

# Inhalt

<b>ISMS einrichten – warum?</b> .....	1
<b>1 Einleitung</b> .....	3
1.1 Abgrenzung .....	4
1.2 Zum Nutzen eines ISMS .....	5
1.3 Struktur dieses Buches .....	6
<b>2 Rechtlicher Rahmen</b> .....	9
2.1 Vorschriften zum Management von Informationssicherheit .....	9
2.2 Rechtliche Verpflichtungen zur Einrichtung eines ISMS .....	10
<b>3 Hintergründe zur Normung</b> .....	15
3.1 Historische Entwicklung .....	15
3.2 Die Branchenstandards der ISO .....	15
3.3 Aktualisierungszyklen .....	17
3.3.1 Die sechs Stufen des Normungsprozesses .....	17
3.4 Hilfreiche Informationen .....	18
3.4.1 Weitere Dokumententypen .....	18
3.4.2 Das ISO-Netzwerk .....	18
3.4.3 Übersetzungen .....	19
3.4.4 Abkürzungen .....	19
3.4.5 RSS-Feeds .....	20
<b>4 Überblick über die Normungsfamilie ISO 2700x</b> .....	21
4.1 Vokabular .....	21
4.1.1 ISO/IEC 27000:2016 .....	21
4.2 Anforderungsstandards .....	23
4.2.1 ISO/IEC 27001:2013 .....	23
4.2.2 ISO/IEC 27006:2015 .....	23
4.2.3 ISO/IEC 27009:2016 .....	24
4.3 Anleitende Standards .....	24
4.3.1 ISO/IEC 27002:2013 .....	24
4.3.2 ISO/IEC 27003:2017 .....	25
4.3.3 ISO/IEC 27004:2016 .....	25
4.3.4 ISO/IEC 27005:2011 .....	25
4.3.5 ISO/IEC 27007:2011 .....	26
4.3.6 ISO/IEC TR 27008:2011 .....	26

4.3.7	ISO/IEC 27013:2015 .....	26
4.3.8	ISO/IEC 27014:2013 .....	26
4.3.9	ISO/IEC TR 27016:2014 .....	27
4.3.10	ISO/IEC 27021 .....	27
4.3.11	ISO/IEC TR 2023:2015 .....	27
4.4	Sektorspezifische Standards .....	27
4.4.1	ISO/IEC 27010:2015 .....	27
4.4.2	ISO/IEC 27011:2016 .....	27
4.4.3	ISO/IEC TR 27015:2012 .....	28
4.4.4	ISO/IEC 27017:2015 .....	28
4.4.5	ISO/IEC 27018:2014 .....	28
4.5	Maßnahmenspezifische Standards .....	28
<b>5</b>	<b>Integrierte Managementsysteme .....</b>	<b>31</b>
5.1	Einleitung .....	31
5.2	ISO-Richtlinie zur Vereinheitlichung von Managementsystem- normen .....	32
5.3	Plan-Do-Check-Act .....	33
5.4	Managementsysteme und Systemtheorie .....	34
5.5	Integration von Managementsystemen (IMS) .....	37
5.6	Literaturverzeichnis .....	40
	<b>ISMS eingerichtet – was nun? .....</b>	<b>41</b>
<b>6</b>	<b>Betriebsdokumentation eines ISMS nach ISO/IEC 27001:2013 ...</b>	<b>43</b>
6.1	Einleitung .....	43
6.2	Dokumentenpyramide .....	46
6.2.1	Leitlinien, Leitplanken und Geltungsbereich .....	46
6.2.2	Richtlinien und steuernde Vorgaben .....	49
6.2.3	Konzepte und Prozesse .....	51
6.2.4	Nachweise und Aufzeichnungen .....	54
6.3	Literaturverzeichnis .....	56
<b>7</b>	<b>Ressourcen bereitstellen und Kompetenz gewährleisten .....</b>	<b>59</b>
7.1	Ressourcenmanagement .....	59
7.1.1	Anforderungen an das Ressourcenmanagement .....	60
7.1.2	Notwendigkeit von Ressourcen für den ISMS-Betrieb und für Sicherheitsmaßnahmen .....	61
7.1.2.1	Ressourcen für ISMS-Maßnahmen .....	63

