
Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XVII
Einleitung	1
I Regulatorisches Umfeld	7
1 Vertrauensverlust in die Kapitalmärkte durch Finanzskandale	7
2 Der Sarbanes-Oxley Act	13
2.1 Geltungsbereich des Gesetzes	13
2.2 Maßnahmen und Inhalt des Gesetzes	14
2.2.1 Abschnitt I: Public Company Accounting Oversight Board	15
2.2.2 Abschnitt II: Auditor Independence	16
2.2.3 Abschnitt III: Corporate Responsibility	18
2.2.4 Abschnitt IV: Enhanced Financial Disclosures	20
2.2.5 Abschnitte V bis XI	22
3 Final Rule zu internen Kontrollen der Finanzberichterstattung	23
4 Das Public Company Accounting Oversight Board	24
4.1 Organisation des PCAOB	24
4.2 Aufgabenbereiche des PCAOB	25
5 Gesetze und Initiativen in Europa	27
5.1 Bestrebungen auf EU-Ebene	27
5.1.1 Mitteilung zur Stärkung der Abschlussprüfung in der EU	27
5.1.2 Aktionsplan zur Modernisierung des Gesellschaftsrechts	28
5.2 Bestrebungen in Deutschland	29
5.2.1 Maßnahmenkatalog zur Stärkung der Unternehmensintegrität und des Anlegerschutzes	29
5.2.2 Gesetzesentwurf zur Stärkung der Rolle des Abschlussprüfers	32

5.2.3	Gesetzesentwurf zur Überwachung der Rechtmäßigkeit konkreter Unternehmensabschlüsse	33
5.3	Bestrebungen in Österreich und der Schweiz	34
6	Zusammenfassende Betrachtung des regulatorischen Umfelds	35
II	Auswirkungen auf das Unternehmen	37
1	Sarbanes-Oxley im Unternehmensfokus	37
2	Transparenz interner Kontrollen	38
2.1	Einrichtung von Disclosure Controls and Procedures	38
2.1.1	Definition und Anwendungsbereich	38
2.1.2	Pflicht zur eidesstattlichen Bestätigung von Berichten (Certification)	39
2.1.3	Ausgestaltung von Disclosure Controls and Procedures	42
2.1.4	Aufgaben eines Disclosure Committee	44
2.2	Einrichtung von Internal Control over Financial Reporting	45
2.2.1	Gesetzliche Anforderungen	45
2.2.2	Auswirkungen auf das Management	46
2.2.2.1	Bericht über das interne Kontrollsystem der Finanzberichterstattung	46
2.2.2.2	Identifizierung von internen Kontrollen der Finanzberichterstattung	47
2.2.2.3	Vorschriften zur Bewertung von internen Kontrollen der Finanzberichterstattung	48
2.3	Abgrenzungen zwischen Disclosure Controls and Procedures und Internal Control over Financial Reporting	49
3	Ethics & Corporate Governance	54
3.1	Das Audit Committee und die Stärkung von Corporate Governance	55
3.1.1	Entwicklung von Audit Committees	55
3.1.2	Anforderungen an das Audit Committee gemäß Sarbanes-Oxley Act	57
3.1.3	Mitglieder eines Audit Committees	59
3.1.3.1	Unabhängigkeit der Audit Committee-Mitglieder	59
3.1.3.2	Anforderungen an einen Financial Expert	60

