Inhaltsverzeichnis

Vorwort 5
Vorbemerkung 7

1 Einleitung
1.1 Versionshistorie 19
1.2 Zielsetzung 19
1.3 Adressatenkreis 20
1.4 Anwendungsweise 21

2 Einführung in die Informationssicherheit
2.1 Überblick über Normen und Standards zur Informationssicherheit 22
2.1.1 ISO-Normen zur Informationssicherheit 23
2.1.2 Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit 24
2.1.3 Weitere Sicherheitsstandards 28

3 ISMS-Definition und Prozessbeschreibung 30
3.1 Komponenten eines Managementsystems für Informationssicherheit 30
3.2 Prozessbeschreibung und Lebenszyklus-Modell 32
3.2.1 Der Lebenszyklus in der Informationssicherheit 32
3.2.2 Beschreibung des Prozesses Informationssicherheit 33

4 Management-Prinzipien 35
4.1 Aufgaben und Pflichten des Managements 35
4.2 Kommunikation und Wissen 37
4.3 Erfolgskontrolle im Sicherheitsprozess 40
4.4 Kontinuierliche Verbesserung des Sicherheitsprozesses 41

5 Ressourcen für Informationssicherheit 42

6 Einbindung der Mitarbeiter in den Sicherheitsprozess 43

7 Der Sicherheitsprozess 44
7.1 Planung des Sicherheitsprozesses 44
7.2 Aufbau einer Sicherheitsorganisation [DOK] 46
7.3 Umsetzung der Leitlinie zur Informationssicherheit 46
7.4 Aufrechterhaltung der Informationssicherheit 47
7.5 Kontinuierliche Verbesserung der Informationssicherheit 48

8 Sicherheitskonzept 49
8.1 Erstellung des Sicherheitskonzepts 49

8.2 Umsetzung des Sicherheitskonzepts ... 53
8.3 Erfolgskontrolle des Sicherheitskonzepts ... 53
8.4 Kontinuierliche Verbesserung des Sicherheitskonzepts ... 55

9 Zertifizierung des ISMS ... 57

10 Das ISMS auf Basis von BSI IT-Grundschutz ... 58
10.1 IT-Grundschutz-Methodik ... 58
10.2 Der Sicherheitsprozess nach IT-Grundschutz ... 59
10.2.1 Integrierte Risikobewertung im IT-Grundschutz ... 59
10.2.2 Sicherheitskonzeption ... 62

11 Anhang ... 66
11.1 Literaturverzeichnis ... 66

1 Einleitung ... 71
1.1 Versionshistorie ... 71
1.2 Zielsetzung ... 71
1.3 Adressatenkreis ... 72
1.4 Anwendungsweise ... 73
1.5 Aufbau des BSI-Standards 200-2 ... 73

2 Informationssicherheitsmanagement mit IT-Grundschutz 76
2.1 Ganzheitliches Konzept ... 76
2.2 Managementsystem für die Informationssicherheit ... 76
2.3 Verantwortung für die Informationssicherheit ... 77
2.4 Elemente des IT-Grundschutzes ... 78
2.5 Thematische Abgrenzung ... 79
2.6 Übersicht über den Informationssicherheitsprozess ... 80
2.7 Anwendung des IT-Grundschutz-Kompendiums ... 83

3 Initiierung des Sicherheitsprozesses 86
3.1 Übernahme von Verantwortung durch die Leitungsebene ... 86
3.2 Konzeption und Planung des Sicherheitsprozesses ... 87
3.2.1 Ermittlung von Rahmenbedingungen ... 87
3.2.2 Formulierung von allgemeinen Informationssicherheitszielen ... 90
3.2.3 Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse ... 91
3.2.4 Ersterfassung der Prozesse, Anwendungen und IT-Systeme ... 93
3.3 Entscheidung für Vorgehensweise ... 95
3.3.1 Basis-Absicherung ... 96
3.3.2 Kern-Absicherung ... 96

