

Inhalt

Geleitwort von Wolfgang Lassmann	19
Geleitwort von Monika Egle	21
Geleitwort von Jose Estrada	23
Einleitung	25

Teil I: Grundlagen des Risikomanagements und der IT-Sicherheit

1 Risiko- und Kontrollmanagement 33

1.1 Sicherheitsziele	34
1.2 Unternehmenswerte	37
1.2.1 Typen von Unternehmenswerten	38
1.2.2 Klassifizierung von Unternehmenswerten	39
1.3 Risiken	41
1.3.1 Risikotypen	42
1.3.2 Klassifizierung von Risiken	46
1.4 Kontrollen	47
1.4.1 Kontrolltypen	47
1.4.2 Klassifizierung von Kontrollen	48

2 Enterprise-Risk-Management-Strategie 51

2.1 Status quo	53
2.2 Komponenten	55
2.2.1 Rahmenbedingungen	59
2.2.2 Strategie	60
2.2.3 Methoden	61
2.2.4 Best Practices	62
2.2.5 Dokumentation	63
2.3 Best Practices einer SAP-Sicherheitsstrategie	63
2.3.1 Vorgehensweise	64
2.3.2 Prinzip der Informationsverantwortung	73
2.3.3 Identity Management	78

3 Anforderungen 85

3.1 Rechtliche Anforderungen	85
3.1.1 Sarbanes-Oxley Act	86
3.1.2 SOX-Umsetzung in Japan	96

3.1.3	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme	98
3.1.4	International Financial Reporting Standards	100
3.2	Branchenspezifische Anforderungen	101
3.2.1	Nahrungsmittel- und pharmazeutische Industrie und Medizintechnik	101
3.2.2	Finanz-, Kredit- und Bankwirtschaft – Basel (I, II, III) ...	103
3.2.3	Chemiestoffe und Umweltschutz	106
3.3	Innerbetriebliche Anforderungen	108
4	Sicherheitsstandards	111
4.1	Internationale Sicherheitsstandards	112
4.1.1	ISO/IEC 27002:2005	112
4.1.2	CobiT	118
4.1.3	IT Infrastructure Library	121
4.1.4	COSO	123
4.2	Länderspezifische Sicherheitsstandards	129
4.2.1	NIST Special Publication 800-12	129
4.2.2	IT-Grundschutz-Kataloge	133
4.2.3	PIPEDA	136
5	Informationstechnische Sicherheit	141
5.1	Kryptografie	142
5.1.1	Symmetrisches Verschlüsselungsverfahren	142
5.1.2	Asymmetrisches Verschlüsselungsverfahren	143
5.1.3	Kryptografie mit elliptischen Kurven	145
5.1.4	Hybrides Verschlüsselungsverfahren	146
5.1.5	Secure-Socket-Layer-Verschlüsselung	148
5.1.6	Hash-Verfahren	149
5.1.7	Digitale Signatur	150
5.2	Public-Key-Infrastruktur	153
5.3	Authentisierungsverfahren	156
5.3.1	Benutzername und Passwort	156
5.3.2	Challenge Response	157
5.3.3	Kerberos	157
5.3.4	Secure Token	159
5.3.5	Digitales Zertifikat	160
5.3.6	Biometrische Verfahren	160

5.4	Netzwerkgrundlagen und Sicherheitsaspekte	161
5.4.1	OSI-Schichtenmodell	161
5.4.2	Firewall-Technologien im Überblick	168

Teil II: Sicherheit in SAP NetWeaver und Anwendungssicherheit

6 ERM Navigation Control Map 173

6.1	SAP-Anwendungen	181
6.2	Komponenten von SAP NetWeaver	183
6.3	Sicherheitstechnologien	186
6.3.1	Berechtigungen, Risiko- und Änderungsmanagement und Revision	186
6.3.2	Identity Management	188
6.3.3	Gesicherte Authentisierung und Single Sign-on	191
6.3.4	Technische Sicherheit	191
6.4	Einflussfaktoren	193

7 Webservices, Enterprise Services und serviceorientierte Architekturen 195

7.1	Einführung und technische Grundlagen	197
7.2	Sicherheitskriterien für Webservices	202
7.2.1	Sicherheit und Risikomanagement für service- orientierte Architekturen	207
7.2.2	SAP Enterprise Services	208
7.2.3	Sicherheitsrichtlinien für SAP Enterprise Services	212
7.3	Serviceorientierte Architekturen und Governance	215

