

# Inhaltsübersicht

|          |   |            |
|----------|---|------------|
| <b>1</b> | <b>Einleitung</b>                                   | <b>1</b>   |
| <b>2</b> | <b>Einführung und Grundlagen</b>                    | <b>7</b>   |
| 2.1      | Die neue Rolle der IT .....                         | 7          |
| 2.2      | Trends und Treiber .....                            | 8          |
| 2.3      | Geschäftsarchitektur für IT-Governance .....        | 20         |
| 2.4      | IT-Governance: Begriff und Aufgaben .....           | 22         |
| 2.5      | Unterstützende Referenzmodelle .....                | 25         |
| 2.6      | Akzeptanz von IT-Governance .....                   | 27         |
| <b>3</b> | <b>Das COBIT-Referenzmodell</b>                     | <b>41</b>  |
| 3.1      | Einleitung und Übersicht .....                      | 42         |
| 3.2      | COBIT-Merkmale .....                                | 49         |
| 3.3      | COBIT-Komponenten .....                             | 56         |
| 3.4      | Das COBIT-Gesamtmodell .....                        | 91         |
| 3.5      | COBIT-Produkte .....                                | 103        |
| 3.6      | COBIT und COSO .....                                | 122        |
| 3.7      | COBIT in der Umsetzung des Sarbanes-Oxley Act ..... | 126        |
| 3.8      | Zertifizierung und Qualifizierung .....             | 139        |
| 3.9      | Einordnung und Bewertung .....                      | 139        |
| <b>4</b> | <b>Das Val-IT-Referenzmodell</b>                    | <b>143</b> |
| 4.1      | Überblick .....                                     | 143        |
| 4.2      | Zielsetzung von Val IT .....                        | 144        |
| 4.3      | Abgrenzung zu COBIT .....                           | 145        |
| 4.4      | Aufbau und Komponenten des Val-IT-Frameworks .....  | 146        |
| 4.5      | Der Business Case .....                             | 150        |
| 4.6      | Einordnung und Bewertung .....                      | 163        |

|           |   |            |
|-----------|---|------------|
| <b>5</b>  | <b>Das Risk-IT-Referenzmodell (Risk IT)</b>                       | <b>165</b> |
| 5.1       | Einleitung und Zielsetzung .....                                  | 165        |
| 5.2       | Adressaten und deren spezifischer Nutzen .....                    | 166        |
| 5.3       | Aufbau des Risk-IT-Referenzmodells .....                          | 167        |
| 5.4       | Weitere Produkte in Risk IT .....                                 | 185        |
| 5.5       | Einordnung und Bewertung .....                                    | 187        |
| <b>6</b>  | <b>Weitere IT-Governance-Referenzmodelle</b>                      | <b>189</b> |
| 6.1       | Der Standard ISO/IEC 38500: Corporate Governance of IT .....      | 189        |
| 6.2       | Das ITIL-Referenzmodell .....                                     | 196        |
| 6.3       | ISO/IEC 20000 .....   | 229        |
| 6.4       | Informationssicherheitsmanagement .....                           | 236        |
| 6.5       | CMMI .....  | 242        |
| <b>7</b>  | <b>Vergleich und Integration von Referenzmodellen</b>             | <b>253</b> |
| 7.1       | Einleitung und Übersicht .....                                    | 253        |
| 7.2       | Vergleich der Referenzmodelle .....                               | 255        |
| 7.3       | Kombination und Integration der Referenzmodelle .....             | 262        |
| 7.4       | Bewertung .....   | 272        |
| <b>8</b>  | <b>SOA- und Cloud-Computing-Governance</b>                        | <b>273</b> |
| 8.1       | Einleitung und Übersicht .....                                    | 273        |
| 8.2       | SOA-Governance .....  | 275        |
| 8.3       | Cloud-Computing-Governance .....                                  | 288        |
| 8.4       | Service-Governance als gemeinsame Aufgabenstellung .....          | 296        |
| <b>9</b>  | <b>Praxisbeispiel:</b>  |            |
|           | <b>Prüfung und Bewertung eines Governance-Konzepts für die IT</b> | <b>299</b> |
| 9.1       | Ausgangssituation und Motivation .....                            | 299        |
| 9.2       | Methodische Aspekte einer Prüfung .....                           | 302        |
| 9.3       | Zusammenfassung .....   | 319        |
| <b>10</b> | <b>Schlussbetrachtung</b>   | <b>321</b> |
|           | <b>Abkürzungsverzeichnis</b>                                      | <b>323</b> |
|           | <b>Literaturverzeichnis</b>                                       | <b>327</b> |
|           | <b>Index</b>  | <b>339</b> |

