

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>Teil I</b>		
<b>COBIT verstehen</b>		<b>5</b>
<b>2</b>	<b>Entwicklung und Bedeutung von COBIT</b>	<b>7</b>
2.1	ISACA und das IT Governance Institute . . . . .	7
2.2	Entstehung und Entwicklung von COBIT . . . . .	9
2.3	COBIT-Produktfamilie . . . . .	12
<b>3</b>	<b>Die fünf Kernprinzipien</b>	<b>17</b>
3.1	Prinzip 1: Erfüllen der Anforderungen der Anspruchsgruppen . . . . .	17
3.2	Prinzip 2: Abdecken des gesamten Unternehmens . . . . .	18
3.3	Prinzip 3: Anwenden eines einheitlichen, integrierten Rahmenwerks . . . . .	20
3.4	Prinzip 4: Ermöglichen eines ganzheitlichen Ansatzes . . . . .	21
3.5	Prinzip 5: Unterscheiden zwischen Governance und Management . . . . .	23
<b>4</b>	<b>Enabler und deren Dimensionen</b>	<b>25</b>
4.1	Anspruchsgruppen . . . . .	26
4.2	Ziele . . . . .	27
4.3	Lebenszyklus . . . . .	28
4.4	Bewährte Verfahren . . . . .	28
<b>5</b>	<b>Prinzipien, Richtlinien und Rahmenwerke</b>	<b>31</b>
5.1	Anspruchsgruppen . . . . .	31
5.2	Ziele . . . . .	32
5.3	Lebenszyklus . . . . .	33
5.4	Bewährte Verfahren . . . . .	33

<b>6</b>	<b>Organisationsstrukturen</b>	<b>35</b>
6.1	Anspruchsgruppen . . . . .	35
6.2	Ziele . . . . .	35
6.3	Lebenszyklus . . . . .	36
6.4	Bewährte Verfahren . . . . .	36
<b>7</b>	<b>Kultur, Ethik und Verhalten</b>	<b>37</b>
7.1	Anspruchsgruppen . . . . .	37
7.2	Ziele . . . . .	38
7.3	Lebenszyklus . . . . .	38
7.4	Bewährte Verfahren . . . . .	38
<b>8</b>	<b>Services, Infrastruktur und Anwendungen</b>	<b>41</b>
8.1	Anspruchsgruppen . . . . .	41
8.2	Ziele . . . . .	42
8.3	Lebenszyklus . . . . .	42
8.4	Bewährte Verfahren . . . . .	42
<b>9</b>	<b>Mitarbeiter, Fähigkeiten und Kompetenzen</b>	<b>45</b>
9.1	Anspruchsgruppen . . . . .	45
9.2	Ziele . . . . .	45
9.3	Lebenszyklus . . . . .	46
9.4	Bewährte Verfahren . . . . .	46
<b>10</b>	<b>Prozesse</b>	<b>47</b>
10.1	Anspruchsgruppen . . . . .	47
10.2	Ziele . . . . .	47
10.3	Lebenszyklus . . . . .	48
10.4	Bewährte Verfahren . . . . .	48
<b>11</b>	<b>Prozessreferenzmodell</b>	<b>49</b>
11.1	Domänen und Prozesse . . . . .	49
11.1.1	Governance-Domäne EDM . . . . .	50
11.1.2	Management-Domänen . . . . .	51
11.1.2.1	Management-Domäne APO . . . . .	53
11.1.2.2	Management-Domäne BAI . . . . .	55
11.1.2.3	Management-Domäne DSS . . . . .	57
11.1.2.4	Management-Domäne MEA . . . . .	58

