



Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz Arbeitshandbuch

DIN ISO/IEC 27001 DIN ISO/IEC 27002

BSI-Standards 200-1/2/3

2., aktualisierte Auflage 2017



Bundesanzeiger
Verlag

Inhaltsverzeichnis

Vorwort	5
Einführung	11
Interview zum neuen IT-Grundschutz mit Holger Schildt und Isabel Münch	13
Hinweis des Verlages (2. Auflage)	23

Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementssysteme – Anforderungen

DIN EN ISO/IEC 27001:2017-06	25
------------------------------------	----

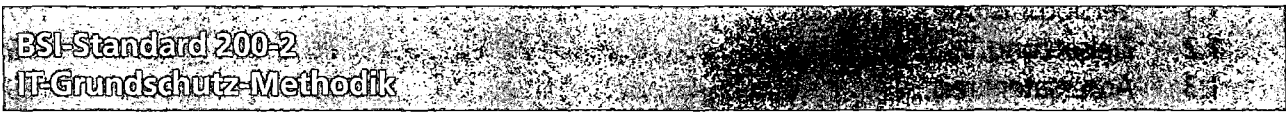
Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen

DIN EN ISO/IEC 27002:2017-06	63
------------------------------------	----

BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)

1 Einleitung	
1.1 Versionshistorie	177
1.2 Zielsetzung	179
1.3 Adressatenkreis	179
1.4 Anwendungsweise	179
2 Einführung in die Informationssicherheit	
2.1 Überblick über Normen und Standards zur Informationssicherheit	182
2.1.1 ISO-Normen zur Informationssicherheit	183
2.1.2 Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit	184
2.1.3 Weitere Sicherheitsstandards	187
3 ISMS-Definition und Prozessbeschreibung	189
3.1 Komponenten eines Managementsystems für Informationssicherheit	189
3.2 Prozessbeschreibung und Lebenszyklus-Modell	191
3.2.1 Der Lebenszyklus in der Informationssicherheit	191

3.2.2	Beschreibung des Prozesses Informationssicherheit.	192
4	Management-Prinzipien	194
4.1	Aufgaben und Pflichten des Managements.	194
4.2	Kommunikation und Wissen	196
4.3	Erfolgskontrolle im Sicherheitsprozess.	198
4.4	Kontinuierliche Verbesserung des Sicherheitsprozesses.	199
5	Ressourcen für Informationssicherheit	200
6	Einbindung der Mitarbeiter in den Sicherheitsprozess	201
7	Der Sicherheitsprozess	202
7.1	Planung des Sicherheitsprozesses	202
7.2	Aufbau einer Sicherheitsorganisation [DOK]	204
7.3	Umsetzung der Leitlinie zur Informationssicherheit.	204
7.4	Aufrechterhaltung der Informationssicherheit.	204
7.5	Kontinuierliche Verbesserung der Informationssicherheit	205
8	Sicherheitskonzept	206
8.1	Erstellung des Sicherheitskonzepts	206
8.2	Umsetzung des Sicherheitskonzepts	210
8.3	Erfolgskontrolle des Sicherheitskonzepts.	210
8.4	Kontinuierliche Verbesserung des Sicherheitskonzepts	212
9	Zertifizierung des ISMS	213
10	Das ISMS auf Basis von BSI IT-Grundschutz	214
10.1	IT-Grundschutz-Methodik	214
10.2	Der Sicherheitsprozess nach IT-Grundschutz	214
10.2.1	Integrierte Risikobewertung im IT-Grundschutz.	215
10.2.2	Sicherheitskonzeption	217
11	Anhang	221
11.1	Literaturverzeichnis	221



1	Einleitung	225
1.1	Versionshistorie	335
1.2	Zielsetzung.	225
1.3	Adressatenkreis	226
1.4	Anwendungsweise	227
1.5	Aufbau des BSI-Standards 200-2.	228
2	Informationssicherheitsmanagement mit IT-Grundschutz	229
2.1	Ganzheitliches Konzept.	229
2.2	Managementsystem für die Informationssicherheit.	229
2.3	Verantwortung für die Informationssicherheit.	230
2.4	Elemente des IT-Grundschutzes	230

