

Inhaltsverzeichnis

1	Einleitung	1
1.1	Aufbau des Buches	2
Teil I		
COBIT verstehen		5
2	Entwicklung und Bedeutung von COBIT	7
2.1	ISACA und das IT Governance Institute	7
2.2	Entstehung und Entwicklung von COBIT	9
2.3	COBIT-Produktfamilie	13
3	Die sechs Prinzipien eines Governance-Systems	17
3.1	Prinzip 1: Mehrwert für die Anspruchsgruppen bereitstellen	18
3.2	Prinzip 2: Ganzheitlicher Ansatz	19
3.3	Prinzip 3: Dynamisches Governance-System	21
3.4	Prinzip 4: Governance getrennt vom Management	22
3.5	Prinzip 5: Zugeschnitten auf die Bedürfnisse des Unternehmens	23
3.6	Prinzip 6: End-to-End-Governance-System	25
4	Prinzipien für Governance-Rahmenwerke	27
4.1	Prinzip 1: Basierend auf einem konzeptionellen Modell	27
4.2	Prinzip 2: Offen und flexibel	27
4.3	Prinzip 3: An wichtigen Standards ausgerichtet	28
5	Komponenten und ihre Dimensionen	29
5.1	Anspruchsgruppen	30
5.2	Ziele	31
5.3	Lebenszyklus	32
5.4	Bewährte Verfahren	33

6	Prinzipien, Richtlinien und Verfahren	35
6.1	Anspruchsgruppen	35
6.2	Ziele	36
6.3	Lebenszyklus	36
6.4	Bewährte Verfahren	37
7	Organisationsstrukturen	39
7.1	Anspruchsgruppen	40
7.2	Ziele	40
7.3	Lebenszyklus	40
7.4	Bewährte Verfahren	41
8	Kultur, Ethik und Verhalten	43
8.1	Anspruchsgruppen	43
8.2	Ziele	44
8.3	Lebenszyklus	44
8.4	Bewährte Verfahren	45
9	Services, Infrastruktur und Anwendungen	47
9.1	Anspruchsgruppen	47
9.2	Ziele	48
9.3	Lebenszyklus	48
9.4	Bewährte Verfahren	49
10	Mitarbeiter, Fähigkeiten und Kompetenzen	51
10.1	Anspruchsgruppen	51
10.2	Ziele	52
10.3	Lebenszyklus	52
10.4	Bewährte Verfahren	53
11	Prozesse	55
11.1	Anspruchsgruppen	55
11.2	Ziele	55
11.3	Lebenszyklus	56
11.4	Bewährte Verfahren	56

12	Information	57
12.1	Anspruchsgruppen	57
12.2	Ziele	59
12.3	Lebenszyklus	62
12.4	Bewährte Verfahren	63
13	Kernmodell	65
13.1	Domänen mit Governance- und Managementzielen	66
13.1.1	Governance-Domäne	68
13.1.2	Management-Domänen	69
13.1.2.1	Management-Domäne APO	70
13.1.2.2	Management-Domäne BAI	72
13.1.2.3	Management-Domäne DSS	74
13.1.2.4	Management-Domäne MEA	75
13.1.3	Übergreifende Elemente des Kernmodells	76
13.1.3.1	Name des Governance- und Managementziels	76
13.1.3.2	Beschreibung und Zweck	76
13.1.3.3	Unternehmensziele und IT-bezogene Ziele	77
13.1.4	Prozesse im Kernmodell	77
13.1.4.1	Prozesspraktiken und beispielhafte Metriken	78
13.1.4.2	Prozessaktivitäten und zugeordneter Fähigkeitsgrad	81
13.1.4.3	Zugehörige Leitfäden und detaillierte Referenzen	84
13.1.5	Organisationstrukturen im Kernmodell	85
13.1.6	Informationsflüsse und -elemente im Kernmodell	90
13.1.7	Mitarbeiter, Fähigkeiten und Kompetenzen im Kernmodell	92
13.1.8	Richtlinien und Verfahren im Kernmodell	93
13.1.9	Kultur, Ethik und Verhalten im Kernmodell	93
13.1.10	Services, Infrastruktur und Anwendungen im Kernmodell	94
14	COBIT Performance Management	95
14.1	CMMI Development	96
14.2	Prozessbewertungsmodell (COBIT 2019)	97
14.3	ISO/IEC 15504 und ISO/IEC 33000	98
14.4	Prozessbewertungsmodell (PAM)	103
14.4.1	Indikatoren für die Prozessdurchführung	105
14.4.2	Indikatoren für die Prozessfähigkeit	109

