# Inhaltsverzeichnis


| | | |
|---|---|---|
| **1** | **Einleitung** | 1 |
| 1.1 | Abgrenzung | 2 |
| 1.2 | Über den Nutzen eines ISMS | 3 |
| 1.3 | Aufbau des Buches | 4 |
| **2** | **Rechtlicher Rahmen** | 8 |
| 2.1 | Vorschriften zum Management von Informationssicherheit | 8 |
| 2.2 | Rechtliche Verpflichtungen zur Einrichtung eines ISMS | 10 |
| 2.3 | Kritische Infrastrukturen | 15 |
| 2.3.1 | Kurzvorstellung der kritischen Infrastrukturen und ihrer nationalen wie europäischen Verpflichtungen | 16 |
| 2.3.2 | Rolle und Bedeutung eines ISMS im Bereich der kritischen Infrastrukturen | 17 |
| 2.3.3 | Ergänzung des ISMS durch branchenspezifische Sicherheitsstandards | 18 |
| 2.3.4 | Forderung eines ISMS gemäß IT-Sicherheitskatalog und Ergänzung durch sektorspezifische Norm | 19 |
| 2.3.5 | Ergänzung des ISMS im Bereich Smart Metering | 20 |
| 2.3.6 | Systeme zur Angriffserkennung (SzA) | 21 |
| **3** | **Hintergründe zur Normung** | 25 |
| 3.1 | Historische Entwicklung | 25 |
| 3.2 | Die Branchenstandards der ISO | 25 |
| 3.3 | Die sechs Stufen des Normungsprozesses | 27 |
| 3.4 | Aktualisierungszyklen | 28 |
| 3.5 | Hilfreiche Informationen | 28 |
| 3.5.1 | Weitere Dokumententypen | 28 |
| 3.5.2 | Das ISO-Netzwerk | 28 |
| 3.5.3 | Übersetzungen | 29 |
| 3.5.4 | Abkürzungen | 29 |
| 3.5.5 | Lifecycle einer Norm | 30 |
| **4** | **Überblick über die Normen der Reihe ISO 27000** | 31 |
| 4.1 | Vokabular | 31 |
| 4.2 | Anforderungsstandards | 33 |
| 4.3 | Anleitende Standards | 34 |
| 4.4 | Sektorspezifische Standards | 39 |
| 4.5 | Maßnahmenspezifische Standards | 39 |

| | | |
|---|---|---|
| **5** | **Integrierte Managementsysteme** | 41 |
| 5.1 | Einleitung | 41 |
| 5.2 | ISO-Richtlinie zur Vereinheitlichung von Managementsystemnormen | 42 |
| 5.3 | Plan-Do-Check-Act | 43 |
| 5.4 | Managementsysteme und Systemtheorie | 45 |
| 5.5 | Integration von Managementsystemen | 48 |
| 5.6 | Integrierte Managementsysteme in der Praxis | 51 |
| **6** | **Betriebsdokumentation eines ISMS nach DIN EN ISO/IEC 27001** | 54 |
| 6.1 | Einleitung, historischer Abriss und obligatorische Dokumente | 54 |
| 6.2 | Die drei Seiten der Dokumentenpyramide | 58 |
| 6.2.1 | Leitlinien und ihr Geltungsbereich mit Schnittstellen | 61 |
| 6.2.2 | Richtlinien und steuernde Vorgaben | 65 |
| 6.2.3 | Konzepte und Prozesse | 67 |
| 6.2.4 | Dokumentenlandkarte | 70 |
| 6.2.5 | Dokumentenweiterentwicklung – Das Release-Management | 71 |
| 6.2.6 | Bidirektionale Nachweise, Aufzeichnungen und Kontrolle | 73 |
| **7** | **Ressourcen bereitstellen und Kompetenz gewährleisten** | 76 |
| 7.1 | Ressourcenmanagement | 76 |
| 7.1.1 | Anforderungen an das Ressourcenmanagement | 77 |
| 7.1.2 | Notwendigkeit von Ressourcen für den ISMS-Betrieb und für Sicherheitsmaßnahmen | 78 |
| 7.1.3 | Ressourcenmanagement als Prozess | 86 |
| 7.2 | Kompetenz gewährleisten | 90 |
| 7.2.1 | Anforderungen an das Personal – je nach Rolle | 90 |
| 7.2.2 | Weiterbildungsmöglichkeiten – Zertifizierungen | 96 |
| **8** | **Bewusstsein schaffen und Kommunikation verbessern** | 100 |
| 8.1 | Bewusstsein | 101 |
| 8.2 | Kommunikation | 104 |
| 8.2.1 | Kommunikation: Senden und Empfangen von Nachrichten | 104 |
| 8.2.2 | Systemische Kommunikation | 109 |
| 8.2.3 | Verhaltenskreuz nach Schulz von Thun | 111 |
| 8.2.4 | Normenkreuz nach Gouthier | 113 |
| 8.2.5 | Kombination von Verhaltens- und Normenkreuz | 117 |
| 8.2.6 | Zusammenfassung | 118 |
| 8.3 | Sicherheitskultur ausbilden und Awareness schaffen | 119 |