3.3.3 Standard-Absicherung ... 97
3.3.4 Festlegung des Geltungsbereichs ... 98
3.3.5 Managemententscheidung ... 99
3.4 Erstellung einer Leitlinie zur Informationssicherheit ... 100
3.4.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie ... 101
3.4.2 Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie 101
3.4.3 Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie 101
3.4.4 Bekanntgabe der Sicherheitsleitlinie ... 102
3.4.5 Aktualisierung der Sicherheitsleitlinie ... 103

4 Organisation des Sicherheitsprozesses ... 104
4.1 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse ... 104
4.2 Aufbau der Informationssicherheitsorganisation ... 105
4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation ... 107
4.4 Der Informationssicherheitsbeauftragte ... 108
4.5 Das IS-Management-Team ... 111
4.6 Bereichs- und Projekt-Sicherheitsbeauftragte bzw. Beauftragter für IT-Sicherheit ... 112
4.7 Der ICS-Informationssicherheitsbeauftragte (ICS-ISB) ... 113
4.8 IS-Koordinierungsausschuss ... 115
4.9 Der Datenschutzbeauftragte ... 116
4.10 Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen ... 117
4.11 Einbindung externer Sicherheitsexperten ... 119

5 Dokumentation im Sicherheitsprozess ... 121
5.1 Klassifikation von Informationen ... 121
5.2 Informationsfluss im Informationssicherheitsprozess ... 124
5.2.1 Berichte an die Leitungsebene ... 124
5.2.2 Dokumentation im Informationssicherheitsprozess ... 125
5.2.3 Anforderungen an die Dokumentation ... 127
5.2.4 Informationsfluss und Meldewege ... 129

6 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-Absicherung ... 131
6.1 Festlegung des Geltungsbereichs für die Basis-Absicherung ... 132
6.2 Auswahl und Priorisierung für die Basis-Absicherung ... 132
6.2.1 Modellierung nach IT-Grundschutz ... 133
6.2.2 Reihenfolge der Baustein-Umsetzung ... 133
6.2.3 Zuordnung von Bausteinen ... 133
6.2.4 Ermittlung konkreter Maßnahmen aus Anforderungen ... 134
6.3 IT-Grundschutz-Check für Basis-Absicherung ... 134
6.4 Realisierung ... 136
6.5 Auswahl einer folgenden Vorgehensweise ... 137

7 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Kern-Absicherung ... 138
7.1 Die Methodik der Kern-Absicherung ... 139
7.2 Festlegung des Geltungsbereichs für die Kern-Absicherung ... 140
7.3 Identifikation und Festlegung der kritischen Assets (Kronjuwelen) ... 140
7.4 Strukturanalyse ... 142
7.5 Schutzbedarfsfeststellung ... 143
7.6 Modellierung: Auswahl und Anpassung von Anforderungen ... 144
7.7 IT-Grundschutz-Check ... 145
7.8 Risikoanalyse und weiterführende Sicherheitsmaßnahmen ... 145
7.9 Umsetzung und weitere Schritte ... 145

8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung ... 147
8.1 Strukturanalyse ... 150
8.1.1 Komplexitätsreduktion durch Gruppenbildung ... 151
8.1.2 Erfassung der Geschäftsprozesse und der zugehörigen Informationen ... 152
8.1.3 Erfassung der Anwendungen und der zugehörigen Informationen 153
8.1.4 Netzplanerhebung ... 159
8.1.5 Erhebung der IT-Systeme ... 163
8.1.6 Erhebung der ICS-Systeme ... 167
8.1.7 Erhebung sonstiger Geräte ... 169
8.1.8 Erfassung der Räume ... 172
8.2 Schutzbedarfsfeststellung ... 176
8.2.1 Definition der Schutzbedarfskategorien ... 176
8.2.2 Vorgehen bei der Schutzbedarfsfeststellung ... 181
8.2.3 Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen ... 183
8.2.4 Schutzbedarfsfeststellung für IT-Systeme ... 187
8.2.5 Schutzbedarfsfeststellung für ICS-Systeme ... 192
8.2.6 Schutzbedarfsfeststellung für sonstige Geräte ... 195
8.2.7 Schutzbedarfsfeststellung für Räume ... 197
8.2.8 Schutzbedarfsfeststellung für Kommunikationsverbindungen ... 199
8.2.9 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung ... 204
8.3 Modellierung eines Informationsverbunds ... 207
8.3.1 Das IT-Grundschutz-Kompendium ... 207
8.3.2 Modellierung eines Informationsverbunds: Auswahl von Bausteinen ... 209
8.3.3 Reihenfolge der Baustein-Umsetzung ... 212
8.3.4 Zuordnung von Bausteinen ... 213
8.3.5 Modellierung bei Virtualisierung und Cloud-Systemen ... 214
8.3.6 Anpassung der Baustein-Anforderungen ... 217

