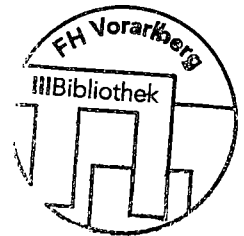


# Informationssicherheits- managementsystem

Damoklesschwert Daten-Gau –  
Systematische Prüfung  
und wirksame Prävention

Institut für Interne Revision Österreich –  
IIA Austria



**Linde**  
*international*

# Inhaltsverzeichnis

Vorwort .....	V
Autorenverzeichnis .....	VII
Abbildungsverzeichnis .....	XIII
Abkürzungsverzeichnis .....	XV
<b>Einleitung</b> .....	1
<b>1. Grundlagen und Ziele für ein Informationssicherheitsmanagementsystem (ISMS)</b> .....	2
1.1. Managementprinzipien .....	2
1.1.1. Corporate Governance .....	2
1.1.2. Internes Kontrollsystem (IKS) .....	4
1.1.3. Risikomanagementsystem (RMS) .....	5
1.1.4. Interne Revision (IR) .....	5
1.1.5. Compliance Management System (CMS) .....	5
1.1.6. Informationssicherheitsmanagementsystem (ISMS) .....	6
1.2. Informationssicherheitsstrategie .....	7
1.3. Stakeholder .....	9
1.3.1. Management .....	9
1.3.2. Chief Information Security Officer (CISO) .....	9
1.3.3. IT-Bereich .....	10
1.3.4. Mitarbeiter .....	10
1.3.5. Externe Personengruppen .....	10
1.4. Informationssicherheitsmanagementprozess .....	10
<b>2. Vorschriften und Empfehlungen</b> .....	13
2.1. Gesetze und Verordnungen in Österreich .....	13
2.1.1. Datenschutzgesetz 2000 (DSG); Fassung vom 7.7.2016 .....	13
2.1.2. Arbeitsverfassungsgesetz .....	14
2.1.3. Telekommunikationsgesetz .....	15
2.1.4. Signaturgesetz .....	15
2.1.5. Dienstnehmerhaftpflichtgesetz .....	16
2.1.6. Betrugsbekämpfungsgesetz 2010 .....	16
2.1.7. Unternehmensrechts-Änderungsgesetz (URÄG 2008) .....	17
2.1.8. KFS/DV1 .....	17
2.2. Gesetze und Verordnungen in Deutschland .....	18
2.2.1. KontraG .....	18
2.2.2. Bundesdatenschutzgesetz (BDSG) .....	18
2.2.3. Arbeitnehmerhaftung .....	19
2.2.4. Telekommunikationsgesetz (TKG) .....	19
2.2.5. Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) .....	20
2.2.6. IT-Sicherheitsgesetz .....	20

2.3.	Normen und Leitfäden .....	21
2.3.1.	Normenreihe ISO/IEC 27000 .....	21
2.3.2.	Normenreihe ISO/IEC 20000 .....	22
2.3.3.	Control Objectives for Information and Related Technology (COBIT) .....	22
2.3.4.	Information Technology Infrastructure Library (ITIL) .....	22
2.3.5.	Bundesamt für Sicherheit in der Informationstechnik (BSI) .....	23
2.3.6.	Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) .....	23
2.4.	Interne Richtlinien .....	24
2.5.	Zukünftige Entwicklungen .....	24
<b>3.</b>	<b>Die Interne Revision als Prüfer und Projektleiter von IT-Sicherheitsaudits ..</b>	<b>27</b>
3.1.	IT-Sicherheitsaudits .....	27
3.2.	Rahmenkonzepte und Prüfansätze .....	29
3.2.1.	Rahmenkonzepte für IT-Sicherheitsaudits .....	30
3.2.2.	Prüfansatz für IT-Sicherheitsaudits .....	30
3.3.	Festsetzung des Prüfungsumfangs (Scoping) .....	31
3.3.1.	Konkretisierung durch laufenden Erkenntnisgewinn: Das mehrphasige Prüfprogramm und andere Herangehensweisen .....	32
3.3.2.	BSI-Leitfaden .....	33
3.3.3.	Informationsbeschaffung .....	34
3.3.4.	Prüfungsabgrenzung .....	36
3.3.5.	Prüfmethodik .....	37
3.3.6.	Prüfprogramm/Prüfkriterien/Field Work Matrix .....	38
3.4.	Interne Revision als Projektleiter von IT-Sicherheitsaudits .....	38
3.4.1.	Abwicklung von Prüfungsaufträgen mit externen Prüfern .....	39
3.4.2.	Mitwirkung der Internen Revision an Prüfungsaufträgen von externen Prüfern .....	39
<b>4.</b>	<b>Organisatorische Aspekte .....</b>	<b>41</b>
4.1.	Sicherheitsorganisation .....	41
4.1.1.	Aufbau- und Ablauforganisation .....	41
4.1.2.	Organisation der Systemlandschaft .....	43
4.1.3.	Informationsklassifizierung .....	44
4.1.4.	Umgang mit Sicherheitsvorfällen .....	46
4.2.	Zugriffssicherheit (Zugriffsmanagement) .....	48
4.2.1.	Berechtigungskonzept .....	49
4.2.2.	Berechtigungsvergabe und -entzugsprozess .....	51
4.2.3.	Prävention von unfreiwilligem Datenabfluss (Data Leakage) .....	53
4.2.4.	Penetration Testing .....	54
4.3.	Änderungsmanagement .....	56
4.3.1.	Prozessbeschreibung Änderungsmanagement .....	56
4.3.2.	Sicherheitsrelevante Aspekte des Änderungsmanagements .....	58
4.4.	Business Continuity Management .....	59
4.4.1.	Analyse der Geschäftsprozesse zur Sicherung des IT-Betriebs .....	60
4.4.2.	Notfallvorsorge und Disaster Recovery .....	62
4.4.3.	Absicherung der Maßnahmen durch wiederkehrende Tests .....	64