---

11.1.3	Prozesselemente	59
11.1.3.1	Prozessidentifizierung	59
11.1.3.2	Prozessbeschreibung und Prozesszweck	59
11.1.3.3	IT-bezogene Ziele und zugehörige Metriken	60
11.1.3.4	Prozessziele und zugehörige Metriken	61
11.1.3.5	RACI-Diagramm	62
11.1.3.6	Prozesspraktiken	66
11.1.3.7	Inputs und Outputs	69
11.1.3.8	Prozessaktivitäten	72
11.1.3.9	Referenzmaterial	75
11.1.4	Anforderungen an alle Prozesse (Process Control Objectives)	75
11.1.5	Anforderungen an Geschäftsprozesse (Application Control Objectives)	77
<b>12</b>	<b>Information</b>	<b>81</b>
12.1	Anspruchsgruppen	81
12.2	Ziele	83
12.3	Lebenszyklus	84
12.4	Bewährte Verfahren	85
12.5	Governance und Management des Enablers Information	90
12.5.1	Enabling Information für die regulatorische Compliance	91
<b>13</b>	<b>Reifegradmodelle</b>	<b>95</b>
13.1	ISO/IEC 15504	95
13.2	Prozessreifegradmodelle von COBIT 5	100
13.2.1	COBIT-5-Prozessbefähigungsmodell	100
13.2.1.1	Indikatoren für die Prozessdurchführung	102
13.2.1.2	Indikatoren für die Prozessfähigkeit	106
13.2.2	Reifegradmodell mit Attributen	113
<b>14</b>	<b>Referenzen für COBIT</b>	<b>117</b>
14.1	Einleitung	117
14.2	COSO: Internal Control – Integrated Framework	122
14.2.1	COSO I	122
14.2.2	COSO 2013	127
14.3	COSO: Enterprise Risk Management – Integrated Framework	131
14.4	ITIL und ISO/IEC 20000	131
14.5	Capability Maturity Model (Integrated)	135
14.6	PRINCE2/PMBOK	136

14.7	TOGAF . . . . .	139
14.8	COBIT als Integrator . . . . .	140
15	<b>Die wesentlichen Veränderungen zu COBIT 4.1</b>	143
<b>Teil II</b>		
<b>COBIT anwenden</b>		<b>147</b>
16	<b>Geschäftsrelevante IT-Prozesse identifizieren</b>	149
16.1	COBIT-5-Zielkaskade . . . . .	149
16.2	Anforderungen an die Informationsqualität definieren . . . . .	156
17	<b>Reifegrad von IT-Prozessen ermitteln</b>	161
17.1	Prozessbefähigungsbeurteilungen durchführen . . . . .	161
17.2	Selbsteinschätzung der Prozessbefähigung durchführen . . . . .	164
17.3	Attribut-Reifegradmodell anwenden . . . . .	166
18	<b>Kennzahlensysteme aufbauen</b>	169
18.1	IT Balanced Scorecard . . . . .	169
18.2	COBIT-Ziele und -Metriken in eine IT Balanced Scorecard integrieren . . . . .	172
18.2.1	COBIT-Ziele in eine IT Balanced Scorecard integrieren . . . . .	172
18.2.2	COBIT-Metriken in eine IT Balanced Scorecard integrieren . . . . .	175
19	<b>IT-Governance ausüben</b>	179
19.1	Grundlagen der IT-Governance . . . . .	179
19.1.1	IT-Governance . . . . .	180
19.1.2	ISO/IEC 38500: Corporate Governance of IT . . . . .	180
19.2	COBIT als IT-Governance-Rahmenwerk . . . . .	184
19.3	Kernbereiche der IT-Governance . . . . .	186
19.3.1	Strategische Ausrichtung der IT . . . . .	188
19.3.2	Wertbeitrag der IT . . . . .	191
19.3.3	Management der IT-Ressourcen . . . . .	193
19.3.4	Risikomanagement in der IT . . . . .	194
19.3.5	Messen der IT-Performance . . . . .	197
19.4	IT Governance Policy erstellen . . . . .	198