15	Referenzen für COBIT	117
15.1	Entwicklung der COBIT-Referenzen	117
15.2	COSO Enterprise Risk Management	121
15.3	ITIL und ISO/IEC 20000	126
15.4	Capability Maturity Model (Integration)	130
15.5	PMBOK	134
15.6	TOGAF	136
15.7	COBIT als Integrationsrahmenwerk	136
16	Die wesentlichen Veränderungen zu COBIT 5	141
Teil II		
COBIT anwenden		147
<hr/>		
17	Geschäftsrelevante IT-Prozesse identifizieren	149
17.1	COBIT-Zielkaskade	150
17.2	Designfaktoren	155
18	Reifegrad von IT-Prozessen ermitteln	159
18.1	Prozessaktivitäten beurteilen	159
18.2	Prozesspraktiken und Arbeitsprodukte beurteilen	163
18.3	Selbsteinschätzung der Prozessbefähigung durchführen	165
19	Kennzahlensysteme aufbauen	169
19.1	IT Balanced Scorecard	169
19.2	COBIT-Ziele und -Metriken in eine IT Balanced Scorecard integrieren	172
19.2.1	COBIT-Ziele in eine IT Balanced Scorecard integrieren	172
19.2.2	COBIT-Metriken in eine IT Balanced Scorecard integrieren	175
20	Geschäftsprozesskontrollen optimieren	177
21	IT-Governance ausüben	181
21.1	Grundlagen der IT-Governance	181
21.2	ISO/IEC 38500: Corporate Governance of IT	182
21.3	COBIT als IT-Governance-Rahmenwerk	186

21.4	Kernbereiche der IT-Governance	188
21.4.1	Strategische Ausrichtung der IT	190
21.4.2	Wertbeitrag der IT	193
21.4.3	Management der IT-Ressourcen	195
21.4.4	Risikomanagement in der IT	197
21.4.5	Messen der IT-Performance	199
21.5	IT Governance Policy erstellen	201
22	IT-Governance kontinuierlich verbessern	203
22.1	Implementierungs-Lebenszyklus	203
22.1.1	Programmmanagement	207
22.1.2	Änderungsmanagement	208
22.1.3	Kontinuierliche Verbesserung	211
22.1.4	Herausforderungen und Erfolgsfaktoren	212
22.1.5	Business Case	216
22.2	Governance System Design Workflow	218
23	IT-Risiken managen	221
23.1	Grundlagen des Risikomanagements	222
23.2	IT-Risikomanagement im COBIT-Kernmodell	224
23.2.1	Governance-Ziel EDM03	224
23.2.2	Managementziel APO12	225
23.2.3	Risikobehandlung in anderen COBIT-Prozessen	227
23.2.3.1	Programm- und Projektrisikomanagement	227
23.2.3.2	Lieferantenrisikomanagement	228
23.2.3.3	Risikoanalyse bei der Softwareauswahl und -entwicklung	229
23.3	Umsetzungsleitfaden »COBIT 5 for Risk«	230
23.4	Governance und Management der Risikofunktion	230
23.4.1	Prinzipien, Richtlinien und Rahmenwerke für die Risikofunktion	231
23.4.2	Prozesse für die Risikofunktion	232
23.4.3	Organisationsstrukturen für die Risikofunktion	234
23.4.4	Kultur, Ethik und Verhalten für die Risikofunktion	235
23.4.5	Informationselemente für die Risikofunktion	236
23.4.6	Services, Infrastruktur und Anwendungen für die Risikofunktion	242
23.4.7	Fähigkeiten und Kompetenzen für die Risikofunktion	243

