

Inhalt

5	Abkürzungen
9	1 Vorwort
13	2 Informationssicherheit beginnt beim Management
13	2.1 Managementbereitschaft
14	2.2 Schritt für Schritt zum Erfolg
19	3 Informationssicherheitsmanagementsystem (ISMS): Darauf kommt es an
19	3.1 Wieviel Informationssicherheit ist notwendig?
23	3.2 Wie wirtschaftlich ist Informationssicherheit?
25	3.3 IS-Risikomanagement
27	3.4 Sicherheitsorganisation
28	3.5 Rollen und Verantwortlichkeiten
30	3.6 Sicherheitsprozesse
31	3.7 Technische Sicherheit
39	4 ISMS-Normen und -Standards
39	4.1 IS-Risikomanagement
42	4.2 Die ISO/IEC 27001 „Information technology – Security techniques – Information security management systems – Requirements“
42	4.2.1 Einführung und Historie
44	4.2.2 Hauptteil der Norm
45	4.2.3 Anhang A der Norm
45	4.2.4 Anwendung der Norm
48	4.3 COBIT
49	4.4 Informationssicherheitsmanagement nach IT Infrastructure Library (ITIL)
52	4.5 Statement on Standards for Attestation Engagements (SSAE) / International Standard on Assurance Engagements (ISAE)
53	4.5.1 Beteiligte bei Prüfung nach ISAE 3402

53	4.5.2	Einsatzszenarien
54	4.5.3	Prüfungsanlass und Mehrwert der ISAE 3402
57	5	Business Continuity Management (BCM)
57	5.1	Aufbau eines BCM
59	5.2	Ablauf einer Business Impact Analyse
59	5.2.1	Auswahl der einzubeziehenden Organisations- einheiten und Geschäftsprozesse
59	5.2.2	Schadensanalyse
59	5.2.3	Festlegung der Wiederanlaufparameter
60	5.2.4	Berücksichtigung von Abhängigkeiten
60	5.2.5	Priorisierung und Kritikalität der Geschäfts- prozesse
60	5.2.6	Erhebung der Ressourcen für Normal- und Notbetrieb
60	5.2.7	Kritikalität und Wiederanlaufzeiten der Res- ourcen
63	6	Rechtliche Aspekte
69	7	Zusammenfassung
73	8	Literatur- und Normenverzeichnis
73	8.1	Literatur
73	8.2	Verzeichnis der wichtigsten referenzierten ISO-Normen
77		Der Autor