

SAP PRESS

Handbuch SAP-Revision

Internes Kontrollsystem (IKS) und GRC, inkl. Process Control 10.0

Bearbeitet von
Maxim Chuprunov

erweitert 2012. Buch. 743 S. Hardcover

ISBN 978 3 8362 1928 0

Format (B x L): 16 x 24 cm

[Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit,
Geschäftssoftware > SAP](#)

schnell und portofrei erhältlich bei

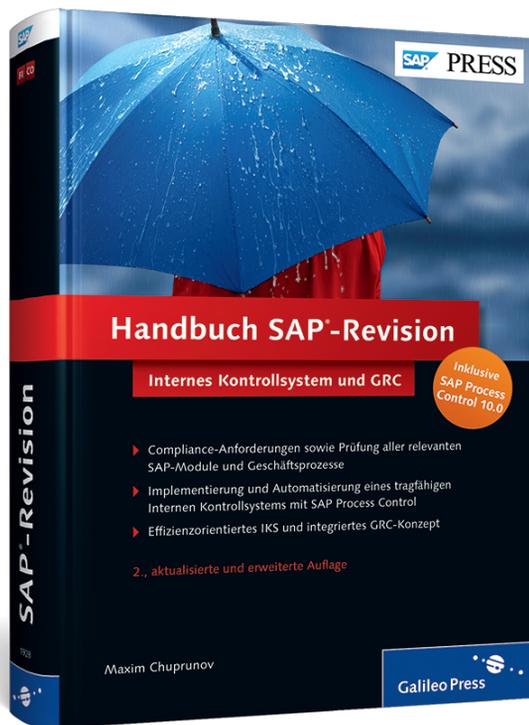

DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Maxim Chuprunov

Handbuch SAP®-Revision

Internes Kontrollsystem und GRC



Galileo Press

Bonn • Boston

Auf einen Blick

TEIL I Vom Paragrafen zum Konzept:

IKS und Compliance im ERP-Umfeld

1	Gesetzliche Anforderungen im Bereich IKS-Compliance	41
2	Der Prüfer kommt: Wann, warum und wie man damit umgeht	65
3	IKS-Anforderungen und ERP-Systeme: Grundsätze, Frameworks, Struktur	87
4	Wie geht SAP mit dem Thema Compliance um?	117

TEIL II Vom Konzept zum Inhalt:

Kontrollen in SAP ERP

5	Revisionsrelevante SAP-Basics	169
6	Generelle IT-Kontrollen in SAP ERP	215
7	Übergreifende Applikationskontrollen in SAP ERP	263
8	Kontrollen in der Finanzbuchhaltung	295
9	Kontrollmechanismen im SAP ERP-gestützten Procure-to-Pay-Prozess	355
10	Kontrollmechanismen im SAP ERP-gestützten Order-to-Cash-Prozess	385
11	Datenschutz-Compliance in SAP ERP Human Capital Management	407
12	Betrug im SAP-System	443
13	Exkurs: FDA-Compliance und Kontrollen in SAP	465
14	Exemplarische effizienz- und wirtschaftlichkeitsorientierte Analyseszenarien in SAP ERP	481

TEIL III Von Konzept und Inhalt zur Umsetzung:

Die Automatisierung eines Internen Kontrollsystems

15	IKS-Automatisierung: Wie bringt man den COSO-Cube ins Rollen?	525
16	IKS-Automatisierung mithilfe von SAP Process Control ...	549
17	Umsetzung von automatisierten Test- und Monitoring-Szenarien im SAP ERP-Umfeld	627
18	Praxis- und Projekterfahrungen	671

