

Inhaltsverzeichnis

| | | |
|---------------|--|-----------|
| 1 | Einleitung | 1 |
| Teil I | COBIT verstehen | 5 |
| 2 | Entwicklung und Bedeutung von COBIT | 7 |
| 2.1 | ISACA und das IT Governance Institute | 7 |
| 2.2 | Entstehung von COBIT, Val IT und Risk IT | 8 |
| 2.3 | Anspruch von COBIT | 10 |
| 2.4 | COBIT-Produktfamilie | 11 |
| 3 | Die Kerneigenschaften von COBIT | 15 |
| 3.1 | Kerneigenschaft 1: Fokussiert auf das Geschäft | 15 |
| 3.2 | Kerneigenschaft 2: Orientiert an Prozessen | 18 |
| 3.2.1 | Domänen und Prozesse | 18 |
| 3.2.2 | Prozesselemente | 26 |
| 3.2.2.1 | Prozessbeschreibung | 26 |
| 3.2.2.2 | Leitlinien für das Management | 28 |
| 3.3 | Kerneigenschaft 3: Basierend auf Anforderungen | 31 |
| 3.3.1 | Anforderungen an die IT-Prozesse (IT control objectives) | 31 |
| 3.3.2 | Anforderungen an alle Prozesse (process control objectives) | 34 |
| 3.3.3 | Anforderungen an Geschäftsprozesse (application control objectives) | 36 |
| 3.4 | Kerneigenschaft 4: Gesteuert durch Messungen | 38 |
| 3.4.1 | Reifegradmodelle | 39 |
| 3.4.1.1 | Aufbau der Reifegradmodelle | 39 |
| 3.4.1.2 | Reifegradmodell auf Prozessebene | 40 |

| | | |
|----------|--|-----------|
| 3.4.1.3 | Reifegradmodell mit Attributen | 42 |
| 3.4.1.4 | Reifegradmodell für das interne Kontrollsystem ... | 44 |
| 3.4.2 | Ziele und Metriken | 45 |
| 3.4.2.1 | Ziele | 46 |
| 3.4.2.2 | Metriken | 46 |
| 4 | Primäre Referenzen für COBIT | 49 |
| 4.1 | Einleitung | 49 |
| 4.2 | COSO: Internal Control – Integrated Framework | 50 |
| 4.3 | COSO: Enterprise Risk Management – Integrated Framework | 55 |
| 4.4 | OGC: IT Infrastructure Library | 55 |
| 4.5 | ISO/IEC 17799: Code of Practice for Information Security Management | 57 |
| 4.6 | SEI: Capability Maturity Model (Integrated) | 61 |
| 4.7 | PMI: Project Management Body of Knowledge | 65 |
| 4.8 | ISF: Standard of Good Practice for Information Security | 69 |
| 4.9 | COBIT als Integrator | 73 |
| 5 | Val IT als Ergänzung zu COBIT | 75 |
| 5.1 | Ziele und Leitsätze von Val IT | 77 |
| 5.2 | Val-IT-Domänen, Prozesse und Managementpraktiken | 78 |
| 5.3 | Val-IT-Prozesselemente | 81 |
| 5.3.1 | Prozesseingangs- und -ausgangswerte | 81 |
| 5.3.2 | RACI-Tabellen | 82 |
| 5.3.3 | Ziele und Metriken | 84 |
| 5.4 | Val-IT-Reifegradmodelle | 86 |
| 5.4.1 | Reifegradmodell auf hoher Ebene | 86 |
| 5.4.2 | Detailliertes Reifegradmodell | 87 |
| 5.5 | Val IT und andere Standards | 89 |
| 6 | Risk IT als Ergänzung zu COBIT | 91 |
| 6.1 | Ziele und Leitsätze von Risk IT | 91 |
| 6.2 | Risk-IT-Domänen, Prozesse und Kernaktivitäten | 93 |
| 6.3 | Risk-IT-Prozesselemente | 95 |
| 6.3.1 | Detaillierte Prozessbeschreibung | 95 |
| 6.3.2 | Prozesseingangs- und -ausgangswerte | 96 |
| 6.3.3 | Leitlinien für das Management | 97 |
| 6.3.3.1 | RACI-Tabellen | 97 |
| 6.3.3.2 | Ziele und Metriken | 98 |

