

Sarbanes-Oxley und Corporate Compliance

Nachhaltigkeit, Optimierung, Integration

Bearbeitet von
Christof Menzies

1. Auflage 2009 2006. Buch. XXIV, 506 S. Hardcover

ISBN 978 3 7910 2490 5

Format (B x L): 17 x 24 cm

Gewicht: 1103 g

Wirtschaft > Unternehmensfinanzen > Controlling, Wirtschaftsprüfung, Revision

Zu Leseprobe

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of increasing size. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, red, all-caps, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Inhaltsverzeichnis

Preface	V
Vorwort	VII
Abkürzungsverzeichnis	XVII
Einleitung	IXX

I Corporate Compliance in einem dynamischen Umfeld	1
1 Der Compliance-Begriff	2
2 Bedeutende globale Regeln und Standards	9
2.1 OECD Principles of Corporate Governance	9
2.2 Industriespezifische Regeln und Standards	11
2.3 Neugestaltung von Eigenkapitalvorschriften für Kreditinstitute (Basel II)	12
3 Der Sarbanes-Oxley Act und der Foreign Corrupt Practices Act als Beispiele wesentlicher Bestimmungen für US-börsennotierte Unternehmen	15
3.1 Der Sarbanes-Oxley Act – Auswirkungen und aktuelle Entwicklungen	15
3.1.1 Auswirkungen des Sarbanes-Oxley Act	16
3.1.2 Compliance-Zeitpunkte für die Umsetzung der Section 404	17
3.1.3 Weiterentwicklung von Prüfungsstandards durch das Public Company Accounting Oversight Board	19
3.1.4 Committee of Sponsoring Organizations of the Treadway Commission	22
3.1.5 Weitere Strategie der Securities and Exchange Commission	23
3.2 Der Foreign Corrupt Practices Act – Bedeutung und Auswirkungen für Unternehmen	24
3.2.1 Ursprung und Entwicklung	25
3.2.2 Anti-Korruptionsvorschriften	26
3.2.3 Rechnungslegungs- und Buchführungsvorschriften	28
3.2.4 Verletzungen des FCPA durch Unternehmen	29
3.2.5 Ausblick auf die zukünftige Entwicklung	30
4 Listing-Standards ausgewählter Börsen	31
4.1 Corporate-Governance-Standards der New York Stock Exchange	31
4.2 Corporate-Governance-Standards der London Stock Exchange	32
4.3 Frankfurter Wertpapierbörse	33
5 Entwicklungen in Europa	35
5.1 Umsetzung des EU-Aktionsplans »A modern legal framework for company law and governance in Europe«	35
5.2 Europäisches Corporate-Governance-Forum	36
5.3 Wesentliche Richtlinien und Empfehlungen der EU	36
5.3.1 Stärkung von Abschlussprüfer und Audit Committees durch die 8. EU-Richtlinie (Abschlussprüferrichtlinie)	36