8 GRC-Lösungen in SAP BusinessObjects 219

8.1	Einführung und Funktionalität	219
8.1.1	Ziele der GRC-Lösungen in SAP BusinessObjects	220
8.1.2	Methoden der GRC-Lösungen in SAP BusinessObjects	221
8.1.3	Planung des Einsatzes der GRC-Lösungen in SAP BusinessObjects	223
8.1.4	GRC-Lösungen von SAP BusinessObjects im Überblick	224
8.2	SAP BusinessObjects Risk Management	228
8.2.1	Hauptkomponenten	229
8.2.2	Phasen	230
8.2.3	Verantwortlichkeiten	236
8.2.4	Berichtswesen	238

8.3	SAP BusinessObjects Access Control	239
8.3.1	Allgemeine Anforderungen an das SAP-Berechtigungssystem	239
8.3.2	Hauptkomponenten	247
8.4	SAP BusinessObjects Process Control	256
8.4.1	Eigene Startseite	258
8.4.2	Konformitätsstruktur	259
8.4.3	Bewertungseinrichtung	261
8.4.4	Bewertungsergebnisse	262
8.4.5	Zertifizierung	263
8.4.6	Berichtszentrum	263
8.4.7	Zertifizierung	265
8.5	SAP BusinessObjects Global Trade Services	265
8.5.1	Compliance Management	268
8.5.2	Customs Management	270
8.5.3	Risk Management	272
8.5.4	Electronic Compliance Reporting	275
8.5.5	Systemadministration	275
8.6	SAP Environment, Health, and Safety Management	275
8.6.1	Übersicht	276
8.6.2	Chemikaliensicherheit	278
8.6.3	Umwelt-, Gesundheits- und Arbeitsschutz	280
8.6.4	Einhaltung produktbezogener Umweltauflagen	280
8.6.5	Compliance- und Emissionsmanagement	281
8.7	SAP BusinessObjects Sustainability Performance Management	283

9 SAP NetWeaver Application Server 285

9.1	Einführung und Funktionalität	285
9.2	Risiken und Kontrollen	288
9.3	Anwendungssicherheit	298
9.3.1	Technisches Berechtigungskonzept für Administratoren	298
9.3.2	Berechtigungskonzept für Java-Anwendungen	307
9.3.3	Einschränkung der Berechtigungen bei RFC-Aufrufen	313
9.4	Technische Sicherheit	317
9.4.1	Einführung eines Single-Sign-on- Authentisierungsmechanismus	317
9.4.2	Anbindung des SAP NetWeaver Application Servers an ein zentrales LDAP-Verzeichnis	320

9.4.3	Änderung der Standardpasswörter für Standardbenutzer	321
9.4.4	Sicherheitskonfiguration des SAP-Gateways	322
9.4.5	Einschränkung des Betriebssystemzugriffs	324
9.4.6	Wichtige sicherheitsrelevante Systemparameter konfigurieren	325
9.4.7	Konfiguration von verschlüsselten Kommunikationsverbindungen (SSL und SNC)	328
9.4.8	Überflüssige Internetdienste einschränken	333
9.4.9	Sichere Netzwerkarchitektur für den Einsatz des SAP NetWeaver Application Servers für das Internet ...	335
9.4.10	Einführung eines Application Level Gateways zur Absicherung von Internetanwendungen	336
9.4.11	Einführung von Härtingsmaßnahmen auf Betriebssystemebene	336
9.4.12	Einführung eines Qualitätssicherungsprozesses für die Softwareentwicklung	337
9.4.13	Sicherheits- und Berechtigungsprüfungen in selbst entwickeltem ABAP- und Java-Programmcode	340

10 SAP NetWeaver Business Warehouse **343**

10.1	Einführung und Funktionalität	343
10.2	Risiken und Kontrollen	344
10.3	Anwendungssicherheit	348
10.3.1	Berechtigungen	348
10.3.2	Analyseberechtigungen	352
10.3.3	Weitere Konzepte	354
10.4	Technische Sicherheit	358

