

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung und Motivation</b>	<b>1</b>
1.1	Der Wert von Informationen	1
1.2	Informationssicherheit und IT-Sicherheit	3
1.3	Informationssicherheit, Daten- und Geheimschutz	6
1.3.1	Standards zur Informationssicherheit	7
1.3.2	Datenschutz	10
1.3.3	Geheimschutz	12
1.3.4	Schutzkonzepte und staatliche Vorsorge	14
1.4	Wichtige Prinzipien	16
1.5	Weitere Kapitel und Literaturempfehlungen	17
1.6	Fazit	18
	Literatur	19

## Teil I Informationssicherheits-Management nach ISACA

<b>2</b>	<b>Informationssicherheits-Governance</b>	<b>23</b>
2.1	Grundlagen der Information Security Governance	23
2.1.1	Die Idee des Managementprozesses	24
2.1.2	Die Rolle des IS-Managers	27
2.1.3	IS-Governance im Überblick	27
2.2	Wichtige Sicherheitskonzepte	29
2.2.1	Die Policy-Pyramide	31
2.3	Aufbau und Aufrechterhaltung einer IS-Strategie	32
2.4	Aufbau und Aufrechterhaltung eines IS-Governance Frameworks	34
2.5	Integration der IS-Governance in die Corporate Governance	35
2.6	Aufbau und Fortschreibung eines IS-Policy Frameworks	36
2.7	Business Cases – Entwicklung von praxisnahen Beispielen	39
2.8	Berücksichtigung von internen und externen Faktoren	42
2.9	Einholen der Unterstützung des Managements	44
2.10	Festlegen von Rollen und Verantwortlichkeiten	46

2.11	Grundlagen für die Kommunikation mit dem Management . . . . .	48
2.12	Die Leitsätze des Managements . . . . .	50
2.13	Zwischenfazit . . . . .	50
	Literatur . . . . .	51
<b>3</b>	<b>Informationssicherheits-Risikomanagement . . . . .</b>	<b>53</b>
3.1	Grundlagen des Risikomanagements . . . . .	53
3.1.1	Teilschritte des Risikomanagements . . . . .	57
3.1.2	NIST 800-30 als Beispiel . . . . .	58
3.1.3	Menschen und Risiken . . . . .	63
3.1.4	Weitere Gliederung des Kapitels . . . . .	63
3.2	Prozess zur Klassifizierung der Informationswerte . . . . .	64
3.3	Rechtliche und regulatorische Randbedingungen . . . . .	66
3.4	Regelmäßiges Risikoassessment . . . . .	67
3.5	Möglichkeiten der Risikominimierung – die 4-T-Maßnahmen . . . . .	70
3.6	Kontrollen im Bereich Informationssicherheit . . . . .	70
3.7	Der Prozess des Risikomanagements . . . . .	72
3.8	Einbindung in die Betriebsprozesse der Organisation . . . . .	73
3.9	Monitoring von Risiken . . . . .	74
3.10	Bericht von Compliance-Verletzungen . . . . .	75
3.11	Zwischenfazit . . . . .	76
	Literatur . . . . .	76
<b>4</b>	<b>Umsetzung des Informationssicherheits-Programms . . . . .</b>	<b>77</b>
4.1	Grundlagen zum Informationssicherheits-Programm . . . . .	78
4.1.1	Weitere Gliederung des Kapitels . . . . .	79
4.2	Ausrichtung des IS-Programms an den sonstigen Prozessen der Organisation . . . . .	80
4.3	Bestimmung von internen und externen Ressourcen . . . . .	81
4.4	Sicherheitsarchitektur . . . . .	82
4.5	Standards, Arbeitsanweisungen und Handlungsempfehlungen . . . . .	83
4.6	Security Awareness und Security Training . . . . .	89
4.7	Integration in die Geschäftsprozesse . . . . .	91
4.8	Berücksichtigung von Verträgen . . . . .	95
4.9	Aufbau eines Monitoring- und Reportingsystems unter Nutzung von Metriken . . . . .	98
4.10	Zwischenfazit . . . . .	100
	Literatur . . . . .	100
<b>5</b>	<b>Informationssicherheits-Vorfallsmanagement . . . . .</b>	<b>101</b>
5.1	Grundlagen des Incident-Response-Management . . . . .	101
5.2	Festlegung des Sicherheitsvorfalls . . . . .	103