2.5	Thematische Abgrenzung	232
2.6	Übersicht über den Informationssicherheitsprozess	232
2.7	Anwendung des IT-Grundschutz-Kompendiums	235
3	Initiierung des Sicherheitsprozesses	238
3.1	Übernahme von Verantwortung durch die Leitungsebene	238
3.2	Konzeption und Planung des Sicherheitsprozesses	239
3.2.1	Ermittlung von Rahmenbedingungen	239
3.2.2	Formulierung von allgemeinen Informationssicherheitszielen	241
3.2.3	Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse	242
3.2.4	Ersterfassung der Prozesse, Anwendungen und IT-Systeme	244
3.3	Entscheidung für Vorgehensweise	246
3.3.1	Basis-Absicherung	247
3.3.2	Kern-Absicherung	247
3.3.3	Standard-Absicherung	248
3.3.4	Festlegung des Geltungsbereichs	248
3.3.5	Managemententscheidung	249
3.4	Erstellung einer Leitlinie zur Informationssicherheit	250
3.4.1	Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie	251
3.4.2	Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie	251
3.4.3	Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie	251
3.4.4	Bekanntgabe der Sicherheitsleitlinie	252
3.4.5	Aktualisierung der Sicherheitsleitlinie	253
4	Organisation des Sicherheitsprozesses	254
4.1	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	254
4.2	Aufbau der Informationssicherheitsorganisation	255
4.3	Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation	257
4.4	Der Informationssicherheitsbeauftragte	258
4.5	Das IS-Management-Team	261
4.6	Bereichs- und Projekt-Sicherheitsbeauftragte bzw. Beauftragter für IT-Sicherheit	262
4.7	Der ICS-Informationssicherheitsbeauftragte (ICS-ISB)	263
4.8	IS-Koordinierungsausschuss	264
4.9	Der Datenschutzbeauftragte	265
4.10	Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen	267
4.11	Einbindung externer Sicherheitsexperten	268
5	Dokumentation im Sicherheitsprozess	270
5.1	Klassifikation von Informationen	270
5.2	Informationsfluss im Informationssicherheitsprozess	272
5.2.1	Berichte an die Leitungsebene	273
5.2.2	Dokumentation im Informationssicherheitsprozess	273
5.2.3	Anforderungen an die Dokumentation	275
5.2.4	Informationsfluss und Meldewege	277

6	Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-Absicherung	279
6.1	Festlegung des Geltungsbereichs für die Basis-Absicherung	280
6.2	Auswahl und Priorisierung für die Basis-Absicherung	280
6.2.1	Modellierung nach IT-Grundschutz	280
6.2.2	Reihenfolge der Baustein-Umsetzung	281
6.2.3	Zuordnung von Bausteinen	281
6.2.4	Ermittlung konkreter Maßnahmen aus Anforderungen	281
6.3	IT-Grundschutz-Check für Basis-Absicherung	282
6.4	Realisierung	284
6.5	Auswahl einer folgenden Vorgehensweise	284
7	Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Kern-Absicherung	286
7.1	Die Methodik der Kern-Absicherung	286
7.2	Festlegung des Geltungsbereichs für die Kern-Absicherung	287
7.3	Identifikation und Festlegung der kritischen Assets (Kronjuwelen)	288
7.4	Strukturanalyse	290
7.5	Schutzbedarfsfeststellung	290
7.6	Modellierung: Auswahl und Anpassung von Anforderungen	291
7.7	IT-Grundschutz-Check	292
7.8	Risikoanalyse und weiterführende Sicherheitsmaßnahmen	292
7.9	Umsetzung und weitere Schritte	292
8	Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung	294
8.1	Strukturanalyse	296
8.1.1	Komplexitätsreduktion durch Gruppenbildung	297
8.1.2	Erfassung der Geschäftsprozesse und der zugehörigen Informationen	298
8.1.3	Erfassung der Anwendungen und der zugehörigen Informationen	300
8.1.4	Netzplanerhebung	305
8.1.5	Erhebung der IT-Systeme	309
8.1.6	Erhebung der ICS-Systeme	313
8.1.7	Erhebung sonstiger Geräte	315
8.1.8	Erfassung der Räume	318
8.2	Schutzbedarfsfeststellung	322
8.2.1	Definition der Schutzbedarfskategorien	322
8.2.2	Vorgehen bei der Schutzbedarfsfeststellung	326
8.2.3	Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen	328
8.2.4	Schutzbedarfsfeststellung für IT-Systeme	332
8.2.5	Schutzbedarfsfeststellung für ICS-Systeme	337
8.2.6	Schutzbedarfsfeststellung für sonstige Geräte	339
8.2.7	Schutzbedarfsfeststellung für Räume	341
8.2.8	Schutzbedarfsfeststellung für Kommunikationsverbindungen	343
8.2.9	Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung	348
8.3	Modellierung eines Informationsverbunds	350
8.3.1	Das IT-Grundschutz-Kompendium	350
8.3.2	Modellierung eines Informationsverbunds: Auswahl von Bausteinen	352
8.3.3	Reihenfolge der Baustein-Umsetzung	355