11 BI-Lösungen in SAP BusinessObjects **361**

11.1	Einführung und Funktionalität	362
11.2	Risiken und Kontrollen	363
11.3	Anwendungssicherheit	368
11.3.1	Berechtigungskonzept für SAP BusinessObjects	368
11.3.2	Anwendungsbeispiele für Berechtigungskonzepte	376
11.3.3	Sicherung des administrativen Zugangs und des Gastbenutzers	380
11.3.4	Konfiguration von Passwortregeln	380
11.3.5	Anwendungsberechtigungen	382

11.4	Technische Sicherheit	382
11.4.1	Externe Authentisierung und Single Sign-on	383
11.4.2	Nutzung der Audit-Funktion	384
11.4.3	Netzwerkkommunikation mittels SSL und CORBA-Services	384

12 SAP NetWeaver Process Integration 385

12.1	Einführung und Funktionalität	386
12.2	Risiken und Kontrollen	389
12.3	Anwendungssicherheit	396
12.3.1	Berechtigungen für den Enterprise Services Builder	396
12.3.2	Passwörter und Berechtigungen für technische Servicebenutzer	399
12.3.3	Berechtigungen für den administrativen Zugang zu SAP NetWeaver PI	400
12.3.4	Passwortregeln für Administratoren	401
12.4	Technische Sicherheit	401
12.4.1	Definition von technischen Servicebenutzern für Kommunikationsverbindungen während der Laufzeit	401
12.4.2	Einrichtung der Verschlüsselung für Kommunikationsverbindungen	402
12.4.3	Digitale Signatur für XML-basierte Nachrichten	409
12.4.4	Verschlüsselung von XML-basierten Nachrichten	414
12.4.5	Netzwerkseitige Absicherung von Integrations- szenarien	415
12.4.6	Audit des Enterprise Services Builders	416
12.4.7	Absicherung des File-Adapters auf Betriebssystem- ebene	418
12.4.8	Verschlüsselung der PI-Kommunikations- verbindungen und Webservices	419
12.4.9	Sicherheit für Webservices	420

13 SAP Partner Connectivity Kit 423

13.1	Einführung und Funktionalität	423
13.2	Risiken und Kontrollen	424
13.3	Anwendungssicherheit	428
13.4	Technische Sicherheit	429
13.4.1	Eigener technischer Servicebenutzer für jedes angeschlossene Partnersystem	430

13.4.2	Einrichtung der Verschlüsselung für Kommunikationsverbindungen	430
13.4.3	Digitale Signatur für XML-basierte Nachrichten	430
13.4.4	Netzwerkseitige Absicherung von Integrations-szenarien	430
13.4.5	Audit des Nachrichtenaustausches	430
13.4.6	Absicherung des File-Adapters auf Betriebssystemebene	431

14 Klassische SAP-Middleware 433

14.1	SAP Web Dispatcher	434
14.1.1	Einführung und Funktionalität	434
14.1.2	Risiken und Kontrollen	434
14.1.3	Anwendungssicherheit	437
14.1.4	Technische Sicherheit	438
14.2	SAProuter	446
14.2.1	Einführung und Funktionalität	446
14.2.2	Risiken und Kontrollen	447
14.2.3	Anwendungssicherheit	448
14.2.4	Technische Sicherheit	449
14.3	SAP Internet Transaction Server	450
14.3.1	Einführung und Funktionalität	451
14.3.2	Risiken und Kontrollen	454
14.3.3	Anwendungssicherheit	457
14.3.4	Technische Sicherheit	460

15 SAP NetWeaver Master Data Management 469

15.1	Einführung und Funktionalität	469
15.2	Risiken und Kontrollen	470
15.3	Anwendungssicherheit	475
15.3.1	Identity Management und Berechtigungen	475
15.3.2	Revisionssicherheit	482
15.4	Technische Sicherheit	483
15.4.1	Kommunikationssicherheit	483
15.4.2	Weitere wichtige Komponenten	484