# Inhaltsverzeichnis

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Einleitung</b>                                      | <b>1</b> |
| <b>2</b> | <b>Einführung und Grundlagen</b>                       | <b>7</b> |
| 2.1      | Die neue Rolle der IT .....                            | 7        |
| 2.2      | Trends und Treiber .....                               | 8        |
| 2.2.1    | Wertbeitrag von IT .....                               | 8        |
| 2.2.2    | Business-IT-Alignment .....                            | 13       |
| 2.2.3    | Compliance .....                                       | 16       |
| 2.2.4    | Risikomanagement .....                                 | 18       |
| 2.2.5    | Prozess- und Serviceorientierung .....                 | 18       |
| 2.3      | Geschäftsarchitektur für IT-Governance .....           | 20       |
| 2.4      | IT-Governance: Begriff und Aufgaben .....              | 22       |
| 2.5      | Unterstützende Referenzmodelle .....                   | 25       |
| 2.6      | Akzeptanz von IT-Governance .....                      | 27       |
| 2.6.1    | Weltweite Untersuchungen .....                         | 27       |
| 2.6.2    | Ergebnisübersicht .....                                | 28       |
| 2.6.3    | Die Ergebnisse der ITGI-Studie .....                   | 30       |
| 2.6.3.1  | Bedeutung der IT .....                                 | 30       |
| 2.6.3.2  | Problembereiche der IT .....                           | 32       |
| 2.6.3.3  | Stand der Umsetzung von IT-Governance .....            | 33       |
| 2.6.3.4  | Nutzungsgrad der Referenzmodelle und<br>Methoden ..... | 37       |
| 2.6.3.5  | Bekanntheitsgrad und Bedeutung von COBIT .....         | 38       |

|          |  |           |
|----------|--|-----------|
| <b>3</b> | <b>Das COBIT-Referenzmodell</b>                                | <b>41</b> |
| 3.1      | Einleitung und Übersicht                                       | 42        |
| 3.1.1    | Entstehung und Geschichte                                      | 42        |
| 3.1.2    | Zielsetzungen und Zielgruppen                                  | 43        |
| 3.1.3    | (Basis-)Referenzmodelle und Standards                          | 46        |
| 3.1.4    | Die COBIT-IT-Governance-Perspektive                            | 48        |
| 3.1.4.1  | IT-Governance-Grundverständnis                                 | 48        |
| 3.1.4.2  | IT-Governance-Prozess  | 48        |
| 3.2      | COBIT-Merkmale   | 49        |
| 3.2.1    | Best Practices   | 49        |
| 3.2.2    | Geschäftsorientierung (Business-focused)                       | 51        |
| 3.2.3    | Prozessorientierung (Process-oriented)                         | 52        |
| 3.2.4    | Steuerungs- und Kontrollorientierung (Control-based)           | 53        |
| 3.2.5    | Messung von Leistungen und Risiken<br>(Measurement-driven)     | 55        |
| 3.3      | COBIT-Komponenten  | 56        |
| 3.3.1    | Der COBIT-Informationsraum                                     | 56        |
| 3.3.2    | Kontrollziele  | 57        |
| 3.3.3    | IT-Ressourcen  | 59        |
| 3.3.4    | Informationskriterien  | 60        |
| 3.3.5    | Domänen und IT-Prozesse  | 61        |
| 3.3.5.1  | Planung und Organisation (PO)                                  | 61        |
| 3.3.5.2  | Beschaffung und Implementierung (AI)                           | 62        |
| 3.3.5.3  | Lieferung und Unterstützung (DS)                               | 63        |
| 3.3.5.4  | Überwachung und Evaluierung (ME)                               | 64        |
| 3.3.5.5  | Relevanz der IT-Prozesse für die<br>IT-Governance-Kernbereiche | 65        |
| 3.3.6    | Interdependenzen im COBIT-Informationsraum                     | 68        |
| 3.3.7    | Ziele, Erfolgsmessung und IT-Geschäftsarchitektur              | 71        |
| 3.3.7.1  | Zielarten und Metriken im Überblick                            | 71        |
| 3.3.7.2  | Geschäftsziele   | 71        |
| 3.3.7.3  | IT-Ziele   | 72        |
| 3.3.7.4  | IT-Ziele und IT-Prozesse                                       | 75        |
| 3.3.7.5  | IT-Ziele, Prozess- und Aktivitätsziele                         | 76        |
| 3.3.7.6  | IT-Ziele und IT-Geschäftsarchitektur                           | 78        |