8.3.7 Einbindung externer Dienstleister ... 219
8.4 IT-Grundschutz-Check ... 220
8.4.1 Organisatorische Vorarbeiten für den IT-Grundschutz-Check ... 221
8.4.2 Durchführung des Soll-Ist-Vergleichs ... 224
8.4.3 Dokumentation der Ergebnisse ... 225
8.5 Risikoanalyse ... 227

9 Umsetzung der Sicherheitskonzeption ... 232
9.1 Sichtung der Untersuchungsergebnisse ... 232
9.2 Kosten- und Aufwandsschätzung ... 233
9.3 Festlegung der Umsetzungsreihenfolge der Maßnahmen ... 234
9.4 Festlegung der Aufgaben und der Verantwortung ... 236
9.5 Realisierungsbegleitende Maßnahmen ... 236

10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit ... 239
10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen ... 239
10.1.1 Überprüfung anhand von Kennzahlen ... 240
10.1.2 Bewertung des ISMS mithilfe eines Reifegradmodells ... 241
10.1.3 Überprüfung der Umsetzung der Sicherheitsmaßnahmen ... 242
10.1.4 Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz ... 243
10.2 Eignung der Informationssicherheitsstrategie ... 244
10.3 Übernahme der Ergebnisse in den Informationssicherheitsprozess ... 245

11 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz ... 247

12 Anhang ... 249
12.1 Erläuterungen zu den Schadensszenarien ... 249
12.2 Literaturverzeichnis ... 255

1 Einleitung ... 259
1.1 Versionshistorie ... 259
1.2 Zielsetzung ... 259
1.3 Abgrenzung, Begriffe und Einordnung in den IT-Grundschutz ... 260
1.4 Adressatenkreis ... 262
1.5 Anwendungsweise ... 262

2 Vorarbeiten zur Risikoanalyse ... 264

3 Übersicht über die elementaren Gefährdungen ... 268

4 Erstellung einer Gefährdungsübersicht 271
4.1 Ermittlung von elementaren Gefährdungen ... 271

4.2 Ermittlung zusätzlicher Gefährdungen ... 277
5 Risikoeinstufung ... 280
5.1 Risikoeinschätzung ... 280
5.2 Risikobewertung ... 281
6 Behandlung von Risiken ... 288
6.1 Risikobehandlungsoptionen ... 288
6.2 Risiken unter Beobachtung ... 290
7 Konsolidierung des Sicherheitskonzepts ... 294
8 Rückführung in den Sicherheitsprozess ... 297
9 Anhang ... 298
9.1 Risikoappetit (Risikobereitschaft) ... 298
9.1.1 Einflussfaktoren ... 298
9.1.2 Quantifizierung von Risikoneigung ... 299
9.1.3 Risikoneigung als Eingangsgröße im ISMS ... 304
9.1.4 Auswirkung von Gesetzen und Regularien ... 305
9.2 Moderation der Risikoanalyse ... 306
9.3 Ermittlung zusätzlicher Gefährdungen ... 307
9.4 Zusammenspiel mit ISO/IEC 31000 ... 308
9.5 Literaturverzeichnis ... 311
Glossar ... 313