---

<b>20</b>	<b>Unternehmens-IT kontinuierlich verbessern</b>	<b>201</b>
20.1	Implementierungslebenszyklus . . . . .	201
20.2	Implementierungselemente und Tools . . . . .	207
<b>21</b>	<b>IT-Risiken managen</b>	<b>209</b>
21.1	Grundlagen des Risikomanagements . . . . .	209
21.1.1	COSO Enterprise Risk Management . . . . .	212
21.1.2	ISO/IEC 31000 . . . . .	215
21.2	IT-Risikomanagement im COBIT-5-Prozessreferenzmodell . . . . .	217
21.2.1	COBIT-Prozess EDM03 . . . . .	218
21.2.2	COBIT-Prozess APO12 . . . . .	219
21.2.3	Risikobehandlung in anderen COBIT-5-Prozessen . . . . .	220
21.2.3.1	Projektrisikomanagement . . . . .	220
21.2.3.2	Lieferanten-Risikomanagement . . . . .	221
21.2.3.3	Risikoanalyse bei der Softwareauswahl und -entwicklung . . . . .	221
21.3	Risikoereignisse identifizieren . . . . .	222
21.3.1	Risikoereignisse . . . . .	222
21.3.2	Risikoindikatoren . . . . .	224
21.4	Risikoszenarien bilden . . . . .	225
21.4.1	Generische Risikoszenarien . . . . .	229
21.5	Governance und Management der Risiko-Funktion . . . . .	232
21.5.1	Prinzipien, Richtlinien und Rahmenwerke für die Risiko-Funktion . . . . .	233
21.5.2	Prozesse für die Risiko-Funktion . . . . .	234
21.5.3	Organisationsstrukturen für die Risiko-Funktion . . . . .	236
21.5.4	Kultur, Ethik und Verhalten für die Risiko-Funktion . . . . .	237
21.5.5	Informationselemente für die Risiko-Funktion . . . . .	238
21.5.6	Services, Infrastruktur und Anwendungen für die Risiko-Funktion . . . . .	244
21.5.7	Fähigkeiten und Kompetenzen für die Risiko-Funktion . . . . .	244
21.6	Weitere Prozesse für das Risikomanagement . . . . .	246
21.6.1	Risikoaggregation . . . . .	246
21.6.2	Risikobehandlung . . . . .	247
<b>22</b>	<b>Informationssicherheit managen</b>	<b>249</b>
22.1	Grundlagen der Informationssicherheit . . . . .	249
22.1.1	ISO/IEC-27000-Normenfamilie . . . . .	250
22.1.2	ISF 2011 Standard of Good Practice for Information Security . . . . .	252
22.1.3	NIST Special Publication 800-53 . . . . .	253

---

22.2	Informationssicherheit im COBIT-5-Prozessreferenzmodell . . . . .	254
22.2.1	COBIT-Prozess APO13 . . . . .	254
22.2.2	COBIT-Prozess DSS05 . . . . .	255
22.3	Umsetzungsleitfaden »COBIT 5 for Information Security« . . . . .	256
22.4	Enabler für die Informationssicherheit . . . . .	256
22.4.1	Prinzipien, Richtlinien und Rahmenwerke für die Informationssicherheit . . . . .	257
22.4.2	Prozesse für die Informationssicherheit . . . . .	258
22.4.3	Organisationsstrukturen für die Informationssicherheit . . . . .	260
22.4.4	Kultur, Ethik und Verhalten für die Informationssicherheit . . . . .	261
22.4.5	Informationstypen für die Informationssicherheit . . . . .	262
22.4.6	Services, Infrastruktur und Anwendungen für die Informationssicherheit . . . . .	264
22.4.7	Fähigkeiten und Kompetenzen für die Informationssicherheit . . . . .	264
23	<b>IT-Compliance erreichen</b>	267
23.1	Grundlagen der IT-Compliance . . . . .	267
23.1.1	Einhaltung von Gesetzen und Rechtsverordnungen . . . . .	268
23.1.2	Einhaltung sonstiger Anforderungen . . . . .	269
23.2	IT-Compliance im COBIT-5-Prozessreferenzmodell . . . . .	270
23.2.1	COBIT-Prozess MEA03 . . . . .	270
23.3	COBIT als Basis eines IT-Compliance-Rahmenwerks . . . . .	272
24	<b>IT-Outsourcing steuern</b>	277
24.1	COBIT-Prozess APO10 . . . . .	277
24.2	Outsourcing-Assurance . . . . .	278
24.2.1	Assurance Reports . . . . .	280
24.2.2	Umfang und Inhalte eines Berichts nach ISAE 3402 oder PS 951 . . . . .	280
24.3	Anwendung von COBIT bei der Erstellung eines Berichtes nach ISAE 3402 oder PS 951 . . . . .	282
24.3.1	Strukturierung und Beschreibung der Kontrollziele und Kontrollbeschreibungen mit COBIT 5 . . . . .	282