5.3	Entwicklung eines Incident-Response-Plans . . . . .	105
5.4	Aufbau eines Prozesses zur Erkennung von Sicherheitsvorfällen . . . . .	107
5.5	Aufbau eines Prozesses zur Untersuchung von Sicherheitsvorfällen . . . . .	108
5.6	Aufbau eines Prozesses zur Eskalation und Kommunikation von Vorfällen . . . . .	110
5.7	Aufbau und Training der Incident-Response-Teams . . . . .	111
5.8	Erfolg durch praktische Übungen . . . . .	113
5.9	Aufbau von Kommunikationsprozessen . . . . .	114
5.10	Durchführen von Nachvorfallsbehandlungen . . . . .	115
5.11	Integration in Disaster-Recovery- und Business-Continuity-Prozesse . . . . .	116
5.12	Zwischenfazit . . . . .	116
5.13	Fazit und Ausblick . . . . .	117
	Literatur . . . . .	117

## Teil II Vorgehensweise nach BSI IT-Grundschutz

<b>6</b>	<b>Vorgehensweise nach BSI IT-Grundschutz . . . . .</b>	<b>121</b>
6.1	Inhaltliche Übersicht . . . . .	121
6.2	Einführung in das Vorgehen nach IT-GS . . . . .	122
6.3	Initiierung des Informationssicherheitsprozesses . . . . .	123
6.3.1	Übernahme der Verantwortung durch die Leitungsebene . . . . .	123
6.3.2	Konzeption und Planung des IS-Prozesses . . . . .	124
6.3.3	Erstellung einer Leitlinie . . . . .	126
6.3.4	Die Organisation des IS-Prozesses . . . . .	127
6.3.5	Bereitstellung der Ressourcen für die IS . . . . .	129
6.3.6	Einbindung aller Mitarbeiter in den IS-Prozess . . . . .	131
6.4	Erstellung einer Sicherheitskonzeption . . . . .	132
6.4.1	Definition des Informationsverbunds . . . . .	132
6.4.2	Strukturanalyse . . . . .	133
6.4.3	Schutzbedarfsfeststellung . . . . .	134
6.4.4	Modellierung des IT-Verbunds . . . . .	137
6.4.5	Basis-Sicherheitscheck . . . . .	138
6.4.6	Ergänzende Sicherheits- und Risikoanalyse . . . . .	139
6.5	Umsetzung der Sicherheitskonzeption . . . . .	140
6.5.1	Sichtung der Ergebnisse . . . . .	141
6.5.2	Kosten-Aufwand-Abschätzung . . . . .	141
6.5.3	Umsetzungsreihenfolge festlegen . . . . .	142
6.5.4	Festlegung von Aufgaben und Verantwortung . . . . .	142
6.5.5	Begleitende Maßnahmen . . . . .	143
6.6	Aufrechterhaltung und Verbesserung . . . . .	143
6.6.1	Überprüfung des IS-Prozesses . . . . .	143

6.6.2 Informationsfluss im IS-Prozess	145
6.7 Zertifizierung	146
6.8 Fazit	147
Literatur	147

### **Teil III Praxisbeispiele**

<b>7 Bausteine für einen sicheren IT-Betrieb</b>	151
7.1 Von der Anforderung zum sicheren Betrieb	151
7.2 Anforderungsanalyse	156
7.3 Absicherung der Lieferkette	158
7.4 Dokumentenlandkarte	161
7.5 Pseudonymisierung	162
7.6 IT-Sicherheitsgesetz (ITSiG)	164
7.7 Fazit	169
Literatur	169
<b>8 Praxisbausteine zum IT-Grundschutz</b>	171
8.1 Modellierung nach BSI IT-Grundschutz	171
8.2 Basis-Sicherheitscheck nach IT-Grundschutz	177
8.3 Risikoanalyse nach BSI IT-Grundschutz 100-3	180
8.4 Auswahlkriterien für ein IT-Grundschutz-Tool	187
8.5 Fazit	189
Literatur	189
<b>9 Zur Abgrenzung eines Informationsverbundes</b>	191
9.1 Einführung	192
9.2 IV-Abgrenzung mittels dem Regelsatz der Beherrschung	193
9.3 Risikoorientierte Schnittstellenbetrachtung des IV	196
9.4 Fazit	200
Literatur	200
<b>Glossar</b>	201
<b>Sachverzeichnis</b>	207

Informationssicherheits-Management  
Leitfaden für Praktiker und Begleitbuch zur  
CISM-Zertifizierung

Wegener, C.; Milde, Th.; Dolle, W.

2016, XXII, 211 S. 55 Abb., Hardcover

ISBN: 978-3-662-49166-9