23.5	Risikomanagementprozesse	244
23.5.1	Risikoereignisse	244
23.5.2	Risikoindikatoren	247
23.5.3	Risikoszenarien bilden	248
23.5.4	Risikobehandlung	251
24	Informationssicherheit managen	253
24.1	Grundlagen der Informationssicherheit	253
24.1.1	ISO/IEC-27000-Normenfamilie	254
24.1.2	ISF Standard of Good Practice for Information Security	255
24.1.3	NIST Special Publications 800	255
24.1.4	HITRUST CSF	256
24.1.5	CMMI Cybermaturity Platform	257
24.1.6	CIS Critical Security Controls for Effective Cyber Defense ...	257
24.2	Informationssicherheit im COBIT-Kernmodell	258
24.2.1	Informationssicherheitsrelevante Governance- und Managementziele	258
24.2.2	Managementziel APO13	259
24.2.3	Managementziel DSS05	260
24.3	Umsetzungsleitfaden »COBIT 5 for Information Security«	262
24.4	Enabler für die Informationssicherheit	262
24.4.1	Prinzipien, Richtlinien und Rahmenwerke für die Informationssicherheit	263
24.4.2	Prozesse für die Informationssicherheit	264
24.4.3	Organisationsstrukturen für die Informationssicherheit	266
24.4.4	Kultur, Ethik und Verhalten für die Informationssicherheit ...	267
24.4.5	Informationstypen für die Informationssicherheit	268
24.4.6	Services, Infrastruktur und Anwendungen für die Informationssicherheit	270
24.4.7	Fähigkeiten und Kompetenzen für die Informationssicherheit	271
25	IT-Compliance erreichen	273
25.1	Grundlagen der IT-Compliance	273
25.1.1	Einhaltung von Gesetzen und Rechtsverordnungen	274
25.1.2	Einhaltung sonstiger Anforderungen	275
25.2	IT-Compliance im COBIT-Kernmodell	276
25.2.1	Compliance-relevante Governance- und Managementziele ...	276
25.2.2	Managementziel MEA03	278
25.3	Anwendungsbeispiel: COBIT als Basis eines IT-Compliance-Rahmenwerks	280

26	IT-Outsourcing steuern	285
26.1	Outsourcing-relevante Governance- und Managementziele	285
26.2	Managementziel APO10	287
26.3	Outsourcing-Assurance	288
26.3.1	Assurance Reports	289
26.3.2	Umfang und Inhalte eines Berichts nach ISAE 3402 oder PS 951	289
26.4	Bedeutung von COBIT für Berichte nach ISAE 3402 oder PS 951	291
26.4.1	Anwendungsbeispiel: Kontrollziele und -beschreibungen mit COBIT strukturieren	291
27	IT-Assurance-Initiativen durchführen	295
27.1	Grundlagen der Assurance	296
27.2	Assurance im COBIT-Kernmodell	297
27.2.1	Managementziel MEA04	297
27.3	Umsetzungsleitfaden »COBIT 5 for Assurance«	299
27.4	Governance und Management der Assurance-Funktion	300
27.4.1	Prinzipien, Richtlinien und Rahmenwerke für die Assurance	301
27.4.2	Prozesse für die Assurance-Funktion	301
27.4.3	Organisationsstrukturen für die Assurance-Funktion	303
27.4.4	Kultur, Ethik und Verhalten für die Assurance-Funktion	303
27.4.5	Informationstypen für die Assurance-Funktion	305
27.4.6	Services, Infrastruktur und Anwendungen für die Assurance	309
27.4.7	Fähigkeiten und Kompetenzen für die Assurance-Funktion	310
27.5	Assurance über einen Prüfungsgegenstand geben	311
27.5.1	Prüfungsumfang festlegen	312
27.5.2	Enabler verstehen, Beurteilungskriterien festlegen und Beurteilung durchführen	314
27.5.2.1	Beurteilung des Enablers Prinzipien, Richtlinien und Rahmenwerke	315
27.5.2.2	Beurteilung des Enablers Prozesse	317
27.5.2.3	Beurteilung des Enablers Organisationsstrukturen	318
27.5.2.4	Beurteilung des Enablers Kultur, Ethik und Verhalten	320
27.5.2.5	Beurteilung des Enablers Information	322
27.5.2.6	Beurteilung des Enablers Services, Infrastruktur und Anwendungen	323
27.5.2.7	Beurteilung des Enablers Mitarbeiter, Fähigkeiten und Kompetenzen	324
27.5.3	Prüfungsergebnisse kommunizieren	328

