

Inhalt

Vorwort	VII
Wegweiser durch dieses Buch.	IX
1 Herausforderungen in Informationssicherheit und Datenschutz	1
1.1 Einordnung von Informationssicherheit und Datenschutz	3
1.2 Anforderungen an Informationssicherheit und Datenschutz	6
1.2.1 Wesentliche Normen und gesetzliche Vorschriften	7
1.2.2 Cyber-Security	15
1.2.3 ISO/IEC 27001	17
1.2.4 IT-Grundschutz	37
1.2.4.1 Bestandteile des IT-Grundschutzes	38
1.2.4.2 Die IT-Grundschutz-Methodik	40
1.2.4.3 Der Sicherheitsprozess entsprechend IT-Grundschutz	41
1.2.5 EU-DSGVO	44
1.2.5.1 DSGVO-Grundsätze als Teil des Datenschutzkonzepts	49
1.2.5.2 Umsetzung der Anforderungen	51
2 Integriertes Managementsystem für Datenschutz und Informationssicherheit	55
2.1 Was ist ein Managementsystem für Datenschutz und Informationssicherheit?	57
2.2 Bestandteile eines integrierten Managementsystems	61
2.2.1 Warum? – Strategie: Datenschutzpolitik und Informationssicherheitsstrategie	62
2.2.2 Was? – Anforderungen: Festlegung der umzusetzenden Kontrollen	63
2.2.3 Wie? – Sicherheitsorganisation und Sicherheitskonzept	63
2.2.4 Nachweis – Überwachung der Maßnahmendurchführung sowie regelmäßige interne oder externe Audits, um Konformität und Wirksamkeit zu gewährleisten	65
2.3 Erfolgsfaktoren für ein wirksames integriertes Instrumentarium für Datenschutz und Informationssicherheit	71
3 Schritt-für-Schritt-Leitfaden	77
3.1 Vorgehensweise zum Aufbau eines integrierten DS & ISMS	78
3.2 Detaillierter Leitfaden für den Aufbau	84
3.2.1 Datenschutz- und Informationssicherheitsleitlinie und -organisation	85
3.2.2 Konzeption des integrierten Managementsystems	87

3.2.2.1	Teilschritte bei der Konzeption des Instrumentariums	88
3.2.2.2	Umsetzen der Konzeption für das integrierte DS & ISMS und Inbetriebnahme.....	92
3.3	Fazit.....	92
4	Best-Practices	95
4.1	Schutzziele und Schutzbedarfsfeststellung	97
4.1.1	Schutzziele	98
4.1.1.1	Vertraulichkeit	98
4.1.1.2	Integrität	102
4.1.1.3	Verfügbarkeit.....	103
4.1.1.4	Weitere Schutzziele, z. B. Authentizität	104
4.1.2	Schutzbedarfsfeststellung	106
4.1.2.1	Schadensszenarien.....	106
4.1.2.2	Kronjuwelen	109
4.1.2.3	Vorgehen bei der Schutzbedarfsfeststellung	110
4.1.2.4	Zonenkonzept	114
4.1.2.5	Schutzbedarfsfeststellung für Geschäftsprozesse und die dazugehörigen Informationen.....	117
4.2	Risikomanagement	120
4.3	Notfallmanagement.....	128
4.4	ISMS-Reporting	134
4.5	Sicherheits- und Datenschutzorganisation	137
5	Integration von EAM, IT-Servicemanagement und Informations- sicherheit.....	143
5.1	EAM und Informationssicherheit.....	145
5.1.1	Enterprise Architecture Management	145
5.1.2	Zusammenspiel von EAM und DS & ISMS.....	151
5.1.3	Tool-Unterstützung für DS & ISMS	154
5.2	IT-Servicemanagement und Informationssicherheit	157
	Glossar	163
	Abkürzungen.....	195
	Literatur	197
	Stichwortverzeichnis.....	201