5.3.2	Empfehlungen der Kommission zu den Aufgaben der nicht geschäftsführenden Direktoren/Aufsichtsratsmitglieder sowie zu den Ausschüssen des Verwaltungs- bzw. Aufsichtsrats	39
5.3.3	Moderne Rechnungslegungsstandards in der EU	39
5.3.4	Harmonisierung von Anforderungen an Prospekte	41
5.3.5	Kontrolle durch mehr Transparenz	42
5.3.6	Vereinfachung und Modernisierung der Zweiten Gesellschaftsrechtsrichtlinie über die Erhaltung und Änderung des Kapitals von Aktiengesellschaften.	43
5.3.7	Einheitliche europäische Rechtsform für Kapitalgesellschaften	44
5.3.8	Verschmelzungen von Kapitalgesellschaften innerhalb der Europäischen Union	45
5.3.9	Übernahmerichtlinie	45
5.3.10	Änderung der Bilanzrichtlinien	46
5.3.11	Richtlinienvorschlag zur Stärkung der Aktionärsrechte	47
6	Die Transformation von EU-Anforderungen in das Regelwerk eines Mitgliedstaats am Beispiel Deutschlands	49
6.1	Das Bilanzkontrollgesetz.	49
6.2	Das Bilanzrechtsreformgesetz	50
6.3	Das Anlegerschutzverbesserungsgesetz	52
6.4	Das Kapitalanleger-Musterverfahrensgesetz	53
6.5	Offenlegung der Vorstandsvergütungen	54
6.6	Haftung versus Business Judgement Rule	55
6.7	Strengere Haftung für falsche Kapitalmarktinformationen.	57
6.8	Gesetz zur Einführung der Europäischen Gesellschaft	57
6.9	Elektronisches Unternehmensregister.	58
6.10	Umsetzung des Deutschen Corporate Governance Kodex in der Unternehmenspraxis.	59
7	Zusammenfassung und Ausblick	62
II	Das GRC-Stufenmodell – Nachhaltigkeit, Optimierung und Integration von Governance, Risikomanagement und Compliance	63
1	Corporate Compliance stufenweise erreichen	63
1.1	Das GRC-Stufenmodell	65
1.1.1	Compliance (Stufe 1)	67
1.1.2	Transformation und Optimierung (Stufe 2)	69
1.1.3	Compliance-Driven Optimization (stufenübergreifend)	71
1.1.4	Integration und Optimierung (Stufe 3).	73
1.2	Bedeutung der Strukturmerkmale im Stufenmodell	76
2	Compliance am Beispiel von Section 404 des Sarbanes-Oxley Act	78
2.1	Wesentliche Erfahrungen aus SOA-404-Projekten	79
2.1.1	Erfahrungen nach Projektphasen.	80
2.1.1.1	Projektorganisation/Projektmanagement festlegen	81
2.1.1.2	Scope festlegen	88
2.1.1.3	Prozesse und Kontrollen dokumentieren und bewerten	90
2.1.1.4	Wirksamkeit des internen Kontrollsystems testen	94
2.1.1.5	Kontrollschwächen beheben.	97

2.1.1.6	Sign-off und Managementberichterstattung durchführen . .	100
2.1.2	Veröffentlichte Material Weaknesses: Erste Erfahrungen	102
2.1.3	Ausgewählte Aspekte bei der Umsetzung des Sarbanes-Oxley Act in der Informationstechnologie	104
2.1.4	Erfüllung der SOA-404-Anforderungen im Steuerbereich	111
2.1.5	SAS 70 – Erfahrungen, Trends und Entwicklungen	114
2.1.6	Nutzen und Nutzenpotentiale von Section 404 aus Sicht der Unternehmen	117
2.2	Auswirkungen des Sarbanes-Oxley Act auf das Investorenverhalten – Analyse empirischer Befunde	121
2.2.1	Einleitung	121
2.2.2	Aufwendungen für die Umsetzung des SOA	122
2.2.3	Auswirkungen auf das Investorenverhalten	124
2.2.3.1	Verabschiedung des SOA	124
2.2.3.2	Zertifizierung durch CEO und CFO	126
2.2.3.3	Delisting	127
2.2.3.4	Material Weaknesses	128
2.2.4	Zusammenfassung und Ausblick	129
2.3	Umfrage von PricewaterhouseCoopers zu »Sarbanes-Oxley/ Internal Control Compliance« in Deutschland	133
2.3.1	Aufbau der Befragung	133
2.3.2	Zusammenfassung der Ergebnisse	135
2.4	Zusammenfassung und Ausblick	137
3	Compliance Sustainability – der Weg zu nachhaltiger Compliance	139
3.1	Umsetzungsmethodik zum Erreichen der Nachhaltigkeit	144
3.1.1	Analysephase	146
3.1.2	Designphase	146
3.1.3	Gestaltungsphase	147
3.1.4	Umsetzungsphase	147
3.1.5	Durchführungsphase	147
3.2	Change Management	150
3.3	Compliance-Sustainability-Elemente	154
3.3.1	Compliance-Aufbauorganisation	156
3.3.2	Compliance-Rahmenwerk	163
3.3.3	Kommunikationsprozesse	167
3.3.4	Trainings- und Personalentwicklungsprogramme	171
3.3.5	Scoping- und Risikobewertungsprozess	176
3.3.6	Überwachung und Sicherung des Compliance-Status (Compliance Controlling)	179
3.3.7	Remediation-Prozess: Vorgehensweise zum Umgang mit Abweichungen von Compliance-Anforderungen	185
3.3.8	Compliance-Dokumentationsprozesse	189
3.3.9	Technologieunterstützung	193
3.4	Exkurs: SOA-/Compliance Tools zur Unterstützung der Anforderungen des SOA und deren Einführung	201
3.4.1	Ausgewählte SOA-/Compliance Tools	201
3.4.1.1	SAP – Management of Internal Controls	202
3.4.1.2	IDS-Scheer – ARIS Compliance Management Solution	204
3.4.1.3	Paisley Consulting – Risk Navigator	206

