

Inhaltsverzeichnis

1	Gesetze und Standards im Umfeld der Informationssicherheit.....	1
1.1	Corporate Governance und Risikomanagement.....	1
1.2	Die Bedeutung des öffentlichen Beschaffungsrechts.....	6
1.3	Standards zu Management-Systemen.....	8
1.4	Zertifizierfähige Modelle.....	11
1.5	Konkrete Standards zur IT-Sicherheit.....	15
2	Vergleich der Begrifflichkeiten.....	21
2.1	Organisation, Werte und Sicherheitsziele.....	22
2.2	Risiken und Analysen.....	25
2.3	Maßnahmenauswahl und Risikobehandlung.....	31
2.4	Sicherheitsdokumente.....	34
2.5	Übersetzungsprobleme bei der deutschen Ausgabe des Standards.....	38
3	Das ISMS nach ISO 27001.....	41
3.1	Das Modell des ISMS.....	41
3.2	PLAN: Das ISMS festlegen und verwalten.....	45
3.3	DO: Umsetzen und Durchführen des ISMS.....	63
3.4	CHECK: Überwachen und Überprüfen des ISMS.....	72
3.5	ACT: Pflegen und Verbessern des ISMS.....	78
3.6	Anforderungen an die Dokumentation.....	82
3.7	Dokumentenlenkung.....	85
3.8	Lenkung der Aufzeichnungen.....	89
3.9	Verantwortung des Managements.....	90
3.10	Interne ISMS-Audits.....	94
3.11	Managementbewertung des ISMS.....	95
3.12	Verbesserung des ISMS.....	98
3.13	Maßnahmenziele und Maßnahmen.....	100
4	Festlegung des Anwendungsbereichs und Überlegungen zum Management.....	107
4.1	Anwendungsbereich des ISMS zweckmäßig bestimmen.....	107

Inhaltsverzeichnis

4.2	Das Management-Forum für Informationssicherheit	109
4.3	Verantwortlichkeiten für die Informationssicherheit	110
4.4	Integration von Sicherheit in die Geschäftsprozesse.....	111
4.5	Bestehende Risikomanagementansätze ergänzen.....	112
4.6	Bürokratische Auswüchse	113
5	Informationswerte bestimmen	115
5.1	Welche Werte sollen berücksichtigt werden?	115
5.2	Wo und wie kann man Werte ermitteln?	117
5.3	Wer ist für die Sicherheit der Werte verantwortlich?.....	121
5.4	Wer bestimmt, wie wichtig ein Wert ist?	122
6	Risiken einschätzen	125
6.1	Normative Mindestanforderungen aus ISO 27001	126
6.2	Schutzbedarf nach IT-Grundschutz	135
6.3	Erweiterte Analyse nach IT-Grundschutz.....	140
6.4	Die monetäre Einschätzung von Risiken.....	141
7	Maßnahmenziele und Maßnahmen bearbeiten	147
A.5	Sicherheitsleitlinie	148
A.6	Organisation der Informationssicherheit	149
A.7	Management von organisationseigenen Werten.....	158
A.8	Personelle Sicherheit.....	163
A.9	Physische und umgebungsbezogene Sicherheit.....	170
A.10	Betriebs- und Kommunikationsmanagement.....	182
A.11	Zugangskontrolle	213
A.12	Beschaffung, Entwicklung und Wartung von Informationssystemen	235
A.13	Umgang mit Informationssicherheitsvorfällen	248
A.14	Sicherstellung des Geschäftsbetriebs	252
A.15	Einhaltung von Vorgaben.....	257
8	Maßnahmen: Validieren und Freigeben.....	269
8.1	Validierung von Maßnahmen.....	269
8.2	Maßnahmenbeobachtung und -überprüfung.....	271
8.3	Maßnahmenfreigabe	272
8.4	Alternative Vorgehensweise	272

9	Metriken zu ISMS und Sicherheitsmaßnahmen	275
9.1	Stand der ISO 27004	275
9.2	Praktische Empfehlungen zur Einführung von Metriken	280
10	Audits und Zertifizierungen	287
10.1	Ziele und Nutzen	287
10.2	Prinzipielle Vorgehensweise	290
10.3	Vorbereiten eines Audits	297
10.4	Durchführung eines Audits	301
10.5	Erfahrungen aus realen Audits.....	304
10.6	Auswertung des Audits und Optimierung der Prozesse	308
10.7	Grundschutz-Audit.....	309
11	Zum Abschluss.....	311
	Beispiel einer Informationssicherheitsleitlinie	315
	Verzeichnis der Maßnahmen aus Anhang A der ISO 27001	321
	Verzeichnis der Grundschutzmaßnahmen	329
	Einige Fachbegriffe: deutsch / englisch	335
	Verzeichnis der Abbildungen und Tabellen	337
	Verwendete Abkürzungen.....	339
	Quellenhinweise.....	343
	Sachwortverzeichnis.....	349