

Inhaltsverzeichnis

Abbildungsverzeichnis.....	XIII
Tabellenverzeichnis.....	XV
Abkürzungsverzeichnis	XVII
1 Einleitung	1
1.1 Motivation: Compliance als Herausforderung für das IT-Management	1
1.2 Untersuchungsbereich, Untersuchungsobjekt und Ziele der Arbeit.....	14
1.3 Wissenschaftliche Methodik und Aufbau der Untersuchung.....	16
2 Governance und Compliance – Begriff und Bezugsrahmen	27
2.1 Systematisierung.....	27
2.2 Corporate Governance und Corporate Compliance.....	28
2.3 IT-Governance und IT-Compliance	35
2.4 Anspruchsgruppen der IT-Compliance.....	37
2.5 Rahmenbedingungen für IT-Compliance	40
2.6 Standards und Frameworks als Lösungsansätze für IT-Compliance.....	43
3 Anforderungen an ein Control-Framework für IT-Compliance.....	47
3.1 Systematisierung der Anforderungsanalyse	47
3.2 Eigenkapitalgeber und Prüfer	49
3.2.1 Zur Systematik der Anforderungen von Eigenkapitalgebern und Prüfern.....	49
3.2.2 Unternehmensweites IKS zur Risikosteuerung für Eigenkapitalgeber ..	50
3.2.3 Wirtschaftsprüfer als Erfüllungsgehilfen der Eigenkapitalgeber	54
3.2.4 Prüfung des internen Kontrollsystems und Abschlussprüfung bei IT-Einsatz.....	58
3.2.5 Grundsätze ordnungsmäßiger Buchführung und IT-gestützte Buchführungssysteme	68
3.2.6 Prüfung von Dienstleistern und Zertifizierung von Teilbereichen	70

3.3 Unternehmensleitung	72
3.3.1 Zur Systematik der Anforderungen der Unternehmensleitung	72
3.3.2 Enthaftung als Ziel des Compliance-Managements	74
3.3.3 Absicherung gegen Haftungsrisiken durch D&O-Versicherungen	76
3.3.4 Verantwortung und Delegation	80
3.3.5 Buchführungspflicht und IT-gestützte Rechnungslegung	83
3.3.6 Wirtschaftlichkeit der Maßnahmen	86
3.4 IT-Management	92
3.4.1 Zur Systematik der Anforderungen des IT-Managements	92
3.4.2 Die „klassische“ Sicht der IT-Sicherheit	93
3.4.3 Compliance und Alignment als Ziele des IT-Management	94
3.5 Weitere Anspruchsgruppen	102
3.5.1 Zur Systematik der Anforderungen der weiteren Anspruchsgruppen ..	102
3.5.2 Betriebliche Mitbestimmung und Persönlichkeitsrechte der Mitarbeiter	103
3.5.3 Outsourcing als Risikofaktor im Rahmen der IT-Compliance	106
3.5.4 Persönlichkeitsrechte von Kunden	107
3.6 Zusammenfassung der Anforderungen	109
4 Aufbau eines Control-Frameworks für IT-Compliance	115
4.1 Einleitung und Kapitelüberblick	115
4.2 Dimensionen von IT-Compliance-Controls	117
4.2.1 Risikoorientierter Aufbau von IT-Compliance-Controls	117
4.2.2 Operationalisierung und Konkretisierung	120
4.2.3 Organisatorische Einbettung der IT-Compliance	122
4.2.4 Nachweisbarkeit, Dokumentation und Transparenz	126
4.2.5 Dimensionen der IT-Compliance-Controls	128
4.3 Systematisierung der fachlich-inhaltlichen Ausgestaltung des IT-Compliance-Frameworks	130
4.3.1 Methodik der Integration	130
4.3.2 Auswahl der Ausgangs-Frameworks	134
4.3.3 Konsolidierung der Domänen der ausgewählten Frameworks	142

5 Ableitung des Control-Frameworks für IT-Compliance.....	149
5.1 Systematisierung der Ableitung des IT-Compliance-Frameworks	149
5.2 Mapping der Inhalte aus CobiT, ISO 27001 und ISO 20000-1	151
5.3 Operative Aufgabenverteilung im IT-Compliance-Framework	192
5.4 Control Framework für IT-Compliance.....	197
5.4.1 Strategy & Planning.....	197
5.4.2 Organization.....	207
5.4.3 Risk	226
5.4.4 Security	236
5.5 Fazit zur Ableitung und den Inhalten des IT-Compliance-Frameworks	246
6 Schlussbetrachtung und Ausblick.....	247
6.1 Zusammenfassung der Untersuchungsergebnisse	247
6.2 Kritische Reflektion und weiterer Forschungsbedarf.....	252
Literaturverzeichnis	255