---

<b>25</b>	<b>IT-Assurance-Initiativen durchführen</b>	<b>287</b>
25.1	Grundlagen der Assurance . . . . .	287
25.2	Governance und Management der Assurance-Funktion . . . . .	289
25.2.1	Prinzipien, Richtlinien und Rahmenwerke für die Assurance . . . . .	290
25.2.2	Prozesse für die Assurance-Funktion . . . . .	290
25.2.3	Organisationsstrukturen für die Assurance-Funktion . . . . .	291
25.2.4	Kultur, Ethik und Verhalten für die Assurance-Funktion . . . . .	292
25.2.5	Informationstypen für die Assurance-Funktion . . . . .	294
25.2.6	Services, Infrastruktur und Anwendungen für die Assurance . . . . .	297
25.2.7	Fähigkeiten und Kompetenzen für die Assurance-Funktion . . . . .	298
25.3	Assurance über einen Prüfungsgegenstand geben . . . . .	300
25.3.1	Festlegung des Prüfungsumfangs . . . . .	301
25.3.2	Verständnis der Enabler, Festlegung der Beurteilungskriterien und Durchführung der Beurteilung . . . . .	302
25.3.2.1	Beurteilung des Enablers Prinzipien, Richtlinien und Rahmenwerke . . . . .	304
25.3.2.2	Beurteilung des Enablers Prozesse . . . . .	306
25.3.2.3	Beurteilung des Enablers Organisationsstrukturen . . . . .	306
25.3.2.4	Beurteilung des Enablers Kultur, Ethik und Verhalten . . . . .	309
25.3.2.5	Beurteilung des Enablers Information . . . . .	310
25.3.2.6	Beurteilung des Enablers Services, Infrastruktur und Anwendungen . . . . .	312
25.3.2.7	Beurteilung des Enablers Mitarbeiter, Fähigkeiten und Kompetenzen . . . . .	313
25.3.3	Kommunikation der Prüfungsergebnisse . . . . .	317
<b>Teil III</b>		
<b>COBIT in der Praxis</b>		<b>319</b>
<b>26</b>	<b>COBIT-Einführung – ein Assimilationsprozess</b>	<b>321</b>
26.1	Change-Agent-Ausbildung . . . . .	322
26.2	Aufbau internes Kontrollsyste . . . . .	322
26.3	IT-Governance und Globalisierung . . . . .	322
26.4	IT-Compliance mittels IT-Reviews . . . . .	324
26.5	Business-IT-Alignment . . . . .	324
26.6	IT Security . . . . .	324
26.7	Jüngste Aktivitäten . . . . .	324
26.8	Fazit . . . . .	326