16 SAP NetWeaver Portal 485

16.1	Einführung und Funktionalität	485
16.1.1	Technische Architektur	487

16.1.2	Bedeutung der User Management Engine	489
16.2	Risiken und Kontrollen	493
16.3	Anwendungssicherheit	503
16.3.1	Aufbau und Design von Portalrollen	503
16.3.2	Berechtigungen für die User Management Engine	510
16.3.3	Portalsicherheitszonen	511
16.3.4	Authentisierungsprüfung für iView-Zugriff	517
16.3.5	Standardportalrollen und delegierte Benutzeradministration	518
16.3.6	Abgleich der Portalrollen mit ABAP-Rollen	521
16.3.7	Änderungsmanagementprozess für neue Portalinhalte	528
16.4	Technische Sicherheit	530
16.4.1	Anschluss des SAP NetWeaver Portals an ein zentrales LDAP-Verzeichnis oder SAP-System	530
16.4.2	Einführung eines SSO-Mechanismus auf Basis einer Ein-Faktor-Authentisierung	533
16.4.3	Einführung eines SSO-Mechanismus auf Basis einer integrierten Authentisierung	536
16.4.4	Einführung eines SSO-Mechanismus auf Basis von personenbezogenen Zertifikaten	538
16.4.5	Konfiguration für den anonymen Zugriff	541
16.4.6	Sichere Erstkonfiguration	542
16.4.7	Sichere Netzwerkarchitektur	543
16.4.8	Einführung eines Application Level Gateways zur Absicherung von Portalanwendungen	546
16.4.9	Konfiguration von verschlüsselten Kommunikationsverbindungen	550
16.4.10	Einsatz eines Viren-Scanners zur Vermeidung einer Vireninfection	552

17 SAP NetWeaver Mobile **555**

17.1	Einführung und Funktionalität	556
17.2	Risiken und Kontrollen	558
17.3	Anwendungssicherheit	566
17.3.1	Berechtigungskonzept für mobile Anwendungen	566
17.3.2	Berechtigungskonzept für die Administration	570
17.3.3	Einschränkung der Berechtigungen des RFC-Benutzers auf Backend-Anwendungen	571
17.4	Technische Sicherheit	571

17.4.1	Einrichtung von verschlüsselten Kommunikationsverbindungen	571
17.4.2	Synchronisationskommunikation absichern	573
17.4.3	Überflüssige Dienste auf dem SAP NetWeaver Mobile-Server deaktivieren	575
17.4.4	Sichere Netzwerkarchitektur	576
17.4.5	Monitoring	577
17.4.6	Sicherer Programmcode	577

18 SAP Auto-ID Infrastructure 581

18.1	Einführung und Funktionalität	581
18.2	Risiken und Kontrollen	583
18.3	Anwendungssicherheit	587
18.3.1	Berechtigungskonzept für die SAP Auto-ID Infrastructure	587
18.3.2	Berechtigungskonzept für die Administration	587
18.3.3	Einschränkung der Berechtigungen des RFC-Benutzers auf Backend-Anwendungen	588
18.3.4	Authentisierung, Passwortregeln und Sicherheit	589
18.4	Technische Sicherheit	589
18.4.1	Einrichtung von verschlüsselten Kommunikationsverbindungen	589
18.4.2	Überflüssige Dienste auf dem Server deaktivieren	590
18.4.3	Sichere Netzwerkarchitektur	590

19 SAP Solution Manager 591

19.1	Einführung und Funktionalität	591
19.2	Risiken und Kontrollen	595
19.3	Anwendungssicherheit	599
19.4	Technische Sicherheit	605
19.4.1	Sicherheitsmaßnahmen für den Benutzerzugang	605
19.4.2	Systemüberwachungsfunktion	606
19.4.3	RFC-Kommunikationssicherheit	606
19.4.4	Datenkommunikationssicherheit	607
19.4.5	Wichtige Komponenten von SAP NetWeaver	608

20 Berechtigungen in SAP ERP 609

20.1	Einführung und Funktionalität	609
20.2	Risiken und Kontrollen	610

20.3	Anwendungssicherheit	617
20.3.1	Authentisierung	618
20.3.2	Berechtigungen	618
20.3.3	Weitere Berechtigungskonzepte	634
20.3.4	Best-Practice-Lösungen	645
20.4	Technische Sicherheit	653

