

Inhaltsübersicht

Vorwort	1
A. Regulatorische Rahmenbedingungen und Tendenzen	5
B. Praxisfragen des Informationssicherheitsmanagements	87
C. Wichtige IKS-Schnittstellen des Informationssicherheitsmanagements	235
Vita der Herausgeber	301

Inhaltsverzeichnis

Vorwort	1
A. Regulatorische Rahmenbedingungen und Tendenzen	5
I. Aus MaRisk und BAIT – aufsichtsrechtliche Erwartungshaltung an den Informationssicherheitsbeauftragten und Prüfungspraxis (<i>Kühn</i>)	5
1. Einleitung – oder: Einige Worte zum Umfeld dieses Beitrags	5
2. Aufsichtsrechtliche Erwartungshaltungen an die IT-Steuerung einer Bank – und was der Informationssicherheitsbeauftragte damit zu tun hat	6
3. Grundlagen des Informationsrisikomanagements	10
a) Informationsrisikomanagement in den BAIT	11
b) Informationsrisikomanagement im Regelkreis	14
4. Vom Informationsrisiko- zum Informationssicherheitsmanagement	22
a) Informationssicherheitsmanagement in der schriftlich fixierten Ordnung	22
b) Informationssicherheitsmanagement in der Aufbauorganisation	24
c) Wesentliche weitere Arbeitsschwerpunkte des Informationssicherheitsmanagements	28
5. Datenqualität – (k)ein Thema der Informationssicherheit?	28
6. Zusammenfassung	34
II. Kritische Infrastrukturen im Sektor Finanz- und Versicherungswesen (<i>Finkler/Gampe</i>)	36
1. Einführung	36
a) Gesamtwirtschaftliche Bedeutung Kritischer Infrastrukturen	36
b) Kooperative Zusammenarbeit von Wirtschaft und Staat	37
2. Rechtsgrundlagen	38

a)	Rechtsgrundlagen für Kritische Infrastrukturen	38
b)	Rechtsgrundlagen im Finanzsektor: SSM-Verordnung, Kreditwesengesetz und Zahlungsdiensteaufsichtsgesetz	44
3.	Grundsätzliche Anforderungen an KRITIS-Betreiber gemäß §§ 8a und b BSIG	46
a)	Pflicht zur Prävention bei der Sicherheit in der Informationstechnik für Betreiber Kritischer Infrastrukturen gemäß § 8a BSIG	46
b)	Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen gemäß § 8b BSIG	50
4.	Spezifische Anforderungen an KRITIS-Betreiber im Finanzsektor	54
a)	Bankaufsichtliche Anforderungen an die IT	54
b)	Bereichsspezifische Audits im Bankenbereich	54
c)	Bereichsspezifische Meldepflichten im Bankenbereich	55
5.	Zusammenarbeit von BSI und BaFin bei der Aufsicht über Kritische Infrastrukturen im Finanzsektor	57
III.	Cloud Computing für Kreditinstitute – Sicherheit, Regulierung und Governance (<i>Held</i>)	58
1.	Einleitung	58
2.	Grundlagen des Cloud Computing	59
a)	Was ist eigentlich Cloud Computing?	59
b)	Cloud-spezifische Risiken	63
3.	Regulierung und Standards	70
a)	Cloud Computing aus regulatorischer Sicht	70
b)	Gängige Standards zum Cloud Computing	73

4.	Wesentliche Aspekte beim Vorgehen zum Cloud-Einsatz	80
a)	Strategie	80
b)	Regelung der Cloud-Nutzung	81
c)	Realistische Planung und klare Definition der Anforderungen	81
d)	Festlegung von Schutzbedarfen, Sicherheitsanforderungen und -maßnahmen	82
e)	Transparenz herstellen!	83
5.	Zusammenfassung	84
B. Praxisfragen des Informationssicherheitsmanagements		87
I.	Herausforderungen und Lösungen beim Betreiben des Informationssicherheitsmanagements in einer Großsparkasse (<i>Kizilelma</i>)	89
1.	Ansatz für das Informationssicherheits- Managementsystem als Regelsystem	90
a)	Aufbau eines technischen Regelsystems	90
b)	Ableitungen aus dem Regelsystemgedanken für das ISMS	91
c)	Detailbetrachtungen	92
2.	Aufbauorganisation Implementierung des ISMS	98
3.	Prozess des ISMS	100
a)	Unternehmenswerte	101
b)	Strukturanalyse	101
c)	Schutzbedarfsfeststellung	101
d)	Soll/Ist-Vergleich	101
e)	Risikomanagement in der Informationssicherheit	102
f)	IS-Organisation	106
g)	Bedrohungen und Konzepte	106
4.	Cyberisiken	107
a)	IDENTIFY	108
b)	PROTECT	110
c)	DETECT	113
d)	RESPOND	114
e)	RECOVER	115