Inhalt

Vorwort	23
Vertrauen ist gut, Kontrolle ist billiger: Einleitung	25

Teil I Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld

1 Gesetzliche Anforderungen im Bereich IKS-Compliance	41
1.1 Begriffsdefinitionen und Abgrenzung	41
1.1.1 Compliance	41
1.1.2 Internes Kontrollsystem (IKS)	43
1.2 Gesetzliche IKS-Anforderungen in Übersee – die vielen Gesichter von SOX	44
1.2.1 SOX in den USA	45
1.2.2 SOX in Kanada (NI 52-109)	46
1.2.3 SOX in Japan	46
1.2.4 SOX in China	48
1.3 IKS-Anforderungen in Europa	48
1.3.1 8. EU-Richtlinie	49
1.3.2 Deutschland	50
1.3.3 Schweiz	52
1.3.4 Österreich	53
1.3.5 Vereinigtes Königreich Großbritannien und Nordirland	53
1.3.6 Frankreich	54
1.3.7 Dänemark	54
1.3.8 Italien	55
1.3.9 Spanien	56
1.4 IKS-Anforderungen in der Finanzbranche	56
1.4.1 Solvency II im Versicherungswesen	57
1.4.2 Basel II und III im Bankwesen	58
1.5 Unternehmenserfolg durch IKS?	60
1.6 Resümee	62

2 Der Prüfer kommt: Wann, warum und wie man damit umgeht 65

- 2.1 IKS im IT-Umfeld aus der Sicht der Wirtschaftsprüfung 66
 - 2.1.1 Herausforderung durch die Informationstechnologie 67
 - 2.1.2 Systemprüfung als Prüfungsansatz im IT-Umfeld 67
 - 2.1.3 Ansätze bei der Systemprüfung: IKS im Fokus 69
 - 2.1.4 IKS und die Systemprüfung als Pflicht 71
- 2.2 IKS-Assurance in der Praxis 75
 - 2.2.1 Ausrichtungen der Prüfer 75
 - 2.2.2 Ausgewählte Prüfungsgrundsätze 77
 - 2.2.3 Arten der externen Prüfung im ERP-Umfeld 80
 - 2.2.4 Empfehlungen zum Umgang mit dem Prüfer 83
- 2.3 Resümee 86

3 IKS-Anforderungen und ERP-Systeme: Grundsätze, Frameworks, Struktur 87

- 3.1 IKS-Inhalte im SAP ERP-Umfeld definieren 87
 - 3.1.1 IKS-Grundsätze im ERP-Umfeld: Von GoB zu GoBS 88
 - 3.1.2 Wer definiert die Spielregeln im SAP-Umfeld? 90
 - 3.1.3 Kontroll-Identifizierungsprozess 91
 - 3.1.4 Struktur eines klassischen IKS-Frameworks im ERP-Umfeld 94
 - 3.1.5 Struktur der effizienz- und wirtschaftlichkeitsorientierten Kontrollen im ERP-Umfeld 100
- 3.2 IKS-relevante Referenzmodelle und Standards 103
 - 3.2.1 COSO 104
 - 3.2.2 CobiT 104
 - 3.2.3 ITIL 106
 - 3.2.4 GAIT 107

3.2.5	ITAF	107
3.2.6	Risk IT	108
3.2.7	Val IT	109
3.2.8	CMMI	111
3.2.9	MOF	112
3.2.10	ISO 27k	112
3.2.11	PCI-DSS	113
3.2.12	Zusammenfassende Sicht auf Referenzmodelle	114
3.3	Resümees	115

4 Wie geht SAP mit dem Thema Compliance um? 117

4.1	Softwarezertifizierung	117
4.1.1	SAP-Hinweis 671016	118
4.1.2	Zertifizierungsberichte	119
4.2	Compliancerelevante Leitfäden	122
4.2.1	SAP-Online-Ressourcen	122
4.2.2	Sicherheitsleitfäden	125
4.2.3	DSAG-Leitfäden: Prüfleitfäden, Datenschutzleitfäden	131
4.3	Integrierter Ansatz in den SAP-Lösungen für GRC 10.0 und weitere compliancerelevante Lösungen	132
4.3.1	SAP-Lösungen für Governance, Risk, and Compliance 10.0	133
4.3.2	SAP Process Control 10.0	134
4.3.3	SAP Access Control 10.0	137
4.3.4	Richtlinienverwaltung	145
4.3.5	SAP Risk Management 10.0	145
4.3.6	Zusammenfassende Übersicht über Integrierungsszenarien in den SAP-Lösungen für GRC 10.0	148
4.3.7	SAP Audit Management	149
4.3.8	SAP Audit-Informationssystem	150
4.3.9	SAP Security Optimization Service	152
4.3.10	RSECNOTE-Tool	152
4.4	Compliancerelevanter Content	153
4.4.1	Direkter IKS-Content: Welche Kontrollen gibt es in SAP?	153