|         |   |     |
|---------|---|-----|
| 3.3.8   | Controls .....  | 79  |
| 3.3.8.1 | Controls der Geschäftsprozesse<br>(Business Process Controls) ..... | 80  |
| 3.3.8.2 | Controls der Applikationen<br>(Application Controls) .....          | 81  |
| 3.3.8.3 | IT-Management-Controls (IT-General-Controls) ...                    | 83  |
| 3.3.8.4 | Wirkungsbereich der Controls .....                                  | 84  |
| 3.3.8.5 | Controls im Outsourcing (Process Controls) .....                    | 86  |
| 3.3.9   | Das COBIT-Reifegradmodell .....                                     | 87  |
| 3.4     | Das COBIT-Gesamtmodell .....  | 91  |
| 3.4.1   | Makrostruktur:<br>Prozessorientierte Anordnung der Domänen .....    | 91  |
| 3.4.2   | Mikrostruktur: Der Aufbau der IT-Prozesse .....                     | 93  |
| 3.4.2.1 | Prozessbeschreibung .....   | 93  |
| 3.4.2.2 | Kontrollziele .....   | 96  |
| 3.4.2.3 | Management-Richtlinien .....  | 97  |
| 3.4.2.4 | Maturitätsmodell .....  | 100 |
| 3.4.3   | Funktionalität der IT-Prozesse .....                                | 101 |
| 3.5     | COBIT-Produkte .....  | 103 |
| 3.5.1   | Überblick .....   | 103 |
| 3.5.2   | Implementierung von IT-Governance .....                             | 104 |
| 3.5.3   | Der IT Assurance Guide .....  | 110 |
| 3.5.4   | Control Practices .....   | 118 |
| 3.5.5   | COBIT-Quickstart .....  | 120 |
| 3.5.6   | COBIT-Online .....  | 122 |
| 3.6     | COBIT und COSO .....  | 122 |
| 3.7     | COBIT in der Umsetzung des Sarbanes-Oxley Act .....                 | 126 |
| 3.7.1   | Der Sarbanes-Oxley Act (SOX) .....                                  | 126 |
| 3.7.2   | Herstellung von SOX-Compliance .....                                | 128 |
| 3.7.2.1 | Vorgehensweise .....  | 129 |
| 3.7.2.2 | Planung und Eingrenzung der Controls .....                          | 130 |
| 3.7.2.3 | Bewertung der Risiken .....   | 132 |
| 3.7.2.4 | Dokumentation der Controls .....                                    | 134 |
| 3.7.2.5 | Evaluierung der Effektivität der Controls .....                     | 137 |
| 3.8     | Zertifizierung und Qualifizierung .....                             | 139 |
| 3.9     | Einordnung und Bewertung .....                                      | 139 |

