Inhalt

1 Einleitung 1
1.1 Gesetzliche und regulatorische Vorgaben 2
2 Bedeutung der IT-Sicherheit in Unternehmen 5
3 COBIT und BSI als Leitschnur der IT Sicherheit 13
4 ‚Grundgesetz' der IT Sicherheit 19
4.1 Regelungsziele nach Cobit 19
4.1.1 Planung und Organisation 20
4.1.2 Monitoring 23
4.2 Vorschlag für eine IT Sicherheitspolicy 24
4.2.1 Vorbemerkung und Einführung 25
4.2.2 Übergeordnete Aspekte 26
4.2.3 Infrastruktur 37
4.2.4 IT-Systeme 39
4.2.5 Netze 44
4.2.6 IT-Anwendungen 48
5 Schutz von Daten 53
5.1 Regelungsziele nach Cobit 53
5.1.1 Planung und Organisation 54
5.1.2 Delivery & Support 54
5.1.3 Monitoring 56
5.2 Vorschlag für eine Datenschutzrichtlinie 56
5.2.1 Geltungsbereich 57
5.2.2 Begriffsbestimmung und Eingrenzung 57
5.2.3 Ziele des Datenschutzes im Unternehmen 58
5.2.4 Verankerung des Datenschutzes in der Organisation 58
5.2.5 Grundsätze des Datenschutzes 60
5.3 Vorschlag für eine Richtlinie zum Schutz von Unternehmensdaten 63
5.3.1 Datenschutz 63
5.3.2 Authentikation 67
5.3.3 Verschlüsselung 69
5.3.4 Datensicherung und Archivierung 73
5.4 Hinweise für ein Datensicherungskonzept 78
5.4.1 Definitionen 78
5.4.2 Gefährdungslage 78
5.4.3 Regelungsbedarfe je IT-System 78
5.4.4 Datensicherungsplan je IT-System 80
5.4.5 Minimaldatensicherungskonzept 81
5.4.6 Verpflichtung der Mitarbeiter zur Datensicherung 81
5.4.7 Sporadische Restaurierungsübungen 82

6 Sicherheitsmanagement 83
6.1 Regelungsziele nach Cobit 83
6.1.1 Prozess und Organisation 84
6.1.2 Akquisition und Implementierung 88
6.1.3 Delivery & Support 89
6.1.4 Monitoring 91
6.2 Vorschlag für eine Richtlinie zum Sicherheitsmanagement 93
6.2.1 Vorbemerkung und Einführung 94
6.2.2 Rollen und Verantwortlichkeiten 95
6.2.3 Änderungsmanagement 97
6.2.4 Notfallmanagement 98
6.2.5 IT-Sicherheitsziele des Unternehmens 99
6.2.6 IT-Sicherheitskonzept des Unternehmens 101
6.2.7 Sicherheitsmanagementprozess des Unternehmens 104
6.2.8 IT-Strukturanalyse 104
6.2.9 Schutzbedarfsfeststellung 108
6.2.10 Sicherheitsanalyse und Formulierung zielführender Sicherheitsmaßnahmen 112
6.2.11 IT-Sicherheitsreporting an das Management 113
6.2.12 Verhaltensweisen zu Sicherheitsvorfällen 113

7 IT Betrieb 115
7.1 Regelungsziele nach Cobit 115
7.1.1 Planung & Organisation 115
7.1.2 Akquisition & Implementierung 121
7.1.3 Delivery & Support 123
7.1.4 Monitoring 129
7.2 Vorschlag für eine Richtlinie zum Sicheren IT Betrieb 129
7.2.1 Vorbemerkung und Einführung 129
7.2.2 Gebäudesicherheit 130
7.2.3 Organisation und Governance 135
7.2.4 Regelungen zu Zutritt, Zugang, Zugriff 144
7.2.5 Hardware- und Softwareeinsatz 157
7.2.6 Sichere technische Infrastruktur 167
7.2.7 Regelmässige Kontrollmassnahmen 188
7.2.8 Datensicherung und Archivierung 197
7.2.9 Schutz gegen Angriffe 199
7.2.10 Dokumentation 202
7.2.11 Schulung und Training 208
7.2.12 Ergänzende allgemeine Sicherheitsrichtlinien 210

8 IT Systeme 215
8.1 Regelungsziele nach Cobit 215
8.1.1 Planung & Organisation 216
8.1.2 Akquisition & Implementierung 218
8.1.3 Delivery & Support 221
8.1.4 Monitoring 223

8.2 Vorschlag für eine Richtlinie zu IT Systemen 223
8.2.1 Vorbemerkung und Einführung 224
8.2.2 Allgemeine Sicherheitsrichtlinien 224
8.2.3 User Management 227
8.2.4 Server 229
8.2.5 Client 231
8.2.6 Mobile Systeme 233
8.2.7 Externer Zugang 234
8.2.8 Lotus Notes/Domino 234
8.2.9 Webserver 238
8.2.10 Novell 239
8.2.11 Windows XP 242
8.2.12 Windows 247
8.2.13 Windows Server 2003 248
8.2.14 Unix 251
8.2.15 Aktive Netzwerkkomponenten 254
8.2.16 Paketfilter & Proxy 258
8.2.17 Datenbanken 261
8.2.18 SAP 262
8.2.19 Drucker 265
8.2.20 Samba 266
8.2.21 Verzeichnisdienst 266
8.2.22 VPN 269
8.3 Vertiefende Detailregelungen in Arbeitsanweisungen .. 270

9 Verankerung der IT Sicherheit in der Organisation 277
9.1 Regelungsziele nach Cobit 277
9.1.1 Planung und Organisation 277
9.1.2 Delivery & Support 280
9.2 Vorschlag für eine Richtlinie zur IT Organisation 281
9.2.1 Schulung und Training 281

10 Service Management 285
10.1 Regelungsziele nach Cobit 285
10.1.1 Planung und Organisation 285
10.1.2 Akquisition und Implementierung 287
10.1.3 Delivery & Support 295
10.2 Vorschlag für eine Service Management Richtlinie 297
10.2.1 Vorbemerkung und Einführung 298
10.2.2 Incident Management 299
10.2.3 Problem Management 302
10.2.4 Change Management 306
10.2.5 Release Management 314
10.2.6 Configuration Management 321

11 IT Continuity Planung 331
11.1 Regelungsziele nach Cobit 331
11.1.1 Planung und Organisation 331
11.1.2 Delivery & Support 332

11.2 Vorschlag für eine IT Continuity Richtlinie 334
11.2.1 Grundlegende Maßnahmen zur IT Continuity Planung 334
11.2.2 Ziele der IT Continuity Planung 340
11.2.3 Abgrenzung 341
11.2.4 Gegenstand dieser Richtlinie 342
11.2.5 Planung der IT Continuity 344
11.2.6 Contingency Management 345
11.2.7 Prozesse der IT Continuity 345
11.2.8 Organisation der IT Continuity 346
11.2.9 Umgebungswiederherstellung 348
11.2.10 Funktionale Wiederherstellung 352