4.4.2	Content mit IKS-Relevanz: Standard- geschäftsprozesse und -werteflüsse in SAP	161
4.5	Resümee	165

**Teil II Vom Konzept zum Inhalt:
Kontrollen in SAP ERP**

5 Revisionsrelevante SAP-Basics 169

5.1	Am Anfang war die Tabelle: SAP als tabellengesteuerte Applikation	170
5.1.1	Daten im SAP-System	172
5.1.2	Kontrollen im SAP-System	178
5.1.3	Tabellenbezogene Suche	180
5.1.4	Transaktionsbezogene Suche	187
5.1.5	Programmbezogene Suche	189
5.1.6	Beziehung zwischen Programmen und Transaktionen	190
5.1.7	Beziehung zwischen Programmen und Tabellen	192
5.1.8	Zusammenfassung der Suchmöglichkeiten in SAP	195
5.1.9	Organisationsstrukturen im SAP-System	196
5.2	Berechtigungen	198
5.2.1	Ablauf und Hierarchie der Berechtigungskontrollen	198
5.2.2	Berechtigungsobjekte	199
5.2.3	Ermittlung der Berechtigungsobjekte	203
5.2.4	Rollen im SAP-System	207
5.2.5	Benutzer im SAP-System	208
5.2.6	Benutzertypen in SAP	209
5.2.7	Beispiel für eine Berechtigungs- auswertung	211
5.3	Resümee	213

6 Generelle IT-Kontrollen in SAP ERP 215

6.1	Organisatorische Kontrollen	215
6.1.1	IT-Organisation	216

6.1.2	IT-Outsourcing: Wer ist verantwortlich für die Kontrollen?	217
6.1.3	Richtlinien und Dokumentation	220
6.2	Kontrollen im Bereich Change Management und Entwicklung	222
6.2.1	SAP-Systemlandschaft	222
6.2.2	Korrektur und Transportwesen	224
6.2.3	Mandantensteuerung	228
6.2.4	Wartung und Updates	230
6.2.5	SAP Solution Manager	233
6.3	Sicherheitskontrollen beim Zugriff auf das SAP-System und bei der Authentifizierung	235
6.3.1	Identität und Lebenszyklus der Benutzer	235
6.3.2	Passwortschutz	237
6.3.3	Behandlung der Standardbenutzer	240
6.3.4	Notfallbenutzer-Konzept	242
6.4	Sicherheits- und Berechtigungskontrollen innerhalb von SAP ERP	243
6.4.1	Schutz der Programme und Transaktionen – Grundlagen	244
6.4.2	Schutz der Programme und Transaktionen bei weitreichenden Entwicklungen	248
6.4.3	Schutz der Tabellen	255
6.4.4	Kontrollen bei der Steuerung der Berechtigungsprüfungen	256
6.4.5	Kritische Administrationstransaktionen	258
6.4.6	Berücksichtigung der Funktionstrennungsgrundsätze	260
6.5	Resümee	262

7 Übergreifende Applikationskontrollen in SAP ERP 263

7.1	Grundsatz der Unveränderlichkeit	264
7.1.1	Schutz der Daten in Tabellen	264
7.1.2	Debugging	265
7.1.3	Änderbarkeit der Belege	267
7.2	Kontrollen für die datenbezogene Nachvollziehbarkeit	269
7.2.1	Änderungsbelege in SAP	269

7.2.2	Tabellenprotokollierung	271
7.2.3	Belegnummernvergabe	274
7.3	Nachvollziehbarkeit der Benutzeraktivitäten in SAP	276
7.3.1	System-Log	277
7.3.2	Security Audit Log	279
7.3.3	Historie der Transaktionsaufrufe	280
7.3.4	Nachvollziehbarkeit der Systemänderungen im Korrektur- und Transportwesen	281
7.4	Prozessübergreifende Verarbeitungskontrollen	284
7.4.1	Überwachung der Verbuchungsabbrüche	284
7.4.2	Vollständigkeit der ALE- Schnittstellenverarbeitung	287
7.4.3	RFC-Verbindungen (Remote Function Call)	290
7.4.4	Vollständigkeit der Batch-Input- Verarbeitung	292
7.5	Resümee	294

