

Inhalt

Vorwort	IX
1 Herausforderungen in Informationssicherheit und Datenschutz	1
1.1 Einordnung von Informationssicherheit und Datenschutz	3
1.2 Anforderungen an Informationssicherheit und Datenschutz	7
1.2.1 Wesentliche Normen und gesetzliche Vorschriften	8
1.2.2 Cyber-Security	35
1.2.3 ISO/IEC 27001	41
1.2.4 IT-Grundschutz	75
1.2.4.1 Bestandteile des IT-Grundschutzes	80
1.2.4.2 Die IT-Grundschutz-Methodik	84
1.2.4.3 Der Sicherheitsprozess entsprechend IT-Grundschutz ..	86
1.2.5 EU-DSGVO	89
1.2.5.1 DSGVO-Grundsätze als Teil des Datenschutzkonzepts ...	96
1.2.5.2 Umsetzung der Anforderungen	98
2 Integriertes Managementsystem für Datenschutz und Informationssicherheit	103
2.1 Was ist ein Managementsystem für Datenschutz und Informationssicherheit?	106
2.2 Bestandteile eines integrierten Managementsystems	110
2.2.1 Warum? – Strategie: Datenschutzpolitik und Informationssicherheitsstrategie	111

2.2.2	Was? – Anforderungen: Festlegung der umzusetzenden Kontrollen	112
2.2.3	Wie? – Sicherheitsorganisation und Sicherheitskonzept	112
2.2.4	Nachweis – Überwachung der Maßnahmendurchführung sowie regelmäßige interne oder externe Audits, um Konformität und Wirksamkeit zu gewährleisten	115
2.3	Erfolgsfaktoren für ein wirksames integriertes Instrumentarium	122
3	Schritt-für-Schritt-Leitfaden	127
3.1	Vorgehensweise zum Aufbau eines integrierten DS & ISMS	128
3.2	Detaillierter Leitfaden für den Aufbau	135
3.2.1	Datenschutz- und Informationssicherheitsleitlinie und -organisation	137
3.2.2	Konzeption des integrierten Managementsystems	138
3.2.2.1	Teilschritte bei der Konzeption des Instrumentariums ..	140
3.2.2.2	Umsetzen der Konzeption für das integrierte DS & ISMS und Inbetriebnahme	144
3.3	Fazit	145
4	Best-Practices	147
4.1	Schutzziele und Schutzbedarfsfeststellung	149
4.1.1	Schutzziele	151
4.1.1.1	Vertraulichkeit	151
4.1.1.2	Integrität	155
4.1.1.3	Verfügbarkeit	156
4.1.1.4	Weitere Schutzziele	158
4.1.2	Schutzbedarfsfeststellung	160
4.1.2.1	Schadensszenarien	160
4.1.2.2	Kronjuwelen	164
4.1.2.3	Vorgehen bei der Schutzbedarfsfeststellung	165
4.1.2.4	Zonenkonzept	169
4.1.2.5	Schutzbedarfsfeststellung für Geschäftsprozesse und die dazugehörigen Informationen	173
4.2	Risikomanagement	176
4.3	Notfallmanagement	185
4.4	ISMS-Reporting	192
4.5	Sicherheits- und Datenschutzorganisation	196

5 Integration von EAM, IT-Servicemanagement und Informationssicherheit	203
5.1 EAM und Informationssicherheit	205
5.1.1 Enterprise Architecture Management	206
5.1.2 Zusammenspiel von EAM und DS & ISMS	213
5.1.3 Tool-Unterstützung für DS & ISMS	216
5.2 IT-Servicemanagement und Informationssicherheit	220
Glossar	229
Abkürzungen	257
Literatur	261
Stichwortverzeichnis	265