8.3.4	Zuordnung von Bausteinen	356
8.3.5	Modellierung bei Virtualisierung und Cloud-Systemen	357
8.3.6	Anpassung der Baustein-Anforderungen	360
8.3.7	Einbindung externer Dienstleister	362
8.4	IT-Grundschutz-Check	363
8.4.1	Organisatorische Vorarbeiten für den IT-Grundschutz-Check	364
8.4.2	Durchführung des Soll-Ist-Vergleichs	368
8.4.3	Dokumentation der Ergebnisse	369
8.5	Risikoanalyse	370
9	Umsetzung der Sicherheitskonzeption	376
9.1	Sichtung der Untersuchungsergebnisse	376
9.2	Kosten- und Aufwandsschätzung	377
9.3	Festlegung der Umsetzungsreihenfolge der Maßnahmen	378
9.4	Festlegung der Aufgaben und der Verantwortung	379
9.5	Realisierungsbegleitende Maßnahmen	380
10	Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit	382
10.1	Überprüfung des Informationssicherheitsprozesses auf allen Ebenen	382
10.1.1	Überprüfung anhand von Kennzahlen	383
10.1.2	Bewertung des ISMS mithilfe eines Reifegradmodells	383
10.1.3	Überprüfung der Umsetzung der Sicherheitsmaßnahmen	385
10.1.4	Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz	386
10.2	Eignung der Informationssicherheitsstrategie	386
10.3	Übernahme der Ergebnisse in den Informationssicherheitsprozess	387
11	Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz	389
12	Anhang	391
12.1	Erläuterungen zu den Schadensszenarien	391
12.2	Literaturverzeichnis	396

BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz
--

1	Einleitung	401
1.1	Versionshistorie	401
1.2	Zielsetzung	401
1.3	Abgrenzung, Begriffe und Einordnung in den IT-Grundschutz	402
1.4	Adressatenkreis	404
1.5	Anwendungsweise	404
2	Vorarbeiten zur Risikoanalyse	405
3	Übersicht über die elementaren Gefährdungen	409
4	Erstellung einer Gefährdungsübersicht	412
4.1	Ermittlung von elementaren Gefährdungen	412
4.2	Ermittlung zusätzlicher Gefährdungen	419

5	Risikoeinstufung	422
5.1	Risikoeinschätzung	422
5.2	Risikobewertung	423
6	Behandlung von Risiken	429
6.1	Risikobehandlungsoptionen	429
6.2	Risiken unter Beobachtung	431
7	Konsolidierung des Sicherheitskonzepts	435
8	Rückführung in den Sicherheitsprozess	437
9	Anhang	438
9.1	Risikoappetit (Risikobereitschaft)	438
9.1.1	Einflussfaktoren	438
9.1.2	Quantifizierung von Risikoneigung	439
9.1.3	Risikoneigung als Eingangsgröße im ISMS	444
9.1.4	Auswirkung von Gesetzen und Regularien	445
9.2	Moderation der Risikoanalyse	445
9.3	Ermittlung zusätzlicher Gefährdungen	446
9.4	Zusammenspiel mit ISO/IEC 31000	447
9.5	Literaturverzeichnis	450
Glossar		451