3.1.4	Das Verhältnis zwischen Audit Committee und Wirtschaftsprüfer	60
3.1.4.1	Wahl und Vergütung der Wirtschafts- prüfer	61
3.1.4.2	Überwachung der Unabhängigkeit der Wirtschaftsprüfer	61
3.1.5	Zusammenfassende Betrachtung des Audit Committees	62
3.2	Code of Ethics	63
3.2.1	Gesetzliche Anforderungen	63
3.2.2	Auswirkungen auf das Management	64
3.3	Verhinderung und Aufdeckung von Fraud	64
3.3.1	Fraud im Rahmen des Sarbanes-Oxley Act	65
3.3.2	Kontrollen des Managements	66
3.3.3	Kontrollen des Audit Committees	66
3.3.4	Kontrollen des Abschlussprüfers	67
3.4	Whistleblower Protection – Informantenschutz	68
3.4.1	Einrichtung eines Incident Management-Systems	68
3.4.2	Richtlinien für den Umgang mit Fehlverhalten	70
4	Zusammenfassung der wichtigsten Auswirkungen	71
III	Das interne Kontrollsystem	73
1	Einleitung	73
2	Definition des internen Kontrollsystems (IKS)	74
2.1	Grundlegende Definition	74
2.2	COSO als Rahmenwerk für das interne Kontrollsystem	75
2.2.1	Zweck und Auftrag von COSO	76
2.2.2	Die Definition des IKS nach COSO	76
2.2.3	Komponenten des internen Kontrollsystems	78
2.2.4	COSO und die Finanzberichterstattung	81
2.2.5	Die praktische Bedeutung von COSO	81
2.3	Internal Controls nach internationalen und nationalen Prüfungsstandards	84
2.3.1	Die internationalen Prüfungsstandards (ISA)	85
2.3.2	Die deutschen Prüfungsstandards (PS)	87
3	Analyse und Bewertung der Effektivität des IKS	91
3.1	Definition der Effektivität des internen Kontroll- systems	91
3.1.1	Ziele interner Kontrollsysteme	92

3.1.1.1	Interne Kontrollen der Finanzberichterstattung (Financial Reporting)	92
3.1.1.2	Interne Kontrollen der Geschäftstätigkeit (Operations)	94
3.1.1.3	Interne Kontrollen zur Sicherstellung der Einhaltung von Gesetzen und Vorschriften (Compliance)	96
3.1.2	Bewertungskriterien für die Design- und Operating Effectiveness	97
3.1.2.1	Design Effectiveness	98
3.1.2.2	Operating Effectiveness	99
3.1.3	Effizienz des internen Kontrollsystems	100
3.2	Relevante Prüfungsstandards zur Beurteilung der Effektivität interner Kontrollen	100
3.2.1	Überprüfung der Effektivität des IKS nach Section 404 SOA und PCAOB	102
3.2.1.1	Die Vorgehensweise des Abschlussprüfers	102
3.2.1.2	Auswirkungen des PCAOB-Standards auf das Management	107
3.2.2	Prüfung und Beurteilung des IKS nach ISA 315	108
3.2.3	Prüfung und Beurteilung des IKS nach IDW PS 260	109
3.2.4	Prüfung und Beurteilung der IT-Kontrollen	112
4	Der Sarbanes-Oxley Act und Enterprise Risk Management	116
4.1	Interne Kontrollen und Enterprise Risk Management	116
4.2	Das ERM-Rahmenwerk (COSO II)	118
4.2.1	Das IKS nach COSO als Baustein für ERM	118
4.2.2	Ziele und Komponenten von ERM	119
4.3	ERM in der Praxis	122
4.3.1	Voraussetzungen für ERM	122
4.3.2	Prozesse und Schlüsselemente bei der Einführung von ERM	123
4.3.3	Aufbau von ERM-Kompetenzen	123
4.3.4	Erfolgsfaktoren für ERM	124
4.4	Vorteile von ERM	125
5	Zusammenfassung	126

IV	Methodik	127
1	Einleitung	127
2	Projektorganisation und Scope festlegen	131
2.1	Regulatorische Anforderungen verstehen	132
2.2	Projektziele und -struktur definieren	132
2.2.1	Projektziele	132
2.2.2	Projektstruktur	136
2.3	Projekt-Scope festlegen	142
2.3.1	Erstellung des Unternehmensüberblicks	144
2.3.2	Identifizierung der wesentlichen Elemente der Rechnungslegung und Zuordnung der Assertions	144
2.3.3	Festlegung des Abdeckungsgrads	146
2.3.4	Unternehmenseinheiten für den Projekt-Scope auswählen	147
2.3.5	Weitere Aspekte des Scopings auf Unternehmens- ebene	151
2.3.6	Identifizierung der Unternehmensprozesse	153
2.4	Vorgehensweise und Dokumentationsstandards festlegen	161
2.5	Projektplan und Ressourcen festlegen	167
2.6	Tool auswählen	170
2.7	Scope, Vorgehensweise und Projektplan kommunizieren	182
3	Prozess- und Kontrolldesign dokumentieren und bewerten . . .	183
3.1	Zentralen Organisations- und Prozesskatalog aufbauen	185
3.1.1	Organisations- und Prozessstruktur aufnehmen . . .	186
3.1.2	Risiken und Kontrollziele pro Prozess definieren. . .	190
3.1.3	Bilanz- und GuV-Positionen Prozessen zuordnen. .	192
3.1.4	Prozesse den Organisationseinheiten zuordnen. . . .	194
3.2	Tool und Methode einführen	196
3.2.1	Tool installieren und testen	196
3.2.2	Tool- und Methodenschulung konzipieren	201
3.2.3	Pilotprojekt vorbereiten und durchführen	204
3.2.4	Tool und Methoden-Roll-out	204
3.3	Dokumentation und Bewertung des internen Kontrollsystems	206
3.3.1	Aufnahme der übergeordneten COSO- Komponenten	207
3.3.2	Prozessschritte und Kontrollen dokumentieren . . .	210