|          |  |            |
|----------|--|------------|
| <b>4</b> | <b>Das Val-IT-Referenzmodell</b>                           | <b>143</b> |
| 4.1      | Überblick .....  | 143        |
| 4.2      | Zielsetzung von Val IT .....                               | 144        |
| 4.3      | Abgrenzung zu COBIT .....                                  | 145        |
| 4.4      | Aufbau und Komponenten des Val-IT-Frameworks .....         | 146        |
| 4.4.1    | Val-IT-Prinzipien .....                                    | 146        |
| 4.4.2    | Domänen und Prozesse in Val IT .....                       | 147        |
| 4.4.3    | Die Prozessbeschreibungen in Val IT .....                  | 148        |
| 4.4.4    | Reifegradmodelle .....                                     | 150        |
| 4.5      | Der Business Case .....                                    | 150        |
| 4.5.1    | Ziele, Nutzen und Aufgaben .....                           | 150        |
| 4.5.2    | Komponenten des Business Case .....                        | 152        |
| 4.5.3    | Entwicklung und Wartung .....                              | 153        |
| 4.5.3.1  | Schritt 1: Faktensammlung .....                            | 154        |
| 4.5.3.2  | Schritt 2: Alignment .....                                 | 155        |
| 4.5.3.3  | Schritt 3: Finanzanalyse I .....                           | 156        |
| 4.5.3.4  | Schritt 4: Analyse nichtfinanzieller<br>Auswirkungen ..... | 158        |
| 4.5.3.5  | Schritt 5: Risiken .....                                   | 158        |
| 4.5.3.6  | Schritt 6: Risikooptimierung .....                         | 160        |
| 4.5.3.7  | Schritt 7: Dokumentation .....                             | 161        |
| 4.5.3.8  | Schritt 8: Wartung .....                                   | 163        |
| 4.6      | Einordnung und Bewertung .....                             | 163        |
| <b>5</b> | <b>Das Risk-IT-Referenzmodell (Risk IT)</b>                | <b>165</b> |
| 5.1      | Einleitung und Zielsetzung .....                           | 165        |
| 5.2      | Adressaten und deren spezifischer Nutzen .....             | 166        |
| 5.3      | Aufbau des Risk-IT-Referenzmodells .....                   | 167        |
| 5.3.1    | Prinzipien von Risk IT .....                               | 168        |
| 5.3.2    | Risk-IT-Domänen .....                                      | 169        |
| 5.3.2.1  | Risiko-Governance (Risk Governance) .....                  | 170        |
| 5.3.2.2  | Risikoanalyse und -bewertung<br>(Risk Evaluation) .....    | 173        |
| 5.3.2.3  | Risikoreaktion (Risk Response) .....                       | 175        |

|          |  |            |
|----------|--|------------|
| 5.3.3    | Das Risk-IT-Prozessmodell .....                              | 178        |
| 5.3.3.1  | Domänenziel und Domänenmetriken .....                        | 180        |
| 5.3.3.2  | Prozessübersicht und Prozessdetails .....                    | 180        |
| 5.3.3.3  | Management-Richtlinien .....                                 | 182        |
| 5.3.3.4  | Domänen-Reifegradmodell<br>(Domain Maturity Model) .....     | 184        |
| 5.4      | Weitere Produkte in Risk IT .....                            | 185        |
| 5.5      | Einordnung und Bewertung .....                               | 187        |
| <b>6</b> | <b>Weitere IT-Governance-Referenzmodelle</b>                 | <b>189</b> |
| 6.1      | Der Standard ISO/IEC 38500: Corporate Governance of IT ..... | 189        |
| 6.1.1    | Einleitung und Übersicht .....                               | 189        |
| 6.1.2    | Zielsetzung und grundlegendes Verständnis .....              | 190        |
| 6.1.3    | Zielgruppen .....  | 191        |
| 6.1.4    | Komponenten des Standards .....                              | 192        |
| 6.1.5    | Modell der Corporate Governance der IT .....                 | 193        |
| 6.1.6    | Zusammenhang mit COBIT .....                                 | 194        |
| 6.1.7    | Schlussbemerkungen .....                                     | 195        |
| 6.2      | Das ITIL-Referenzmodell .....                                | 196        |
| 6.2.1    | Einleitung und Übersicht .....                               | 196        |
| 6.2.1.1  | Entstehung und Geschichte .....                              | 196        |
| 6.2.1.2  | Ziele, Merkmale und Zielgruppen .....                        | 198        |
| 6.2.1.3  | Serviceorientierung .....                                    | 200        |
| 6.2.1.4  | Struktur von ITIL .....                                      | 201        |
| 6.2.2    | Band I: Service Strategy .....                               | 203        |
| 6.2.2.1  | Financial Management .....                                   | 204        |
| 6.2.2.2  | Service Portfolio Management .....                           | 205        |
| 6.2.2.3  | Demand Management .....                                      | 208        |
| 6.2.3    | Band II: Service Design .....                                | 208        |
| 6.2.3.1  | Service Catalogue Management .....                           | 210        |
| 6.2.3.2  | Service Level Management .....                               | 211        |
| 6.2.3.3  | Capacity Management .....                                    | 211        |
| 6.2.3.4  | Availability Management .....                                | 212        |
| 6.2.3.5  | IT Service Continuity Management .....                       | 212        |
| 6.2.3.6  | Information Security Management) .....                       | 213        |
| 6.2.3.7  | Supplier Management .....                                    | 213        |