3.4.1.4	OpenPages – FCM (Financial Controls Management) . . .	207
3.4.1.5	Microsoft Office Solution for Sarbanes-Oxley	210
3.4.2	Auswahl einer geeigneten Software zur Unterstützung der Erfüllung des Sarbanes-Oxley Act	212
3.4.3	Umsetzung mittels SOA Tool Implementation Methodology	213
3.5	Zusammenfassung und Ausblick.	217
4	Compliance-Driven Optimization	218
4.1	Nutzenorientierte Umsetzungsmethodik für Compliance-Driven Optimization	221
4.2	Analysephase im CDO-Modell.	224
4.2.1	Voranalyse	226
4.2.1.1	Qualitative Aspekte der Voranalyse	227
4.2.1.1.1	Analyse der Company-Level Controls.	228
4.2.1.1.2	Analyse von erkannten, aber nicht behobenen Schwachstellen	231
4.2.1.1.3	Analyse von Quick Fixes.	231
4.2.1.2	Quantitative Verfahren der Voranalyse	232
4.2.1.2.1	Ermittlung der relativen Häufigkeit von Schwachstellen	234
4.2.1.2.2	Ermittlung des Grads der Prozessheterogenität.	237
4.2.1.2.3	Auswerten und Plausibilisieren der Ergebnisse.	240
4.2.1.2.4	Auswertung von externen Informationen (externes Benchmarking)	242
4.2.2	Detailanalyse	245
4.2.2.1	Quantitative Verfahren der Detailanalyse	248
4.2.2.1.1	Internes Benchmarking (Prozesse).	248
4.2.2.1.2	Portfolioanalyse (Kontrollen).	255
4.2.2.2	Qualitative Verfahren der Detailanalyse	263
4.2.2.3	Zusammenführen der Ergebnisse.	264
4.2.3	Aufwand-Nutzen-Analyse (Business Case).	265
4.3	Designphase im CDO-Modell	267
4.3.1	Definition des Soll-Zustands	268
4.3.1.1	Design der Geschäftsprozesse	270
4.3.1.2	Design der internen Kontrollen	272
4.3.1.2.1	Reduzierung oder Eliminierung von Kontrollen	273
4.3.1.2.2	Erhöhung des Automatisierungsgrads von Kontrollen	273
4.3.1.2.3	Standardisierung und Zentralisierung von Kontrollen	275
4.3.1.2.4	Reduzierung der Key Controls	275
4.3.1.2.5	IT-gestützte Control-Evidence-Verwaltung	277
4.3.1.2.6	Automatisiertes Testen der Kontrollfunktion.	278
4.3.1.3	Definition von Anforderungen an Systeme und Technologien	278
4.3.1.4	Design der Organisationsstruktur.	279
4.3.1.5	Konzeption von Verfahrensanweisungen und Richtlinien	280
4.3.2	Entwicklung einer Implementierungsstrategie	281
4.3.2.1	Entwicklung eines Implementierungsansatzes	281
4.3.2.2	Definition des Implementierungsvorgehens	283
4.3.3	Entwicklung einer Schulungsstrategie	285
4.4	Gestaltungsphase im CDO-Modell	286