	3.3.3	Kontrolldesign analysieren und bewerten	219
	3.3.4	Kontrollschwächen identifizieren, dokumentiere und validieren	222
4		Kontrollschwächen beheben	224
	4.1	Maßnahmen zur Behebung der Kontrollschwächen festlegen	224
	4.2	Umsetzung der Maßnahmen überwachen	226
	4.3	Kontrolldesign erneut bewerten bzw. Kontrolltest erneut durchführen.	226
5		Wirksamkeit des internen Kontrollsystems testen	227
	5.1	Umfang der Kontrolltests festlegen	228
	5.2	Zeitraum der Kontrolltests planen und Ressourcen bereitstellen.	233
	5.3	Kontrolltests durchführen	236
	5.4	Ergebnisse der Kontrolltests dokumentieren und bewerten	237
6		Sign-off und Managementberichterstattung.	239
	6.1	Auswertung des Designs und der Wirksamkeit der Kontrollen	240
		6.1.1 Analyse auf Basis der Prozess-Sicht	241
		6.1.2 Analyse auf Basis der festgelegten Kontrollziele	242
		6.1.3 Analyse auf Basis der Konten-Sicht	243
	6.2	Bericht über identifizierte Kontrollschwächen.	244
	6.3	Bericht über die Beseitigung der Kontrollschwächen.	245
	6.4	Sign-off-Prozess	246
	6.5	Managementbericht über das interne Kontrollsystem	248
	6.6	Externe Berichterstattung	249
7		Attestieren und Berichten.	250
	7.1	SOA 404 Prüfungsplanung und -vorgehen	251
	7.2	Beurteilung der Vorgehensweise des Managements	252
	7.3	Beurteilung der COSO-Elemente und der Kontrollen auf der Unternehmensebene (Company-level Controls)	253
	7.4	Prüfung interner Kontrollen durch einen externen Prüfer	254
	7.5	Einschätzung und Bericht des Abschlussprüfers.	259
8		Projektmanagement/Project Support Office	260
9		Projektbegleitende Prüfung/Qualitätssicherung.	264
	9.1	Ziele der projektbegleitenden Qualitätssicherung	266

9.2	Planung und Durchführung der projektbegleitenden Qualitätssicherung	268
9.3	Informationsweitergabe und Kommunikation	281
9.4	Zusammenfassung	281
10	Zusammenfassung	282
V	Praxisberichte aus Sarbanes-Oxley-Projekten	285
1	Projektstruktur und Vorgehensmodell der Bayer AG zur Umsetzung der Anforderungen des Sarbanes-Oxley Act (Section 404)	285
1.1	Zentrales Kernteam mit dezentralen Gesellschaftsteams . .	285
1.2	Projektleitung	286
1.3	Vertretung der Teilkonzerne und Servicegesellschaften . .	287
1.4	Teilprojektstruktur (Subteams)	287
1.4.1	Subteam Processes	287
1.4.2	Subteam Self-Assessment.	287
1.4.3	Subteam Monitoring of ICS	288
1.4.4	Subteam Software Infrastructure	288
1.4.5	Subteam General IS Controls	288
1.4.6	ICS – Requirements.	289
1.4.7	Project-Office	289
1.5	Regionale Koordination	289
1.6	Einbindung des Wirtschaftsprüfers	291
2	Die Bedeutung des Sarbanes-Oxley Act für die Interne Revision der DaimlerChrysler AG	292
2.1	Aktivitäten im Rahmen der Umsetzung des Sarbanes-Oxley Act	293
2.1.1	Bildung von Projektgruppen und Committees	293
2.1.2	Neuordnung der Berichtswege	294
2.1.3	Aktualisierung der Geschäftsordnung des Prüfungsausschusses	294
2.1.4	Herausgabe eines Ethik-Kodex für die oberen Führungskräfte	295
2.1.5	Zertifizierung und Subzertifizierung	295
2.1.6	Projektgruppe »Internal Control over Financial Reporting«	296
2.1.7	Dokumentation der Internen Kontrollsysteme	297
2.1.8	Prüfung der Wirksamkeit der Internen Kontroll- systeme.	298
2.1.9	Erstellung des Internen Kontrollberichts	298