|         |  |     |
|---------|--|-----|
| 6.2.4   | Band III: Service Transition .....               | 215 |
| 6.2.4.1 | Transition Planning and Support .....            | 215 |
| 6.2.4.2 | Change Management .....                          | 216 |
| 6.2.4.3 | Service Asset and Configuration Management ..... | 216 |
| 6.2.4.4 | Release und Deployment Management .....          | 218 |
| 6.2.4.5 | Service Validation and Testing .....             | 218 |
| 6.2.4.6 | Evaluation .....                                 | 220 |
| 6.2.4.7 | Knowledge Management .....                       | 221 |
| 6.2.5   | Band IV: Service Operation .....                 | 221 |
| 6.2.5.1 | Service Desk .....                               | 222 |
| 6.2.5.2 | Event Management .....                           | 222 |
| 6.2.5.3 | Incident Management .....                        | 224 |
| 6.2.5.4 | Request Fulfilment .....                         | 224 |
| 6.2.5.5 | Access Management .....                          | 225 |
| 6.2.5.6 | Problem Management .....                         | 225 |
| 6.2.6   | Band V: Continual Service Improvement .....      | 226 |
| 6.2.7   | ITIL-Zertifizierung .....                        | 227 |
| 6.2.8   | Einordnung und Bewertung .....                   | 228 |
| 6.3     | ISO/IEC 20000 .....                              | 229 |
| 6.3.1   | Ziele und Zielgruppen .....                      | 229 |
| 6.3.2   | Struktur von ISO/IEC 20000 .....                 | 231 |
| 6.3.2.1 | Prozessgruppen .....                             | 231 |
| 6.3.2.2 | Bestandteile des Standards .....                 | 232 |
| 6.3.2.3 | Zertifizierung .....                             | 234 |
| 6.3.2.4 | Vor- und Nachteile .....                         | 234 |
| 6.3.2.5 | Einordnung und Bewertung .....                   | 235 |
| 6.4     | Informationssicherheitsmanagement .....          | 236 |
| 6.4.1   | Sicherheitsstandards .....                       | 236 |
| 6.4.1.1 | Der Standard ISO/IEC 13335 .....                 | 238 |
| 6.4.1.2 | Der Standard ISO/IEC 17799 .....                 | 238 |
| 6.4.1.3 | Der Standard ISO/IEC 27001 .....                 | 239 |
| 6.4.1.4 | Die Standardfamilie ISO/IEC 27000 .....          | 240 |
| 6.4.2   | Einordnung und Bewertung .....                   | 241 |
| 6.5     | CMMI .....                                       | 242 |
| 6.5.1   | Einleitung und Übersicht .....                   | 242 |
| 6.5.2   | Aufbau und Komponenten .....                     | 244 |
| 6.5.3   | Fähigkeits- und Reifegrade .....                 | 248 |
| 6.5.4   | Einordnung und Bewertung .....                   | 251 |



