

Inhaltsverzeichnis

Vorwort.....	7
Inhaltsverzeichnis	9
Abkürzungsverzeichnis.....	13
Abbildungsverzeichnis	19
Kapitel 1: Einführung	21
1.1 Ursprung und Ziele von (IT)-Compliance	21
1.2 Governance.....	25
1.3 IT-Governance.....	28
1.4 Data Governance	31
1.5 Governance-Risk-Compliance (GRC)	32
1.6 Interdisziplinarität der IT-Compliance.....	32
1.7 Zusammenfassende Kapitelübersicht.....	35
Kapitel 2: Wirkungsmodell der IT-Sicherheit.....	37
2.1 Entwicklung der Computersicherheit und Wirkungsmodell der IT-Sicherheit.....	37
2.2 Allgemeines GRC-Wirkungsmodell und Anwendungsbeispiele.....	45
2.3 Pflichtschutzmaßnahmen als regulatorische Anforderungen der IT-Compliance.....	50
2.4 IT-Sicherheit als volkswirtschaftliche Aufgabe.....	52
2.5 Fazit zum Thema IT-Compliance als Pflichtschutzmaßnahme im GRC-Wirkungsmodell	54
Kapitel 3: Treiber von IT-Compliance	55
3.1 Überblick	55
3.2 Treiber der IT-Compliance im Detail.....	56
3.3 Fazit zum Thema Treiber der IT-Compliance.....	66
Kapitel 4: Rechtlicher Rahmen der IT-Compliance	67
4.1 Regulatorische Anforderungen an IT-Compliance	67
4.2 Normenhierarchie und Gültigkeit regulatorischer Anforderungen..	72
4.3 Regulatorische Institutionen der IT-Compliance und deren Ziele...	73
4.4 Diskussion der absoluten oder relativen Zielvorgaben für Pflichtschutzmaßnahmen der IT-Compliance.....	82
4.5 Fazit zum rechtlichen Rahmen der IT-Compliance	86

Kapitel 5: IT-Compliance unter Einsatz von CobiT.....	87
5.1 ISACA, ITGI und CobiT.....	87
5.2 Das CobiT-Referenzmodell im Detail.....	89
Kapitel 6: Kosten der IT-Compliance	97
6.1 Grundsätzliche Überlegungen zur Wirtschaftlichkeit von IT-Compliance.....	97
6.2 Anzahl der Anforderungen und Kostenwirkungen in der Praxis.....	100
6.3 Rentabilitätsanalyse.....	103
6.4 Fazit zur Wirtschaftlichkeits- und Nutzenbetrachtung der IT-Compliance.....	115
Kapitel 7: Management von IT-Compliance	117
7.1 Einleitung zum Management der IT-Compliance	117
7.2 IT-Compliance-Organisation (Aufbau- und Ablauforganisation) ...	121
7.3 Weitere Elemente der IT-Compliance-Organisation	126
Kapitel 8: Der IT-Compliance-Prozess	135
8.1 Gesamtprozess IT-Compliance	135
8.2 Identifikation und Analyse von regulatorischen Anforderungen	136
8.3 Zuordnung und Behebung von Kontrollschwächen	141
8.4 Berichterstattung über Compliance.....	142
8.5 Vorgehensmodell Initialprojekt IT-Compliance	146
Kapitel 9: Werkzeuge des (IT)-Compliance-Managements.....	155
9.1 Einsatz unternehmensübergreifender Standards	155
9.2 Compliance-Management-Software.....	162
9.3 Benchmarking des IT-Compliance-Management	181
9.4 Ergebnisse aus den Benchmarkstudien der IT Policy Compliance Group.....	185
Kapitel 10: Wesentliche Maßnahmen der IT-Compliance.....	191
10.1 Managementansatz auf der Basis der wesentlichen Maßnahmen....	191
10.2 Maßnahmen der IT-Compliance auf Basis der Motivatoren für IT-Sicherheit aus Unternehmenssicht	192
10.3 Maßnahmen der IT-Compliance auf Basis des Unified Compliance Framework (UCF).....	193
10.4 Beschreibung der wesentlichsten IT-Sicherheitsmaßnahmen bzw. IT-Compliance-Anforderungen.....	198
10.5 IT-Sicherheit nach BSI-Leitfaden zur IT-Sicherheit	202
10.6 Fazit zum Bereich der wesentlichen Maßnahmen der IT-Compliance.....	205
Kapitel 11: Outsourcing und IT-Compliance	207
11.1 IT-Outsourcing als gesamtwirtschaftliches Risiko?	207
11.2 Reifegrad der IT und Auslagerungsfähigkeit.....	210

Inhaltsverzeichnis

1.3	Umfang der Abhängigkeit vom Auslagerungsunternehmen und Maßnahmen zur Reduzierung	212
1.4	Nachweise der IT-Compliance bei Outsourcing	215
1.5	Berichtstypen von SAS 70/ ISA 402-basierten Compliance-Nachweisen bei Outsourcing.....	219
1.6	Diskussion zum Thema Nachweis der IT-Compliance bei Outsourcing	221
1.7	Fazit zum Thema Outsourcing und IT-Compliance.....	222
Kapitel 12: Schlussbetrachtung und Ausblick.....		223
Anhang.....		225
/1	Linkliste zu IT-Compliance	225
/2	Übersicht IT-Compliance-Anforderungen des UCF.....	227
/3	Übersicht Compliance-Software	239
/4	Übersicht der Entwicklung von Gesetzen und Richtlinien für automatisierte Anlagen im Gesundheitsbereich.....	248
Quellenverzeichnis		251
Literaturverzeichnis.....		251
Verzeichnis der verwendeten Gesetze, Verordnungen und Entscheidungen		255
Verzeichnis der Internetquellen		256
Fachwortverzeichnis.....		265
Autorenportraits		267