2.2	Auswirkungen auf die Interne Revision als Abteilung . . .	298
2.3	Die Bedeutung des Sarbanes-Oxley Act für die Interne Revision	299
3	Projekt S-OX 404 – Umsetzung der Section 404 bei der Deutschen Telekom	300
3.1	Projekt Set-up	300
3.2	Projektorganisation	300
3.3	Scoping aus Sicht der Deutschen Telekom	302
3.4	Die quantitative Auswahl	303
3.5	Die qualitative Auswahl	304
3.6	Auswahl von Prozessen und Pilotierung	304
3.7	Schlusswort	305
4	Praxisbericht zum SOX-Projekt der Dresdner Bank	306
4.1	Überblick über das Projekt	306
4.2	Perspektive des Sarbanes-Oxley-Projektleiters	307
4.2.1	Projektstruktur und Projekt-Set-up	307
4.2.2	Scoping-Prozess	309
4.2.3	Tool-Auswahl und Pilotierung	309
4.2.4	Nächste Schritte	310
5	Die Initiierung und Konzeption eines konzernweiten Sarbanes-Oxley Act Section 404 Readiness-Projektes bei E.ON.	311
5.1	Ausgangslage	311
5.2	Projektvorgehen	312
5.2.1	Grundlagen	312
5.2.2	Projektinitiierung und -konzeption	312
5.2.3	Nächste Schritte	320
5.2.4	Kritische Erfolgsfaktoren	320
5.3	Fazit	321
6	Die Umsetzung des Sarbanes-Oxley Act bei der SAP AG, Fokus Internes Kontrollsystem (Sec. 404, 302 SOA)	323
6.1	Projektstruktur: Verteilte Verantwortung bei zentraler Koordination	323
6.2	Aufwändigste Anforderung: Dokumentation, Testing und Zertifizierung des Internen Kontrollsystems gemäß Sec. 404, 302 SOA	324
6.3	Herausforderungen des »Regelbetriebs«: Systemtechnische Unterstützung durch das SAP-Tool »Management of Internal Controls (MIC)«	326

7 Erfahrungen von Xerox als Tochter einer US-Firma 331
 7.1 Projektstart 332
 7.2 Definition des Projektumfangs 333
 7.3 Dry Run 334
 7.4 Empfehlungen. 334

VI Unterstützung von SOA- und anderen IKS-Projekten durch SAP's »Management of Internal Controls« 335

1 IT-Unterstützung für das Management interner Kontrollen . . . 336
 1.1 Erwartungen an eine SOA-Anwendung 336
 1.2 SAP-Anwendung Management of Internal Controls 337

2 Die SAP-Anwendung MIC im Detail 338
 2.1 Phasen 338
 2.2 Organisationseinheiten, Prozesse, Kontrollziele, Risiken und interne Kontrollen 338
 2.2.1 Zentrale Definition von Organisationseinheiten, Prozessen, Kontrollzielen und Risiken 338
 2.2.2 Organisationseinheiten-spezifische Definition von Prozessen und internen Kontrollen 340
 2.3 MIC-Aufgaben- und Rollenkonzept 341
 2.4 MIC-Workflow-Konzept. 343
 2.5 Beurteilung des Designs interner Kontrollen. 344
 2.6 Test der Effektivität interner Kontrollen. 346
 2.7 Interne Kontrollen auf Management-Ebene 347
 2.8 Berichtswesen 348
 2.9 Sign-off 350

3 mySAP ERP und Packaged Solution 351

4 Zusammenfassung und Ausblick. 351

VII Zusammenfassung und Ausblick 353

Literaturverzeichnis. 357
 Glossar 363
 Stichwortverzeichnis 367
 Die Autoren 371