<b>27</b>	<b>IT Management – Principles &amp; Policies</b>	<b>327</b>
27.1	Struktur der Policy-Landschaft .....	327
27.2	Warum COBIT? .....	328
27.3	Ableitung der Principles & Policies .....	329
27.4	Implementierungsrichtlinien .....	330
27.5	Review und Sozialisierung .....	332
27.6	Herausforderungen .....	332
27.6.1	Änderungsmanagement .....	332
27.6.2	Konfigurationsmanagement .....	333
27.6.3	Control Objectives .....	335
27.7	COBIT 5 for Information Security .....	335
27.8	Änderungen gegenüber COBIT 5 .....	335
27.8.1	Management von Prozessen .....	335
27.8.2	Internal Audit .....	336
27.8.3	COBIT-Prozess BAI02 .....	336
27.8.4	COBIT-Prozesspraktik BAI03.04 .....	336
27.8.5	COBIT-Prozesspraktik BAI03.05 Entwickeln von Lösungen .....	336
27.8.6	COBIT-Prozesspraktik BAI03.07 .....	336
27.8.7	COBIT-Prozess BAI06 .....	336
27.8.8	COBIT-Prozess BAI07 .....	337
27.8.9	COBIT-Prozess BAI10 .....	337
27.8.10	COBIT-Prozess DSS02 .....	337
27.9	Weiteres Vorgehen .....	337
27.10	Fazit .....	338
<b>28</b>	<b>COBIT als Rahmenwerk für die Revision</b>	<b>339</b>
28.1	Das COBIT-Framework als Grundlage für das Audit Universe in der IT-Revision .....	340
28.2	Definition von Prüfungsobjekten .....	341
28.3	Prüfungsleitfaden .....	343
28.4	Vollständigkeit Audit Universe .....	345
28.5	Schnittstellen zu Fachrevisionsprüfungen .....	346
28.6	Durchführung einer Prüfung .....	347
28.7	Querauswertung von Prüfungsergebnissen .....	349
28.8	Migration auf COBIT 5 .....	350
28.9	Fazit .....	351

---

<b>29</b>	<b>Einführung von COBIT 5</b>	<b>353</b>
29.1	Ausgangslage . . . . .	353
29.2	Vorbereitung . . . . .	354
29.3	Gründe für die Einführung von COBIT 5 . . . . .	354
29.3.1	Technologische Anforderungen . . . . .	354
29.3.2	Beachtung regulatorischer Anforderungen . . . . .	355
29.4	Umsetzung von COBIT 5 . . . . .	356
29.5	Fazit . . . . .	358
 <b>Teil IV</b>		
<b>COBIT-Kenntnisse nachweisen</b>		<b>359</b>
<b>30</b>	<b>Zertifizierungen und Zertifikate</b>	<b>361</b>
30.1	Internationale Zertifizierungen und Zertifikate . . . . .	361
30.1.1	CGEIT: Certified in the Governance of Enterprise IT . . . . .	361
30.1.2	COBIT Foundation . . . . .	363
30.2	Zertifikate des ISACA Germany Chapter . . . . .	365
30.2.1	IT-Governance & IT-Compliance Practitioner . . . . .	366
30.2.2	IT-Governance-Manager . . . . .	368
30.2.3	IT-Compliance-Manager . . . . .	370
 <b>Teil V</b>		
<b>COBIT-Kenntnisse überprüfen</b>		<b>373</b>
<b>31</b>	<b>Wissens- und Verständnisfragen</b>	<b>375</b>
31.1	Wissensfragen zu COBIT 5 . . . . .	375
31.2	Lösungen zu den Wissensfragen . . . . .	384
31.3	Verständnisfragen . . . . .	401

<b>Teil VI</b>		
<b>Anhang</b>	<b>403</b>	
<b>A</b>	<b>Übersicht der COBIT-Domänen und -Prozesse</b>	<b>405</b>
<b>B</b>	<b>Übersicht der COBIT-Prozesse und -Prozesspraktiken</b>	<b>409</b>
<b>C</b>	<b>Übersicht der Unternehmensziele und zugeordneten IT-bezogenen Ziele</b>	<b>425</b>
<b>D</b>	<b>Übersicht der IT-bezogenen Ziele und zugeordneten COBIT-Prozesse</b>	<b>429</b>
	<b>Literaturverzeichnis</b>	<b>435</b>
	<b>Abkürzungsverzeichnis</b>	<b>443</b>
	<b>Index</b>	<b>447</b>