7.1.2.2	Ressourcen für den ISMS-Betrieb .....	63
7.1.3	Ressourcenmanagement als Prozess .....	69
7.2	Kompetenz gewährleisten .....	74
7.2.1	Anforderungen an das Personal – je nach Rolle .....	75
7.2.1.1	Der Informationssicherheitsbeauftragte (ISB) .....	76
7.2.1.2	Die Informationssicherheitskoordinatoren (ISK) .....	77
7.2.1.3	Die Informationssicherheitsauditoren (ISA) .....	79
7.2.2	Weiterbildungsmöglichkeiten – Zertifizierungen .....	81
<b>8</b>	<b>Bewusstsein schaffen und Kommunikation verbessern .....</b>	<b>85</b>
8.1	Bewusstsein .....	86
8.2	Kommunikation .....	89
8.2.1	Kommunikation: Sender – Nachricht – Empfänger .....	89
8.2.2	Systemische Kommunikation .....	94
8.2.3	Verhaltenskreuz nach Schulz von Thun .....	96
8.2.4	Normenkreuz nach Gouthier .....	98
8.2.5	Kombination von Verhaltens- und Normenkreuz .....	101
8.2.6	Zusammenfassung .....	103
8.3	Sicherheitskultur ausbilden und Awareness schaffen .....	104
8.3.1	Das Sicherheitsparadoxon .....	104
8.3.2	Sicherheitsmaßnahmen sind ein Zeichen von Professionalität ....	106
8.3.3	Die Notwendigkeit eines Kommunikationskonzepts .....	107
8.3.4	Die Beeinflussung der Sicherheitskultur durch Awareness- Maßnahmen .....	108
8.3.5	Erfolgsfaktoren von Awareness-Maßnahmen .....	109
8.3.6	Phasen einer Awareness-Kampagne .....	109
8.4	ISO/IEC 27001-Checkliste .....	112
<b>9</b>	<b>Informationssicherheitsrisiken handhaben .....</b>	<b>115</b>
9.1	Einleitung .....	115
9.2	Informationssicherheitsrisikobeurteilung und -behandlung .....	118
9.2.1	Ausgestaltung des Prozesses .....	118
9.2.2	Definition des Kontextes .....	119
9.2.3	Identifikation von Informationssicherheitsrisiken .....	121
9.2.3.1	Identifikation der Prozesse und Assets .....	121
9.2.3.2	Identifikation von Bedrohungen .....	121
9.2.3.3	Identifikation von umgesetzten Maßnahmen .....	123
9.2.3.4	Identifikation von Schwachstellen .....	123

9.2.3.5	Identifikation der Schadensauswirkung .....	124
9.2.4	Analyse von Informationssicherheitsrisiken .....	124
9.2.5	Bewertung von Informationssicherheitsrisiken .....	125
9.2.6	Informationssicherheitsrisikobehandlung .....	126
9.2.7	Informationssicherheitsrisikokommunikation .....	129
9.2.7.1	Informationssicherheitsrisikoberichtswesen .....	129
9.2.7.2	Kommunikation und Beratung .....	130
9.2.8	Aufbauorganisation zum Prozess .....	130
9.2.9	Wirtschaftlichkeitsbetrachtungen im Informationssicherheitsrisiko- management .....	132
9.3	Informationssicherheitsrisikoüberwachung/-überprüfung .....	134
9.3.1	Geplante Überprüfung des Informationssicherheitsrisikomanage- ments .....	134
9.3.2	Überprüfung der Risikoeinschätzung bei Änderungen .....	134
9.3.2.1	Incidents/Sicherheitsvorfälle .....	135
9.3.2.2	Change .....	135
9.3.2.3	Interne Audits .....	136
9.3.2.4	Projektmanagement .....	137
9.3.2.5	Lieferantenmanagement .....	144
9.3.2.6	Änderung an internen und externen Faktoren .....	146
9.4	Literatur .....	147
<b>10</b>	<b>ISMS bewerten</b> .....	<b>149</b>
10.1	Einleitung .....	149
10.2	Reifegradmodelle .....	151
10.2.1	CMMI .....	154
10.2.2	ISO/IEC 15504, auch bekannt als SPICE .....	155
10.2.3	ISO/IEC 21827, auch bekannt als SSE-CMM .....	156
10.2.4	O-ISM <sup>3</sup> .....	157
10.2.5	Methode zur Ermittlung des SOLL-Reifegrades .....	159
10.3	Anwendungsbeispiel: Smart Grid .....	161
10.3.1	Verteilnetze und Smart Grids .....	161
10.3.2	Anforderungen an die Informationssicherheit .....	162
10.4	Messen und Bewerten – Anforderungen und Werkzeuge .....	163
10.4.1	Die Norm ISO/IEC 27004 .....	163
10.4.2	Prozessorientierte Vorgehensmodelle .....	164
10.4.3	Goal Question Metric (GQM) .....	168
10.4.4	Metrisierung .....	170

10.4.5	Abgeleitete Maße und Indikatoren .....	170
10.5	Messen und Bewerten – Anwendung .....	171
10.5.1	Beispiel für die Ermittlung eines ISMS-Zielindikators .....	171
10.5.2	Beispiel für die Ermittlung eines Indikators der Leistung eines Informationssicherheitsprozesses .....	174
10.6	Gesamtbewertung .....	179
10.7	Kurzfassung des Vorgehensmodells .....	181
<b>11</b>	<b>ISMS verbessern</b> .....	<b>183</b>
11.1	Fortlaufende Verbesserung .....	183
11.2	Aufspüren von Nicht-Konformitäten, ineffektiven Maßnahmen und Ineffizienzen .....	186
11.3	Ableiten und Initiieren von Korrekturmaßnahmen .....	195
11.4	Der Verbesserungsprozess im Überblick .....	196