Teil III

COBIT in der Praxis **329**

28	Einführung von COBIT für die IT-Steuerung	331
28.1	Modell der drei Verteidigungslinien	332
28.2	COBIT im regulatorischen Umfeld	334
28.3	Statement of Applicability	335
28.4	COBIT in der IT-Governance	336
28.5	COBIT und die IT-Prozesse	337
28.6	COBIT und die zwei Sichtweisen der IT-Governance	339
	28.6.1 IT-Compliance	339
	28.6.2 IT-Audit	340
28.7	COBIT und die Ausgestaltung von IT-Risiken	340
	28.7.1 Adaption der IT-Risiken mittels COBIT 2019 IT Risk Categories	342
28.8	Zusammenspiel IT-Governance	343
28.9	Fazit	344
29	COBIT als Basis des IT-internen Kontrollsystems	345
29.1	Ausgangslage	345
29.2	Internes Kontrollsystem	346
	29.2.1 Three-Lines-of-Defense-Modell	346
	29.2.2 Internes Kontrollsystem	346
29.3	BMW Group IT-IKS	347
	29.3.1 Weiterentwicklung	349
	29.3.2 ISAE 3402	350
	29.3.3 Migration auf COBIT 2019	350
	29.3.4 Transformation zu einem 100 % agilen Vorgehensmodell	351
29.4	Fazit	352
30	Einführung neuer IT-Governance-Prozesse	353
30.1	Einleitung	353
30.2	Ausgangssituation	354
30.3	IT-Strategiephase	354
30.4	Planung und Durchführung der Transformation	359
	30.4.1 Implementierungsplanung	359
	30.4.2 Veränderung der Ablauforganisation	360
	30.4.3 Gründe für eine Veränderung der Aufbauorganisation	362
	30.4.4 Veränderung der Aufbauorganisation	363

30.5	Kontinuierliche Verbesserung und regelmäßiges Self-Assessment	364
30.6	Fazit	365
31	COBIT als Rahmenwerk für die Revision	367
31.1	COBIT als Grundlage für das Audit Universe in der IT-Revision	368
31.2	Definition von Prüfungsobjekten	369
31.3	Prüfungsleitfäden	371
31.4	Vollständigkeit Audit Universe	373
31.5	Schnittstellen zu Fachrevisionsprüfungen	374
31.6	Durchführung einer Prüfung	375
31.7	Querauswertung von Prüfungsergebnissen	376
31.8	Migration auf neuere COBIT-Versionen	378
31.9	Fazit	380
32	COBIT-Risikoszenarien auf Unternehmensziele anwenden	381
32.1	Einleitung	381
32.2	Kategorisierung von Risiken	382
32.3	Risikoszenarien und Risikokategorien	383
32.4	Anwendung der Kategorisierung	386
32.5	Definition eines angemessenen Sicherheitsniveaus	387
32.6	Quantitative Abhängigkeit der Unternehmensziele vom Sicherheitsniveau	388
32.7	Fazit	392
 Teil IV		
COBIT-Kenntnisse nachweisen		393
33	Zertifizierungen und Zertifikate	395
33.1	Internationale Zertifizierungen und Zertifikate	395
	33.1.1 CGEIT: Certified in the Governance of Enterprise IT	395
	33.1.2 Internationale Zertifikate	397
33.2	Nationale Zertifikate	398
	33.2.1 IT-Governance & IT-Compliance Practitioner	399
	33.2.2 IT-Governance-Manager	401
	33.2.3 IT-Compliance-Manager	403

Teil V**COBIT-Kenntnisse überprüfen 405**

34	Wissens- und Verständnisfragen	407
34.1	Wissensfragen zu COBIT	407
34.1.1	Einführung in das Rahmenwerk	407
34.1.2	COBIT-Prinzipien	408
34.1.3	Governance-System und -Komponenten	410
34.1.4	Governance- und Managementziele	413
34.1.5	Designfaktoren	416
34.1.6	Performance Management, Anpassung und Umsetzung	417
34.2	Lösungen zu den Wissensfragen	419
34.2.1	Lösungen zur Einführung in das Rahmenwerk	419
34.2.2	Lösungen zu COBIT-Prinzipien	421
34.2.3	Lösungen zu Governance-System und -Komponenten	423
34.2.4	Lösungen zu Governance- und Managementzielen	427
34.2.5	Lösungen zu Designfaktoren	431
34.2.6	Lösungen zu Performance Management, Anpassung und Umsetzung	432
34.3	Verständnisfragen zu COBIT	434
34.4	Lösungen zu den Verständnisfragen	435

Teil VI**Anhang 437**

A	Übersicht Governance- und Managementziele	439
B	Übersicht der COBIT-Prozesse und -Prozesspraktiken	443
C	Übersicht der Unternehmensziele und zugeordneten IT-bezogenen Ziele in COBIT 2019	465
D	Übersicht der IT-bezogenen Ziele und zugeordneten COBIT-Prozesse	467
	Abkürzungsverzeichnis	471
	Literaturverzeichnis	475
	Index	483