21 SAP ERP Human Capital Management und Datenschutz ... 655

21.1	Einführung und Funktionalität	655
21.1.1	Datenschutz im Personalwesen	656
21.1.2	Technische und organisatorische Maßnahmen	656
21.2	Risiken und Kontrollen	659
21.3	Anwendungssicherheit	666
21.3.1	Personalstammdatenberechtigungen	668
21.3.2	Bewerberberechtigungen	669
21.3.3	Personalplanungsberechtigungen	670
21.3.4	Berechtigungen im Berichtswesen	670
21.3.5	Strukturelle Berechtigungen	671
21.3.6	Berechtigungen für die Personalentwicklung	671
21.3.7	Toleranzzeiten für Berechtigungen	671
21.3.8	Berechtigungen für Prüfverfahren	672
21.3.9	Kundeneigene Berechtigungsprüfungen	672
21.3.10	Indirekte Rollenzuordnung über die Organisationsstruktur	672
21.3.11	Zusätzliche Transaktionen mit Relevanz für interne Kontrollen	673
21.4	Technische Sicherheit	674

22 SAP Strategic Enterprise Management 675

22.1	Einführung und Funktionalität	675
22.2	Risiken und Kontrollen	676
22.3	Anwendungssicherheit	679
22.4	Technische Sicherheit	679

23 SAP Customer Relationship Management 681

23.1	Einführung und Funktionalität	681
23.2	Risiken und Kontrollen	682
23.3	Anwendungssicherheit	684
23.3.1	Berechtigungen in SAP CRM	685

23.3.2	Berechtigungen für Portalrollen	691
23.4	Technische Sicherheit	692
23.4.1	Technische Absicherung der mobilen Anwendung	693
23.4.2	Weitere wichtige Komponenten	693

24 SAP Supply Chain Management 695

24.1	Einführung und Funktionalität	695
24.2	Risiken und Kontrollen	696
24.3	Anwendungssicherheit	697
24.3.1	Berechtigungen für die iPPE Workbench	698
24.3.2	Berechtigungen für das Supply Chain Planning	699
24.3.3	Berechtigungen für das SAP Event Management	699
24.4	Technische Sicherheit	700

25 SAP Supplier Relationship Management 703

25.1	Einführung und Funktionalität	703
25.2	Risiken und Kontrollen	705
25.3	Anwendungssicherheit	707
25.3.1	Wichtige Berechtigungen	708
25.3.2	Regelbasierte Sicherheitsüberprüfungen anhand von Geschäftspartnerattributen	716
25.3.3	Benutzermanagement	720
25.4	Technische Sicherheit	721
25.4.1	Sicherheitsumgebung basierend auf SAP NetWeaver ...	721
25.4.2	Sicherheitsumgebung für RFC-Kommunikation	723

26 Branchenspezifische SAP-Lösungsportfolios 725

26.1	Einführung und Funktionalität	726
26.2	Risiken und Kontrollen	727
26.3	Anwendungssicherheit	729
26.3.1	SAP MaxSecure Support	729
26.3.2	SAP-Rollenmanager	731
26.4	Technische Sicherheit	734

27 Datenbankserver 735

27.1	Einführung und Funktionalität	735
27.2	Risiken und Kontrollen	736
27.3	Anwendungssicherheit	740
27.4	Technische Sicherheit	741

27.4.1	Änderung von Standardpasswörtern	741
27.4.2	Entfernung von nicht benötigten Datenbankbenutzern	744
27.4.3	Einschränkung des Datenbankzugriffs	744
27.4.4	Erstellung und Implementierung eines Datensicherungskonzeptes	745
27.4.5	Filterung von Datenbankanfragen	746
27.4.6	Erstellung und Implementierung eines Upgrade- Konzeptes	746

28 User Interfaces 749

28.1	SAP GUI	749
28.1.1	Einführung und Funktionalität	750
28.1.2	Risiken und Kontrollen	750
28.1.3	Anwendungssicherheit	753
28.1.4	Technische Sicherheit	760
28.2	Webbrowser	763
28.2.1	Einführung und Funktionalität	763
28.2.2	Risiken und Kontrollen	764
28.2.3	Anwendungssicherheit	766
28.2.4	Technische Sicherheit	766
28.3	Mobile Endgeräte	768
28.3.1	Einführung und Funktionalität	768
28.3.2	Risiken und Kontrollen	769
28.3.3	Anwendungssicherheit	774
28.3.4	Technische Sicherheit	775

Anhang 779

A	Literatur- und Quellenverzeichnis	779
B	Die Autoren	781
	Index	783