5.	Fazit	116
II.	Abstimmungsprozess zur Informationssicherheit (<i>Wagner</i>)	117
1.	Einleitung	117
2.	Zielsetzung des Abstimmprozesses	117
3.	Abstimmungsprozesse	118
a)	Abstimmprozesse zur Errichtung einer IS-Risikomanagementorganisation	118
b)	Operative Abstimmungsprozesse – CERT	128
4.	Fazit	134
III.	Informationssicherheitsmanagement im Rechenzentrum (<i>Dinger</i>)	136
1.	Einleitung	136
a)	Wer ist eigentlich die Fiducia & GAD IT AG?	136
b)	Sicherheitsmanagement im Wandel	136
c)	Ziel: angemessenes Sicherheitsniveau	137
d)	Informationssicherheit ist mehr als Datensicherheit	137
2.	Aktuelle Herausforderungen	138
a)	Cybercrime ist »erfolgreich«: Schlicht, weil es ums Geld geht!	138
b)	Auf dem Weg zu Informationssicherheitsrisiken	141
c)	Regulatorik und Compliance effizient meistern	143
d)	Das Rechenzentrum eines anderen <i>oder</i> Cloud Computing integrieren	143
3.	Lösungsstrategien	144
a)	Die Rolle des Sicherheitsmanagements im Unternehmen	145
b)	Vom Business-Impact her denken	149
c)	Sicherheitskonzepte und Management von Informationssicherheitsrisiken	150
d)	Sicherheitsstrategie: Prävention, Detektion, Reaktion	158
e)	Sicherheitsmanagement auf dem Weg zum »Business Enabler«	163

4.	Fazit & Ausblick	164
IV.	Schutzbedarfsdefinition und Schutzbedarfsfeststellung – Fundamente des Informationssicherheitsmanagements (<i>Ebrlich</i>)	166
1.	Einführung	166
a)	Prozess des Informationssicherheits- managements	167
b)	Unternehmenswerte	168
c)	Verantwortlichkeiten bei der Schutzbedarfsfeststellung	169
d)	Kategorien für den Schutzbedarf	169
e)	Schutzziele	170
2.	Definition, Begründung und Feststellung des Schutzbedarfs	174
a)	Schutzbedarfsdefinitionen	175
b)	Benennung von realistischen Schutzbedarfsdefinitionen	176
c)	Probleme bei der Schutzbedarfsdefinition	179
d)	Feststellung des Schutzbedarfs	181
e)	Beispiel zur Feststellung des Schutzbedarfs	181
f)	Vererbung des Schutzbedarfs und deren Auswirkung	184
g)	Begründung des Schutzbedarfs	185
h)	Schulung der Mitarbeiter	187
i)	Inhalte für eine Schulung	188
j)	Leitfaden zur Schutzbedarfsfeststellung	189
V.	Rahmenbedingungen (<i>Hoffmann/Kullmann/Müller</i>)	190
1.	Problemstellung	190
2.	Betriebswirtschaftlicher Nutzen	190
3.	Gesetzliche & aufsichtsrechtliche Anforderungen	190
VI.	Implementierung eines geeigneten eBMS (<i>Hoffmann/Kullmann/Müller</i>)	192
1.	Grundsatzentscheidung zur Einführung	192
2.	Ansetzen eines Projektes	193

a)	Innerbetriebliche Vorarbeiten	193
b)	Systemauswahl	199
c)	Konzeptionelle Einbindung	202
3.	Anbindung Drittanwendungen	204
4.	Einbindung technischer User	205
VII.	Betrieb des eBMS (<i>Hoffmann/Kullmann/Müller</i>)	206
1.	Workflows	206
a)	Beantragung	207
b)	Vergabe	208
c)	Entzug	208
2.	Rezertifizierung	208
3.	Pflegearbeiten	209
a)	Allgemeine Änderungen	209
b)	Soll-Konzepte	209
4.	Soll-Ist Abgleich	209
5.	Typische Probleme im laufenden Betrieb	210
6.	Soll-Konzepte	210
VIII.	Erfahrung nach 1 Jahr Betrieb eBMS (<i>Hoffmann/Kullmann/Müller</i>)	211
1.	IT-Sicherheit	211
2.	Vorteile	212
IX.	Fazit (<i>Hoffmann/Kullmann/Müller</i>)	213
X.	Individuelle Datenverarbeitung – Herausforderung für die Informationssicherheit (<i>Graf</i>)	214
1.	Rahmenbedingungen	214
a)	Bedeutung von Anwendungen	214
b)	Aufsichtsrechtlicher Rahmen der MaRisk und BAIT	215