4.4.1	Vervollständigung der strukturellen Ausprägungen des Soll-Modells	287
4.4.2	Entwicklung von Implementierungsplänen.	290
4.5	Umsetzungsphase im CDO-Modell.	291
4.5.1	Implementierung der Veränderungen.	292
4.5.2	Messung der Zielerreichung im Rahmen des Benefits Managements.	294
4.5.3	Kontinuierliche Verbesserung im Rahmen des Benefits Managements.	299
4.5.3.1	Kontinuierliche Verbesserung zur weiteren Steigerung des Optimierungsgrads.	299
4.5.3.2	Der kontinuierliche Verbesserungsprozess.	300
4.5.3.2.1	Kontinuierliche Verbesserung durch Analyse der Performance-Indikatoren	301
4.5.3.2.2	Kontinuierliche Verbesserung durch Integration der Mitarbeiter	301
4.5.3.2.3	Kontinuierliche Verbesserung durch eine integrierte Organisationsstruktur	302
4.5.3.2.4	Kontinuierliche Verbesserung durch integrierte Reportingstrukturen	303
4.6	Sonderbeiträge zum Thema Optimierung im Compliance-Umfeld	303
4.6.1	Optimierung durch Zentralisierung und Auslagerung	304
4.6.1.1	Organisatorische Ausprägungen von Prozessen	305
4.6.1.2	Organisation der Dienstleistung	311
4.6.1.3	Instrumente zur Kontrollerreichung	313
4.6.1.4	Zusammenfassung und Ausblick	315
4.6.2	Compliance-gerechtes Management von IT-gestützten Geschäftsprozessen (Mercury)	316
4.6.3	Bewältigung der Funktionstrennung (Segregation of Duties) durch Automatisierung und Prävention: Ein nachhaltiger Ansatz zur Sarbanes-Oxley Compliance (SAP GRC Business Unit)	319
4.7	Exkurs: Konsequente Ausrichtung von Accounting und Reporting an Effektivität und Effizienz.	324
4.8	Zusammenfassung und Ausblick.	331
5	Die Integration von Governance, Risikomanagement und Compliance	332
5.1	Das GRC-Zielmodell	334
5.1.1	Corporate Governance	336
5.1.1.1	Definition und Nutzen von Corporate Governance	337
5.1.1.2	Komponenten einer effektiven Corporate Governance	339
5.1.2	Risikomanagement	343
5.1.2.1	Definition und Nutzen von Risikomanagement	343
5.1.2.2	COSO II – Komponenten eines effektiven Risikomanagements	345
5.1.3	Compliance	349
5.1.3.1	Definition und Nutzen von Compliance	350
5.1.3.2	Rule-Based Compliance Management	351
5.2	Die GRC-Umsetzungsmethodik	353
5.2.1	Analysephase	357
5.2.1.1	Projektstart und Stakeholder-Analyse	358

5.2.1.2	Erstellung und Pflege der unternehmensspezifischen Corporate Rule Base	362
5.2.1.3	Aufnahme des unternehmensweiten GRC-Umfelds	366
5.2.1.4	Identifizierung von GRC-Potentialen	376
5.2.1.5	Benefits, Projekt- und Change Management	377
5.2.2	Designphase	382
5.2.2.1	Entwicklung des unternehmensspezifischen GRC-Zielmodells	383
5.2.2.2	Entwicklung von Implementierungsstrategien	396
5.2.2.3	Trainings- und Schulungsmaßnahmen	399
5.2.3	Gestaltungsphase	402
5.2.3.1	Entwicklung von GRC-bezogenen Komponenten der Organisation und Prozesse	402
5.2.3.2	Entwicklung von GRC-bezogenen Systemen und Technologien	408
5.2.4	Umsetzung und Kontinuität	410
5.3	GRC Operating Model für den Regelbetrieb	411
5.3.1	Strategie, Organisation und Management	413
5.3.2	Monitoring und Reporting	416
5.3.3	Operations und kontinuierliche Verbesserung	418
5.4	Zusammenfassung und Ausblick	420
III Praxisberichte		425
1	Übergang von der SOX-Projektorganisation zur dauerhaften Linienverantwortung bei der Bayer AG	425
1.1	Ausgangssituation	425
1.1.1	Group ICS-Management	426
1.1.2	Subgroup ICS-Manager	427
1.1.3	Die Rolle des ICS-Managers	427
1.1.3.1	Die Einordnung des ICS-Managers in der lokalen Organisation	428
1.1.3.2	Aufgaben und Verantwortung des ICS-Managers	428
1.1.3.3	Ausbildung des ICS-Managers	429
1.2	Erfahrungen mit der neuen Organisation	430
2	Deutsche Telekom: Von einem konzernweiten S-OX404-Projekt zur Compliance-Organisation	432
2.1	Vorwort	432
2.2	Stand und Umsetzung der S-OX404-Anforderungen bei der Deutschen Telekom	432
2.3	Kritische Erfolgsfaktoren der Implementierungsphase	433
2.3.1	Projekt- und Prozessmanagement	433
2.3.2	Schaffung der einheitlichen methodischen Rahmenbedingungen	434
2.3.3	Konsequente Umsetzung eines Top-down-Vorgehens	435
2.3.4	Das Konzept des Control Self Assessments	436
2.3.5	Interaktion in der konzernweiten Beurteilung und Behebung von Kontrollschwächen	437
2.3.6	Qualitätsüberwachung durch die Interne Revision	438