8 Kontrollen in der Finanzbuchhaltung 295

8.1	Grundlegende Kontrollmechanismen im Hauptbuch	296
8.1.1	Grundsatz: Zeitnähe der Buchungen	296
8.1.2	Bilanz	299
8.1.3	Sachkontenstammdaten	301
8.1.4	Konsistenzcheck der Verkehrszahlen mit der großen Umsatzprobe	302
8.1.5	Ausgewählte Kontrollen bei Abschlussarbeiten	303
8.1.6	Abstimmarbeiten im Hauptbuch	304
8.2	Kontrollen zur Richtigkeit und Qualität der Daten im Hauptbuch	306
8.2.1	Richtigkeit der Kontenfindung	307
8.2.2	Feldstatusgruppen	308
8.2.3	Berechnung von Steuern bei manuellen Buchungen	309
8.2.4	Validierungen in SAP	311
8.2.5	Fremdwährungen	312
8.3	Vollständigkeit der Verarbeitung im Hauptbuch	315
8.3.1	Belegvorerfassung	315

8.3.2	Dauerbuchungen	317
8.3.3	Abstimm-Ledger	319
8.4	Sicherheit und Schutz der Daten im Hauptbuch	321
8.4.1	Schutz der Buchungskreise	321
8.4.2	Toleranzgruppen	323
8.4.3	Schutz der Stammdaten	325
8.4.4	Kritische Transaktionen	329
8.4.5	Funktionstrennung im Hauptbuch	329
8.5	Kontrollen in der Anlagenbuchhaltung	331
8.5.1	Grundlagen der Anlagenbuchhaltung in SAP	331
8.5.2	Default-Werte bei Anlagenklassen	333
8.5.3	Kontenfindung in der Anlagen- buchhaltung	334
8.5.4	Konsistenzprüfung der Kontenfindung und der Konfiguration	336
8.5.5	Abschreibungen	337
8.5.6	Anlagengitter	339
8.5.7	Geringwertige Wirtschaftsgüter	341
8.5.8	Berechtigungssteuerung in der Anlagenbuchhaltung	342
8.5.9	Kritische Berechtigungen in der Anlagenbuchhaltung	344
8.6	Kontrollen in der Kreditoren- und Debitorenbuchhaltung	345
8.6.1	Richtigkeit der Abstimmkonten	345
8.6.2	Zahlungsfunktionen	347
8.6.3	Einmalkunden und -lieferanten – Vorsicht!	350
8.6.4	Altersstruktur und Wertberichtigungen	352
8.6.5	Vier-Augen-Prinzip bei der Stammdatenpflege	353
8.7	Resümee	354

9 Kontrollmechanismen im SAP ERP-gestützten Procure-to-Pay-Prozess 355

9.1	Bestellwesen	357
9.1.1	Berechtigungskonsistente Pflege der Organisationsstrukturen	357

9.1.2	Vier-Augen-Prinzip im Bestellwesen	358
9.2	Wareneingänge und Rechnungsprüfung	361
9.2.1	Wareneingänge: Kritische Bewegungsarten	361
9.2.2	3-Way-Match und Zahlungssperren bei der Logistik-Rechnungsprüfung	363
9.2.3	Prüfung auf doppelte Rechnungserfassung	366
9.3	WE/RE-Konto	366
9.3.1	Auszifferung des WE/RE-Kontos	367
9.3.2	Abschlussarbeiten und Ausweis des WE/RE-Kontos in der Bilanz	369
9.4	Kontrollen rund um das Thema Bestände	371
9.4.1	Pflege von Materialstammdaten	371
9.4.2	Unbewertetes Vorratsvermögen und getrennte Bewertung	373
9.4.3	Kontenfindung bei Materialbewegungen	375
9.4.4	Berichtigung des Vorratsvermögens: Inventur und Materialabwertungen	376
9.4.5	Freigabe von Verschrottungen	379
9.4.6	Produktkostenrechnung	380
9.4.7	Ausgänge von unbewertetem Bestand	383
9.5	Corporate Governance	383
9.6	Resümee	384

