit der Kontrollen	108
4.9	Methodische Ansätze des Datenschutzaudits	108
4.10	Fazit	110
	Literatur	111
5	Prüfung kartellrechtlicher Compliance durch Mock Dawn Raids als Prüfungsmethode der IT-Revision	113
5.1	Ausgangslage	113
5.2	Dawn Raid – Hintergründe und Ablauf	114
5.2.1	Hintergründe und Grundlagen	115
5.2.2	Typischer Ablauf einer Dawn Raid	116
5.2.3	Rolle der IT-Revision während einer Dawn Raid	116
5.3	Mock Dawn Raid – oder „Übung macht den Meister“	118
5.3.1	Hintergründe und Ziele der Prüfung	118
5.3.2	Mock Dawn Raid als Prüfungsmethode	119
5.3.3	Ablauf einer Mock Dawn Raid	120
5.4	Rolle der IT-Revision bei einer Mock Dawn Raid	125

5.5	Risiken einer Mock Dawn Raid	126
5.5.1	Strafrechliche Risiken für Mitarbeiter der Internen Revision/externe Kanzleien	126
5.5.2	Mögliche Strafbarkeit der Unternehmensführung	127
5.6	Fazit	128
	Literatur	128
6	IT-Revision bei Betrugsaufdeckung und Investigation	131
6.1	Ausgangslage	131
6.2	Betrug und IT-gestützte Unternehmensprozesse	132
6.3	Relevante Prüfungsarten	134
6.3.1	Betrugsaufdeckung im Rahmen einer Jahresabschlussprüfung	134
6.3.2	Unterschlagungsprüfungen	135
6.3.3	Vergleich JA-Prüfung versus Unterschlagungsprüfung	136
6.3.4	Instrumente einer forensischen Prüfung	136
6.4	IT-forensische Untersuchungen	137
6.4.1	Ziel einer forensischen Untersuchung	139
6.4.2	Cybercrime im Transaktionsumfeld	139
6.4.3	Schritte einer forensischen Untersuchung (Best Practices)	140
6.5	Ausgewählte forensische Techniken	141
6.5.1	Kennzahlenanalyse nach dem Benfordschen Gesetz	142
6.6	Fazit	149
	Literatur	149
7	Der Penetrationstest als Instrument der Internen Revision	151
7.1	Ausgangslage	151
7.2	Der Penetrationstest: Einsatz und Definition einer Qualitätssicherungsmaßnahme	154
7.3	Penetrationstests als Bestandteil von Revisionsprüfungen	156
7.4	Konkrete Gestaltungsmöglichkeiten eines Penetrationstests	160
7.4.1	Klassische Vorgehensweise	160
7.4.2	Typische standardisierte Penetrationstests	163
7.4.3	Planung von Penetrationstestserien mittels mehrperiodiger Prüfpläne	167
7.4.4	Budget	174
7.4.5	Risikosteuerung des Penetrationstests	175
7.4.6	Abschlussbericht und Nachtests	177
7.5	Vergabe von Penetrationstests	178
7.6	Fazit	180
	Literatur	183
8	Data Mining und Data Matching versus Datenschutz	185
8.1	Ausgangslage	185
8.2	Auswertung von Mitarbeiterdaten bei Korruptionsbekämpfung und -prävention	187
8.2.1	Anwendungsbereich des § 32 BDSG	188
8.2.2	Ausnahmen	189

8.3	Data Mining zur Verhinderung und Aufdeckung von Straftaten	190
8.3.1	Verhinderung von Straftaten und präventive Kontrollen	191
8.3.2	Aufdeckung und Verfolgung von Straftaten beim konkreten Tatverdacht	192
8.3.3	Weitere Begrifflichkeiten und Definitionen	196
8.3.4	Data Mining unter Verwendung anonymisierter oder pseudonymisierter Daten	198
8.3.5	Exkurs: Aufdeckung von Betrug und/oder Manipulationen in Transaktionszahlen	199
8.4	Datenschutzrechtliche Aspekte des Data Mining und Data Matching im Internet	200
8.4.1	Data Mining im Internet und in sozialen Netzwerken – aktuelle Diskussion	200
8.5	Fazit	202
	Literatur	203
9	Schlusswort	205