

Inhaltsverzeichnis

1	Gesetze und Standards im Umfeld der Informationssicherheit.....	1
1.1	Corporate Governance und Risikomanagement.....	1
1.2	Die Bedeutung des öffentlichen Beschaffungsrechts.....	7
1.3	Standards zu Management-Systemen.....	9
1.4	Zertifizierfähige Modelle.....	16
1.5	Konkrete Standards zur IT-Sicherheit.....	19
2	Vergleich der Begrifflichkeiten.....	23
2.1	Organisation, Werte und Sicherheitsziele.....	24
2.2	Risiken und Analysen.....	27
2.3	Maßnahmenauswahl und Risikobehandlung.....	34
2.4	Sicherheitsdokumente.....	37
2.5	Übersetzungsprobleme bei der deutschen Ausgabe des Standards.....	41
3	Das ISMS nach ISO 27001.....	45
3.1	Das Modell des ISMS.....	45
3.2	PLAN: Das ISMS festlegen und verwalten.....	49
3.3	DO: Umsetzen und Durchführen des ISMS.....	67
3.4	CHECK: Überwachen und Überprüfen des ISMS.....	75
3.5	ACT: Pflegen und Verbessern des ISMS.....	81
3.6	Anforderungen an die Dokumentation.....	84
3.7	Dokumentenlenkung.....	88
3.8	Lenkung der Aufzeichnungen.....	92
3.9	Verantwortung des Managements.....	93
3.10	Interne ISMS-Audits.....	96
3.11	Managementbewertung des ISMS.....	98
3.12	Verbesserung des ISMS.....	101
3.13	Maßnahmenziele und Maßnahmen.....	103
4	Festlegung des Anwendungsbereichs und Überlegungen zum Management.....	109
4.1	Anwendungsbereich des ISMS zweckmäßig bestimmen.....	109
4.2	Das Management-Forum für Informationssicherheit.....	111

4.3	Verantwortlichkeiten für die Informationssicherheit	112
4.4	Integration von Sicherheit in die Geschäftsprozesse.....	113
4.5	Bestehende Risikomanagementansätze ergänzen.....	114
4.6	Bürokratische Auswüchse	115
5	Informationswerte bestimmen	117
5.1	Welche Werte sollen berücksichtigt werden?	117
5.2	Wo und wie kann man Werte ermitteln?	119
5.3	Wer ist für die Sicherheit der Werte verantwortlich?.....	123
5.4	Wer bestimmt, wie wichtig ein Wert ist?	124
6	Risiken einschätzen	127
6.1	Normative Mindestanforderungen aus ISO 27001	128
6.2	Schutzbedarf nach IT-Grundschutz	137
6.3	Erweiterte Analyse nach IT-Grundschutz.....	142
6.4	Die monetäre Einschätzung von Risiken.....	143
7	Maßnahmenziele und Maßnahmen bearbeiten	149
A.5	Sicherheitsleitlinie	150
A.6	Organisation der Informationssicherheit	151
A.7	Management von organisationseigenen Werten	161
A.8	Personelle Sicherheit.....	166
A.9	Physische und umgebungsbezogene Sicherheit	173
A.10	Betriebs- und Kommunikationsmanagement.....	186
A.11	Zugangskontrolle	218
A.12	Beschaffung, Entwicklung und Wartung von Informationssystemen	242
A.13	Umgang mit Informationssicherheitsvorfällen	255
A.14	Sicherstellung des Geschäftsbetriebs	258
A.15	Einhaltung von Vorgaben.....	264
8	Maßnahmen: Validieren und Freigeben.....	277
8.1	Validierung von Maßnahmen.....	277
8.2	Maßnahmenbeobachtung und -überprüfung	279
8.3	Maßnahmenfreigabe	280
8.4	Alternative Vorgehensweise	280
9	Metriken zu ISMS und Sicherheitsmaßnahmen	283
9.1	Einführung von Metriken	283

9.2	Praktische Empfehlungen zur Einführung von Metriken	288
10	Audits und Zertifizierungen	295
10.1	Ziele und Nutzen	295
10.2	Prinzipielle Vorgehensweise	298
10.3	Vorbereiten eines Audits	306
10.4	Durchführung eines Audits	309
10.5	Erfahrungen aus realen Audits	312
10.6	Auswertung des Audits und Optimierung der Prozesse	316
10.7	Grundschutz-Audit	317
11	Zum Abschluss	325
	Beispiel einer Informationssicherheitsleitlinie	329
	Verzeichnis der Maßnahmen aus Anhang A der ISO 27001	335
	Verzeichnis der Grundschutzmaßnahmen	343
	Einige Fachbegriffe: deutsch / englisch	349
	Verzeichnis der Abbildungen und Tabellen	351
	Verwendete Abkürzungen	353
	Quellenhinweise	357
	Sachwortverzeichnis	363