10 Kontrollmechanismen im SAP ERP-gestützten Order-to-Cash-Prozess 385

10.1	Kontrollen in der vorbereitenden Vertriebsphase	386
10.1.1	Kontrollen bei der Auftragserfassung	386
10.1.2	Qualität der Kundenstammdaten	388
10.1.3	Funktionstrennung bei der Stammdatenpflege	390
10.1.4	Kreditlimitvergabe und -kontrolle	391
10.2	Kontrollen bei der Auftragserfüllung und Umsatzlegung	393
10.2.1	Kontrollen rund um die Warenauslieferung	393
10.2.2	Preisfindung und Umsatzsteuer- ermittlung	395

10.2.3	Rücklieferungen und Gutschriften	398
10.2.4	Fakturavorrat	400
10.2.5	Vollständigkeit der buchhalterischen Erfassung von Fakturen	401
10.2.6	Mahnwesen	402
10.3	Resümee	406

11 Datenschutz-Compliance in SAP ERP Human Capital Management 407

11.1	Gesetzliche Datenschutzanforderungen	408
11.1.1	Datenschutz	408
11.1.2	Grundlagen: Richtlinie der Europäischen Union	410
11.1.3	Mitbestimmung und Arbeitnehmer- datenschutz	419
11.2	Datenschutzrelevante übergreifende Kontrollmechanismen in SAP	422
11.2.1	Änderungen von personenbezogenen Daten nachvollziehen	423
11.2.2	Protokollierung der Reportaufrufe in SAP ERP HCM	425
11.2.3	Daten löschen und unkenntlich machen	425
11.2.4	Personenbezogene Daten außerhalb von SAP ERP HCM	426
11.3	Besondere Anforderungen an SAP ERP HCM	427
11.4	Berechtigungen und Rollen in SAP ERP HCM	429
11.4.1	Differenzierende Attribute in SAP ERP HCM	430
11.4.2	Personalmaßnahmen	432
11.4.3	Strukturelle Berechtigungen	435
11.4.4	Berechtigungshauptschalter	440
11.5	Resümee	442

12 Betrug im SAP-System 443

12.1	Einführung	443
12.1.1	Betrugsarten	444
12.1.2	Betrug und das SAP-System	446

12.2	Betrugsszenarien in der SAP-Basis	448
12.2.1	Write-Debugging-Berechtigungen	448
12.2.2	Abspielen einer Batch-Input-Mappe unter einem anderen Benutzernamen	449
12.3	Betrugsszenarien im Hauptbuch	450
12.3.1	Betrügerische manuelle Belegbuchungen im Hauptbuch	451
12.3.2	Identifizierung und Analyse von manuellen Journaleinträgen	452
12.4	Betrugsszenarien im Vertriebsbereich	454
12.4.1	Fiktive Rechnungen an fiktive Kunden stellen	454
12.4.2	Gewährung nicht ordnungsgemäßer Gutschriften oder Boni	456
12.4.3	Übermäßiger Einsatz von Gratiswaren	457
12.4.4	Nicht ordnungsgemäße Ausbuchung offener Kundenforderungen	459
12.5	Betrugszenarien in der Personalbuchhaltung	459
12.5.1	Fiktive Angestellte	460
12.5.2	Limitierter Zugang zu eigenen HR-Daten	461
12.5.3	Vier-Augen-Prinzip bei vertraulichen Daten	462
12.6	Resümee	463

13 Exkurs: FDA-Compliance und Kontrollen in SAP ... 465

13.1	Gesetzliche Anforderungen im Bereich Arznei- und Lebensmittelherstellung	465
13.1.1	FDA-relevante gesetzliche Anforderungen im internationalen Vergleich	466
13.1.2	GxP – die FDA-Grundsätze	467
13.1.3	IT aus der Sicht von FDA-Compliance	469
13.2	Validierung der IT-Systeme	470
13.2.1	Vorgehensweise bei der Validierung	470
13.2.2	Kontrollen in Implementierungs- prozessen	472
13.3	FDA-Compliance in IT-gestützten Geschäftsprozessen	473
13.3.1	Beispiele: Kontrollen in der Beschaffung	474