8.3.1 Das Sicherheitsparadoxon ... 119
8.3.2 Sicherheitsmaßnahmen sind ein Zeichen von Professionalität ... 121
8.3.3 Die Notwendigkeit eines Kommunikationskonzepts ... 122
8.3.4 Die Beeinflussung der Sicherheitskultur durch Awareness-Maßnahmen ... 123
8.3.5 Erfolgsfaktoren von Awareness-Maßnahmen ... 124
8.3.6 Phasen einer Awareness-Kampagne ... 125
8.4 DIN EN ISO/IEC 27001-Checkliste ... 127

**9 Informationssicherheitsrisiken handhaben ... 129**
9.1 Einleitung ... 129
9.2 Informationssicherheitsrisikobeurteilung und -behandlung ... 133
9.2.1 Ausgestaltung des Prozesses ... 133
9.2.2 Definition des Kontextes ... 133
9.2.3 Identifikation von Informationssicherheitsrisiken ... 135
9.2.4 Analyse von Informationssicherheitsrisiken ... 140
9.2.5 Bewertung von Informationssicherheitsrisiken ... 141
9.2.6 Informationssicherheitsrisikobehandlung ... 141
9.2.7 Informationssicherheitsrisikokommunikation ... 144
9.2.8 Aufbauorganisation zum Prozess ... 145
9.2.9 Wirtschaftlichkeitsbetrachtungen im Informationssicherheitsrisikomanagement ... 147
9.3 Überwachung bzw. Überprüfung des Informationssicherheitsrisikos ... 149
9.3.1 Geplante Überprüfung des Informationssicherheitsrisikomanagements ... 149
9.3.2 Überprüfung der Risikoeinschätzung bei Änderungen ... 149

**10 ISMS bewerten ... 162**
10.1 Die Bedeutung der Zertifizierung ... 162
10.2 Reifegradmodelle und Leistungsfähigkeitsgradmodelle ... 164
10.2.1 Capability Maturity Model Integrated ... 167
10.2.2 ISO/IEC 33001 (Prozessbeurteilung) ... 168
10.2.3 ISO/IEC 21827, auch bekannt als SSE-CMM ... 169
10.2.4 Cybersecurity Capability Maturity Model ... 170
10.2.5 Open Information Security Management Maturity Model ... 171
10.2.6 Leistungsfähigkeitsgrade im Rahmen von IT-Governance ... 173
10.3 Messen und Bewerten – Anforderungen und Werkzeuge ... 175
10.3.1 Die Norm ISO/IEC 27004 ... 175
10.3.2 Prozessorientierte Vorgehensmodelle ... 176

10.3.3 Goal Question Metric ..... 179
10.3.4 Metrisierung ..... 181
10.3.5 Abgeleitete Maße und Indikatoren ..... 182
10.4 Messen und Bewerten – Anwendung am Beispiel des ISMS eines Energienetzbetreibers ..... 183
10.4.1 Anforderungen an die Informationssicherheit von Verteilnetzbetreibern ..... 183
10.4.2 Beispiel für die Ermittlung eines ISMS-Zielindikators ..... 185
10.4.3 Beispiel für die Ermittlung eines Indikators für die Leistung eines Informationssicherheitsprozesses ..... 187
10.4.4 Gesamtbewertung ..... 192
10.4.5 Kurzfassung des Vorgehensmodells ..... 195
10.5 Audits ..... 196
**11 ISMS verbessern** ..... 197
11.1 Fortlaufende Verbesserung ..... 197
11.2 Aufspüren von Nicht-Konformitäten, ineffektiven Maßnahmen und Ineffizienzen ..... 200
11.3 Ableiten und Initiieren von Korrekturmaßnahmen ..... 209
11.4 Der Verbesserungsprozess im Überblick ..... 210