| | | |
|----------------|---|------------|
| 6.4 | Risk-IT-Reifegradmodelle | 99 |
| 6.4.1 | Reifegradmodell auf hoher Ebene | 100 |
| 6.4.2 | Detailliertes Reifegradmodell | 100 |
| Teil II | COBIT anwenden | 103 |
| 7 | Geschäftsrelevante IT-Prozesse identifizieren | 105 |
| 7.1 | Anforderungen an die Informationsqualität definieren | 105 |
| 7.2 | IT-bezogene Geschäftsziele definieren | 108 |
| 7.3 | Bedeutsame und weniger bedeutsame COBIT-Prozesse | 110 |
| 8 | Reifegrad von IT-Prozessen ermitteln | 113 |
| 8.1 | Dimensionen der Prozessreife | 114 |
| 8.2 | Beurteilung der Reifedimension »Fähigkeit« | 114 |
| 8.2.1 | Reifegradmodell auf Prozessebene | 115 |
| 8.2.2 | Reifegradmodell auf Attributebene | 119 |
| 8.3 | Beurteilung der Reifedimension »Abdeckung« | 120 |
| 8.4 | Beurteilung der Reifedimension »Kontrolle und Steuerung« | 121 |
| 9 | Kennzahlensysteme aufbauen | 125 |
| 9.1 | IT Balanced Scorecard | 125 |
| 9.2 | COBIT-Ziele und -Kennzahlen in eine IT Balanced Scorecard integrieren | 128 |
| 10 | IT-Governance | 133 |
| 10.1 | Definition von IT-Governance | 133 |
| 10.1.1 | IT-Governance | 133 |
| 10.1.2 | ISO/IEC 38500: Corporate governance of IT | 134 |
| 10.2 | COBIT als IT-Governance-Rahmenwerk | 137 |
| 10.3 | Kernbereiche der IT-Governance | 140 |
| 10.3.1 | Strategische Ausrichtung der IT | 142 |
| 10.3.2 | Wertbeitrag der IT | 144 |
| 10.3.3 | Management der IT-Ressourcen | 146 |
| 10.3.4 | IT-Risikomanagement | 148 |
| 10.3.5 | Messen der IT-Performance | 150 |
| 10.4 | IT-Governance mit COBIT einführen | 152 |
| 10.5 | Erstellung einer IT-Governance-Policy | 157 |

| | | |
|-----------|---|------------|
| 11 | IT-Risikomanagement | 159 |
| 11.1 | Grundlagen des Risikomanagements | 160 |
| 11.1.1 | COSO Enterprise Risk Management | 162 |
| 11.1.2 | AS/NZS 4360 und ISO/IEC 31000 | 165 |
| 11.2 | IT-Risikomanagement mit COBIT | 167 |
| 11.2.1 | Der COBIT-IT-Risikomanagementprozess | 167 |
| 11.2.2 | Integration von IT-Risikomanagement in COBIT | 169 |
| 11.2.3 | Risikobehandlung in anderen COBIT-Prozessen | 171 |
| 11.2.3.1 | Projektrisikomanagement | 171 |
| 11.2.3.2 | Lieferantenrisikomanagement | 171 |
| 11.2.3.3 | Risikomanagement als Teil des IT-Governance-Zyklus | 172 |
| 11.2.3.4 | Risikoanalyse bei der Softwareauswahl und -entwicklung | 173 |
| 11.2.4 | Risikomanagement im Kontext von Geschäfts- und IT-Zielen | 173 |
| 11.3 | Identifikation und Beurteilung von IT-Risiken | 175 |
| 11.3.1 | Ereignisidentifikation mit Risikotreibern | 175 |
| 11.3.2 | Typische Prozessschwächen und deren Auswirkung | 176 |
| 11.3.3 | Risikoindikatoren | 178 |
| 11.3.4 | Risikoereignisse und -szenarien | 178 |
| 12 | IT-Compliance | 183 |
| 12.1 | Bedeutung der IT-Compliance | 183 |
| 12.1.1 | Einhaltung von Gesetzen und Rechtsverordnungen | 184 |
| 12.1.2 | Einhaltung sonstiger Anforderungen | 185 |
| 12.2 | COBIT als Basis eines IT-Compliance-Rahmenwerks | 186 |
| 13 | IT-Outsourcing | 191 |
| 13.1 | Anforderungen an das Outsourcing | 192 |
| 13.2 | Umfang und Inhalte eines Berichts nach SAS 70 oder IDW PS 951 | 193 |
| 13.3 | Anwendung von COBIT bei der Erstellung eines Berichtes nach SAS 70 oder IDW PS 951 | 195 |
| 13.3.1 | Strukturierung und Beschreibung der Kontrollziele und Kontrollen | 195 |
| 13.3.2 | Vorbereitung auf die Prüfung | 198 |
| 13.4 | Anwendung der »IT Control Objectives for Sarbanes-Oxley« | 199 |