|          |   |            |
|----------|---|------------|
| <b>7</b> | <b>Vergleich und Integration von Referenzmodellen</b>                                 | <b>253</b> |
| 7.1      | Einleitung und Übersicht  | 253        |
| 7.2      | Vergleich der Referenzmodelle   | 255        |
| 7.2.1    | Vergleich mittels zweidimensionaler Matrizen  | 255        |
| 7.2.2    | Vergleich mittels Merkmalkatalogen  | 257        |
| 7.2.2.1  | Vergleich nach Walter/Krcmar  | 257        |
| 7.2.2.2  | Vergleich nach Hochstein/Hunziker   | 259        |
| 7.3      | Kombination und Integration der Referenzmodelle                                       | 262        |
| 7.3.1    | Abgleich von COBIT, ITIL V3 und ISO/IEC 27002   | 262        |
| 7.3.2    | Das Integrationsprojekt COBIT Mapping   | 266        |
| 7.4      | Bewertung   | 272        |
| <b>8</b> | <b>SOA- und Cloud-Computing-Governance</b>  | <b>273</b> |
| 8.1      | Einleitung und Übersicht  | 273        |
| 8.2      | SOA-Governance  | 275        |
| 8.2.1    | Merkmale und Nutzen serviceorientierter Architekturen                                 | 275        |
| 8.2.2    | Governance-Herausforderung SOA  | 276        |
| 8.2.3    | SOA-Governance-Aufgabenbereiche   | 279        |
| 8.2.4    | SOA-Conformance   | 281        |
| 8.2.5    | SOA-Lifecycle-Management  | 282        |
| 8.2.6    | Ein Maturitätsmodell für die SOA-Governance   | 283        |
| 8.2.7    | SOA-Governance-Infrastruktur  | 286        |
| 8.3      | Cloud-Computing-Governance  | 288        |
| 8.3.1    | Merkmale und Nutzen des Cloud Computing   | 289        |
| 8.3.2    | Cloud Computing als Governance-Herausforderung  | 291        |
| 8.3.3    | Aufgabenbereiche der Cloud-Computing-Governance                                       | 295        |
| 8.4      | Service-Governance als gemeinsame Aufgabenstellung                                    | 296        |
| <b>9</b> | <b>Praxisbeispiel:<br/>Prüfung und Bewertung eines Governance-Konzepts für die IT</b> | <b>299</b> |
| 9.1      | Ausgangssituation und Motivation  | 299        |
| 9.2      | Methodische Aspekte einer Prüfung   | 302        |
| 9.2.1    | Grundlagen für die geplanten Prüfungshandlungen                                       | 302        |
| 9.2.2    | IT-Governance-Konzept als Gegenstand der Prüfung                                      | 303        |

|           |   |            |
|-----------|---|------------|
| 9.2.3     | Definition der Kriterien für die Prüfung .....      | 306        |
| 9.2.3.1   | Vollständigkeit .....                               | 307        |
| 9.2.3.2   | Eignung .....                                       | 309        |
| 9.2.3.3   | Konsistenz .....                                    | 310        |
| 9.2.3.4   | Umsetzbarkeit .....                                 | 311        |
| 9.2.4     | Referenzmodell für die IT-Governance .....          | 313        |
| 9.2.4.1   | Anforderungen an das Referenzmodell .....           | 313        |
| 9.2.4.2   | Vorarbeiten bei der Verwendung von COBIT .....      | 313        |
| 9.2.4.3   | Beispiel: Themen für CIO und Geschäftsleitung ....  | 316        |
| 9.2.4.4   | Darstellung und Interpretation der Ergebnisse ..... | 317        |
| 9.2.5     | Zeitlicher Ablauf und Aufwand für die Prüfung ..... | 318        |
| 9.2.6     | Ergebnisse und Nutzen für den Mandanten .....       | 319        |
| 9.3       | Zusammenfassung .....                               | 319        |
| <b>10</b> | <b>Schlussbetrachtung</b>                           | <b>321</b> |
|           | <b>Abkürzungsverzeichnis</b>                        | <b>323</b> |
|           | <b>Literaturverzeichnis</b>                         | <b>327</b> |
|           | <b>Index</b>  | <b>339</b> |