2.3.7	Abbildung von Leistungsbeziehungen	438
2.3.8	Einführung des konzernweiten S-OX404-IT-Tools	439
2.4	Reduzierung des Compliance-Aufwands	439
2.5	Integration der konzernweiten Compliance-Aktivitäten.	440
2.6	Schlusswort	441
3	Umsetzung der Anforderungen hinsichtlich »rechnungsrelevanter Aussagen« bei E.ON	442
3.1	Bedeutung von »rechnungslegungsrelevanten Aussagen« im Rahmen von Section 404 des SOA	442
3.2	Herausforderungen für das SOA-Readiness-Projekt	442
3.3	Verknüpfung von Kontrollen mit rechnungslegungsrelevanten Aussagen	443
3.3.1	Zentrale Verknüpfung	443
3.3.2	Dezentrale Verknüpfung	444
3.4	Praktische Umsetzungsprobleme	445
3.5	Maßnahmen zur Verbesserung der Dokumentationsqualität	445
3.5.1	Änderung im Projektvorgehen.	446
3.5.2	Zentrale fachliche Anleitung	446
3.5.3	Änderungen in SAP MIC.	447
3.6	Erfahrungen mit dem geänderten Projektansatz.	448
3.7	Zusammenfassung und Ausblick.	448
4	Vom Projekt zum Prozess am Beispiel der SAP AG – Nachhaltigkeit und Mehrwert der unternehmensinternen SOX-Compliance Anstrengungen sichern	450
4.1	Zwischen Projekt und Prozess – Statusbericht zu »MIC@SAP«.	450
4.1.1	Stand des Projektes zum 31.12.2005	451
4.1.2	Vorbereitungen zur Überführung in langfristige Organisationsstrukturen	451
4.2	Erste Schritte über die SOX-Compliance hinaus	452
4.2.1	Einbindung von »MIC@SAP« in SAP's Global Risk Management Framework.	453
4.2.2	Ausblick: Integration der Complianceinitiativen der SAP zu einem ganzheitlichen Corporate Governance / Compliance Framework	458
5	Compliance bei Non-SEC-Unternehmen am Beispiel der Schweizerische Bundesbahnen SBB	461
5.1	Intro	461
5.2	Facts and Figures	461
5.3	Ausgangslage	461
5.3.1	Auslöser.	461
5.3.2	Projektauftrag und -ziel	462
5.3.3	Rahmenbedingungen	463
5.4	Ansatz SOX-light	463
5.4.1	Grundsätze.	463
5.4.2	Methodik	463
5.4.2.1	Ansatz	463
5.4.2.2	Projektvorgehen.	464
5.4.3	Projektorganisation.	465
5.4.3.1	Projektteam.	465

5.4.3.2	Einbindung des Wirtschaftsprüfers	465
5.4.3.3	Projektaufwand	465
5.5	Umsetzung SOX-light	465
5.5.1	Scoping	466
5.5.2	Dokumentation.	466
5.5.2.1	Prozesse	466
5.5.2.2	Risiken	466
5.5.2.3	Key Controls	467
5.5.2.4	IT-Tool für die Dokumentation des IKS	468
5.5.3	Test und Maßnahmencontrolling	468
5.5.4	Sign-off	468
5.6	Lessons learned	468
5.7	Nutzen	469
5.8	Ausblick	469
5.9	Fazit	470
 IV Zusammenfassung und Ausblick		471
 Literaturverzeichnis		475
 Glossar		487
 Das Autorenteam		491
 Register		503