

Inhaltsverzeichnis

Vorwort	7
1 Einführung	17
2 Grundlagen und Definitionen	21
2.1 Daten und Informationen	21
2.2 Informationen als Werte	21
2.3 Informationssicherheit	22
2.4 IT-Sicherheit, Datenschutz und Cybersicherheit	24
2.5 Schwachstelle, Bedrohung, Gefährdung und Risiko	26
2.6 Maßnahmen zur Risikobehandlung	28
2.7 Sicherheitskonzept	30
3 Managementsysteme	35
3.1 Abgrenzung zwischen Governance und Management	35
3.2 Managementsystem	36
3.2.1 Managementdomänen	37
3.2.2 Prozesse	38
3.2.3 Prozessmanagement	42
3.3 Integriertes Managementsystem	43
3.4 Informationssicherheitsmanagementsystem	43
4 Anforderungen an Informationssicherheit und deren Steuerung	49
4.1 Anforderungen an die Informationssicherheit	49
4.1.1 Stakeholder außerhalb der Organisation	49
4.1.2 Stakeholder innerhalb der Organisation	50
4.1.2.1 Weitere Managementdomänen	52
4.1.2.2 Fachabteilungen	53
4.2 Anforderungen an das Management der Informationssicherheit	54
5 ISMS-Normen und -Standards	55
5.1 ISO-27000-Normenfamilie	55
5.2 BSI-IT-Grundschutz	56
5.3 Vergleich der Vorgehensweisen – ISO-27000-Normenfamilie und BSI-IT-Grundschutz	58
6 ISMS-Prozessreferenzmodell	65
6.1 Managementprozess – Führung/strategische Steuerung	76
6.2 ISMS-Kernprozesse	82

6.2.1	Steuerung von Sicherheitsvorgaben und -regelungen	84
6.2.2	Steuerung von Anforderungen	92
6.2.3	Identifikation und Bewertung von Risiken	99
6.2.4	Behandlung der Risiken	111
6.2.5	Steuerung der Umsetzung von Maßnahmen	120
6.2.6	Steuerung ausgelagerter Dienstleistungen	125
6.2.7	Gewährleistung von Sensibilisierung und Kompetenz	131
6.2.8	Steuerung von Vorfällen	137
6.2.9	Steuerung von Änderungen	145
6.2.10	Interne Auditierung	151
6.2.11	Bewertung der Leistung (Überwachen und Messen)	157
6.2.12	Verbesserung	163
6.3	Unterstützungsprozesse	167
6.3.1	Steuerung von Aufzeichnungen	167
6.3.2	Steuerung von Ressourcen	173
6.3.3	Kommunikation	179
6.3.4	Steuerung der Kundenbeziehungen	185
6.4	Zusammenfassung des ISMS-Prozessreferenzmodells	190
7	Vorgehen zur Einführung des ISMS-Prozessreferenzmodells	191
7.1	Anforderungsanalyse und Definition des SOLL-Reifegrades	191
7.2	Methoden zur Erhebung des IST-Reifegrades	198
7.2.1	ISO/IEC-15504-Prozess-Assessment	199
7.2.2	ISO/IEC-33000-Normenfamilie	199
7.2.3	COBIT-Prozessbewertungsmodell	199
7.3	Umsetzung des SOLL-Reifegrades	200
8	ISMS-Prozessreferenzmodell für geringe SOLL-Reifegradanforderungen	203
9	Vergleich des ISMS-Prozessreferenzmodells mit etablierten Normen und Standards ...	207
9.1	Vergleich mit der ISO-27000-Familie, ISO 20000-1 sowie COBIT	207
9.2	Vergleich mit dem BSI-IT-Grundschutz	208
10	Anhang A – Konformitätsstatement zu ISO/IEC 33004	217
	Literaturverzeichnis	221
	Stichwortverzeichnis	223
	Die Autoren	227