2.	Individuelle Datenverarbeitung	215
	b) Systementwicklung	220
	c) Individuelle Datenverarbeitung in Kreditinstituten	221
3.	Anforderung an die individuelle Datenverarbeitung im Kontext der Informationssicherheit	222
	a) Risikomanagement	222
	b) Entwicklung von IDV-Anwendungen	225
	c) Rolle des Informationssicherheitsbeauftragten (ISB) im Kontext IDV	232
C. Wichtige IKS-Schnittstellen des Informationssicherheitsmanagements		235
I.	Dienstleistersteuerung und Informationssicherheit (<i>Kühn</i>)	237
	1. Einleitung	237
	2. Grundlagen und Grundsätze	238
	a) Um was geht es eigentlich – Begriffe und ihre Folgen?	238
	b) Und was bedeutet das für den Steuerungsansatz?	242
	3. Grundlagen der Steuerung von IT-Dienstleistern aus Sicht des Informationssicherheitsbeauftragten	244
	4. Weitere Rollen der Steuerung von IT-Dienstleistern aus Sicht des Informationssicherheitsbeauftragten	247
	a) Lieferantenverantwortlicher	248
	b) Weitere Einheiten der 2. und 3. Verteidigungslinie	249
	c) Zentrale Dienstleistersteuerung	250
	5. Typische Fragestellungen aus Sicht des Informationssicherheitsbeauftragten	251
	6. Zusammenfassung	254
II.	Optimale Schnittstellengestaltung von Datenschutz und Informationssicherheit (<i>Seip</i>)	256
	1. Überblick technischer Regelungen aus der EU-DSGVO	257
	2. Grundlegende Gemeinsamkeiten der Tätigkeiten	258

3.	Schnittstellen in der Methodik von Schutzbedarfs- und Risikoanalyse	260
a)	Grundsätze für die Verarbeitung (Art. 5)	260
b)	Sicherheit der Verarbeitung (Art. 32)	262
c)	Datenschutzfolgeabschätzung (Art 35)	263
4.	Schnittstellen bei präventiven Maßnahmen	267
a)	Verantwortung für technische und organisatorischen Maßnahmen (Artikel 24)	267
b)	Auftragsverarbeiter (Artikel 28)	268
c)	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25)	270
d)	Recht auf Löschung (»Recht auf Vergessenwerden«) (Artikel 17)	271
5.	Abgrenzungen	272
a)	Datenminimierung	272
b)	Unabhängigkeit	273
c)	Meldepflicht von Datenschutz- und Informationssicherheitsvorfällen	273
6.	Fazit	274
III.	IT-Revision des Informationssicherheitsmanagements im genossenschaftlichen Finanzverbund (<i>Korn</i>)	276
1.	Bedeutung des Informationssicherheitsmanagements aus Revisionssicht bei Genossenschaftsbanken	276
a)	Ausgangslage, Situation in Genossenschaftsbanken	276
b)	Prüfung des Informationssicherheitsmanagements	278
c)	Bedeutung des Informationssicherheitsbeauftragten in der Genossenschaftsbank	280
2.	Organisation und Struktur des Informationssicherheitsmanagements in Genossenschaftsbanken	282
a)	Strukturen, Arbeitsteilung im genossenschaftlichen Finanzverbund	282
b)	Informationssicherheitsbeauftragter in Genossenschaftsbanken	284
c)	Kombination von Tätigkeiten beim Informationssicherheitsbeauftragten	286

d)	Organisation durch ein IT-Sicherheitsgremium	287
e)	Externe Unterstützung des Informationssicherheitsbeauftragten	288
3.	Prüfungsaspekte zum Informationssicherheits- management	289
a)	IT-Revision im Kontext der Funktion des Informationssicherheits- beauftragten	289
b)	Aufbauorganisation der Funktion des Informationssicherheitsbeauftragten	290
c)	Qualifikation des Informationssicherheits- beauftragten	292
d)	Aufgaben des Informationssicherheits- beauftragten	292
e)	Kontrolltätigkeiten des Informationssicherheits- beauftragten	294
f)	Weitere Fragen zum Informationssicherheits- management	296
g)	Auslagerungen/Dienstleistersteuerung	298
4.	Zusammenfassung	298
	Vita der Herausgeber	301
	Vita Dr. Markus Held	301
	Vita Prof. Dr. Ralf Kühn	301