<b>5. Informationstechnik</b> .....	66
5.1. Informationstechnik und Informationssicherheit .....	66
5.1.1. Informationstechnik und Risiko .....	67
5.1.2. Auswirkungen eines ISMS auf die Sicherheitsmaßnahmen für die IT .....	68
5.2. IT-Services: Geschäftsprozessnahe Applikationen .....	71
5.2.1. Erläuterung des Prüfbereichs .....	71
5.2.2. Risikodarstellung für Applikationen .....	71
5.2.3. Eigen-/Fremdprüfung .....	72
5.3. IT-Services: Sichere Softwareentwicklung .....	73
5.3.1. Erläuterung des Prüfbereichs .....	73
5.3.2. Risikodarstellung für Softwareentwicklung .....	74
5.3.3. Eigen-/Fremdprüfung .....	74
5.4. IT-Services: Outsourcing und Cloud-Dienste .....	75
5.4.1. Erläuterung des Prüfbereichs .....	75
5.4.2. Risikodarstellung für Outsourcing und Cloud-Dienste .....	78
5.4.3. Eigen-/Fremdprüfung .....	79
5.5. IT-Services: Datensicherung, Archivierung und Datenträger .....	80
5.5.1. Erläuterung des Prüfbereichs .....	80
5.5.2. Risikodarstellung für Datensicherung, Archivierung und Datenträger .....	84
5.5.3. Eigen-/Fremdprüfung .....	84
5.6. IT-Infrastruktur: Mobiles Arbeiten .....	85
5.6.1. Erläuterung des Prüfbereichs .....	85
5.6.2. Risikodarstellung für mobiles Arbeiten .....	85
5.6.3. Eigen-/Fremdprüfung .....	86
5.7. IT-Infrastruktur: End Point Security .....	89
5.7.1. Erläuterung des Prüfbereichs .....	89
5.7.2. Risikodarstellung für End Point Security .....	89
5.7.3. Eigen-/Fremdprüfung .....	90
5.8. IT-Infrastruktur: Server, Storage, Betriebssysteme, Plattformen und Datenbanksysteme .....	91
5.8.1. Erläuterung des Prüfbereichs .....	91
5.8.2. Risikodarstellung für Server, Storage, Betriebssysteme, Plattformen und Datenbanksysteme .....	92
5.8.3. Eigen-/Fremdprüfung .....	93
5.9. IT-Infrastruktur: Netzwerke/WLAN .....	97
5.9.1. Erläuterung des Prüfbereichs .....	97
5.9.2. Risikodarstellung für Netzwerke/WLAN .....	100
5.9.3. Eigen-/Fremdprüfung .....	102
5.10. IT-Infrastruktur: Physische Sicherheit .....	106
5.10.1. Erläuterung des Prüfbereichs .....	106
5.10.2. Risikodarstellung für physische Sicherheit .....	108
5.10.3. Eigen-/Fremdprüfung .....	108
<b>6. Faktor Mensch in der Informationssicherheit</b> .....	111
6.1. Einstellung und Verhalten gegenüber Informationssicherheit .....	111
6.1.1. Der Mensch in seinem Informationsumfeld .....	111

6.1.2.	Verhalten des Menschen am Arbeitsplatz .....	114
6.2.	Bedeutung der Rolle Mitarbeiter .....	115
6.2.1.	Rolle des Menschen im Umgang mit Information generell .....	115
6.2.2.	Bedeutung der Rolle IT-Mitarbeiter in der Informationssicherheit .....	116
6.2.3.	Schatten-IT .....	118
6.3.	Organisatorische Aspekte des Faktors Mensch .....	120
6.4.	Social Engineering (SE) .....	123
<b>7.</b>	<b>Smart Meter, Smart Grid, SCADA-Systeme und Industrial Control Systems .....</b>	<b>129</b>
<b>8.</b>	<b>Umfrage zu ISMS .....</b>	<b>130</b>
8.1.	Die ISMS-Umfrage im Überblick .....	130
8.2.	Umfrageergebnisse .....	131
8.3.	Abgeleitete Erkenntnisse .....	133
	Literaturliste .....	135
	Stichwortverzeichnis .....	139