| | | |
|-----------------|--|------------|
| 14 | IT-Assurance | 203 |
| 14.1 | Prüfungsplanung | 205 |
| 14.1.1 | »IT Assurance Universe« aufbauen | 205 |
| 14.1.2 | Rahmenwerk für IT-Prüfungsvorhaben auswählen | 207 |
| 14.1.3 | IT-Prüfung risikoorientiert planen | 208 |
| 14.1.4 | High-Level-Assessments durchführen | 209 |
| 14.1.5 | Prüfungsumfang und -ziele definieren | 210 |
| 14.1.5.1 | Management Awareness Diagnostic | 210 |
| 14.1.5.2 | COBIT Quickstart | 211 |
| 14.2 | Festlegung des Prüfungsumfanges | 213 |
| 14.3 | Prüfungsdurchführung | 216 |
| 14.3.1 | Verfeinere das Verständnis über den Prüfungsgegenstand | 216 |
| 14.3.2 | Verfeinere den Prüfungsumfang | 217 |
| 14.3.3 | Teste das Design der Kontroll- und Steuerungsmaßnahmen | 217 |
| 14.3.4 | Teste das Ergebnis der Kontroll- und Steuerungsmaßnahmen | 219 |
| 14.3.5 | Dokumentiere die Auswirkungen von Feststellungen | 220 |
| 14.3.6 | Entwickle und kommuniziere Schlussfolgerungen und Empfehlungen | 222 |
| 14.4 | Exkurs: COBIT für die IT-Prüfung im Rahmen der Jahresabschlussprüfung einsetzen | 222 |
| Teil III | COBIT-Kenntnisse nachweisen | 225 |
| 15 | Zertifizierungen und Zertifikate | 227 |
| 15.1 | Internationale Zertifizierungen und Zertifikate | 227 |
| 15.1.1 | CGEIT: Certified in the Governance of Enterprise IT | 227 |
| 15.1.2 | COBIT Foundation Exam | 229 |
| 15.2 | Nationale Zertifikate | 229 |
| 15.2.1 | COBIT (Basic) Practitioner | 230 |
| 15.2.2 | IT-Governance-Manager | 232 |
| Teil IV | COBIT-Kenntnisse überprüfen | 235 |
| 16 | Testfragen und Übungen | 237 |
| 16.1 | Beispielfragen für den COBIT Basic Practitioner | 237 |
| 16.2 | Beispielfragen für den COBIT Practitioner | 241 |

| | | |
|---------------|--|------------|
| 16.3 | Übung zur COBIT-Terminologie | 244 |
| 16.3.1 | Wichtige Elemente und Begriffe aus dem COBIT-Rahmenwerk | 244 |
| 16.3.2 | Wichtige Strukturelemente des COBIT-Rahmenwerks | 246 |
| 16.4 | Lösungen zu den Beispielfragen für den COBIT Basic Practitioner | 247 |
| 16.5 | Lösungen zu den Beispielfragen für den COBIT Practitioner | 252 |
| 16.6 | Lösung zur Übung COBIT-Terminologie | 255 |
| Anhang | | 257 |
| A | Übersicht der COBIT-Domänen und -Prozesse | 259 |
| B | Übersicht der COBIT-Prozesse und control objectives | 261 |
| C | Übersicht der Val-IT-Domänen und -Prozesse | 273 |
| D | Übersicht der Val-IT-Prozesse und -Managementpraktiken | 275 |
| E | Übersicht der Risk-IT-Domänen und -Prozesse | 283 |
| F | Übersicht der Risk-IT-Prozesse und -Kernaktivitäten | 285 |
| | Abkürzungsverzeichnis | 289 |
| | Literaturverzeichnis | 293 |
| | Stichwortverzeichnis | 297 |