13.3.2	Beispiele: Kontrollen im Produktionsmanagement	474
13.3.3	Beispiele: Kontrollen im Qualitätsmanagement	475
13.3.4	Beispiele: Kontrollen in der Instandhaltung	476
13.3.5	Beispiele: Kontrollen zur Chargenrückverfolgbarkeit	476
13.3.6	Beispiele: Kontrollen in Lagerverwaltungsprozessen	477
13.4	FDA-Compliance bei Systempflege, -aktualisierung und -änderung aufrechterhalten	479
13.5	Resümee	480

14 Exemplarische effizienz- und wirtschaftlichkeitsorientierte Analyseszenarien in SAP ERP 481

14.1	Prozessbezogene Datenauswertungen	482
14.1.1	Vergleich von Einkaufsbestelldatum mit dem Wareneingangsdatum	483
14.1.2	Fristgerechte Freigabe bzw. Anlage von Bedarfsanforderungen und Bestellungen	488
14.1.3	Zeitspanne zwischen Bestelleingang und Bestätigung des Kundenauftrags	497
14.1.4	Zehn weitere Beispiele möglicher datenbasierter Prozessanalysen	499
14.2	Analyse der Stammdatenqualität	499
14.2.1	Qualität der Kundenstammdaten	500
14.2.2	Produzierte Materialien ohne Stückliste	502
14.2.3	Abstimmung von Materialkosten innerhalb eines Buchungskreises	504
14.2.4	Zehn weitere Beispiele möglicher Stammdatenanalysen	506
14.3	Manuelle Datenänderungen	507
14.3.1	Veränderungen von Bedarfsanforderungen	508
14.3.2	Veränderungen von Einkaufsbelegen	510
14.3.3	Veränderungen von Verkaufsbelegen	515
14.3.4	Zehn weitere Beispiele für manuelle Datenänderungen	517

14.4	Ergänzung von SAP ERP-Standardreports	518
14.4.1	Bestandsanalysen um Planungsparameter erweitert	518
14.4.2	Kreditmanagementanalyse um Kundenstammdaten erweitert	520
14.5	Resümee	521

**Teil III Von Konzept und Inhalt zur Umsetzung:
Die Automatisierung eines Internen Kontrollsystems**

**15 IKS-Automatisierung: Wie bringt man den
COSO-Cube ins Rollen? 525**

15.1	Grundidee der IKS-Automatisierung	525
15.1.1	COSO-Cube in Aktion	526
15.1.2	Idee der IKS-Automatisierung	527
15.2	IKS-relevante Objekte und Dokumentation	530
15.2.1	Organisationseinheiten	530
15.2.2	Prozesse	532
15.2.3	Kontrollen	532
15.2.4	Kontrollziele	534
15.2.5	Risiken	535
15.2.6	Kontengruppen	536
15.2.7	Beispiel eines IKS-Datenmodells	537
15.3	Grundszenarien der IKS-Aktivitäten	538
15.3.1	Dokumentation	539
15.3.2	Selektion und Priorisierung von Kontrollaktivitäten	540
15.3.3	Kontrolldurchführung	541
15.3.4	Designtest	542
15.3.5	Effektivitätstest	542
15.3.6	Umfrage	543
15.3.7	Risikobewertung	544
15.3.8	Behebung	545
15.3.9	Sign-off	545
15.3.10	Reportauswertung	545
15.3.11	Personen als Bindeglied zwischen IKS-Objekten und Aktionen	546
15.4	Resümee	547

16 IKS-Automatisierung mithilfe von SAP Process Control	549
16.1 Einleitung: IKS-Umsetzung mit SAP Process Control	550
16.2 Technischer Implementierungsteil	552
16.2.1 Technische Architektur und Installation	553
16.2.2 Initiale Konfiguration der Standardfunktionen	555
16.2.3 Informationsquellen zu Implementierung, Betrieb und Upgrade von SAP Process Control	557
16.3 Datenmodell	559
16.3.1 IKS-Stammdaten in SAP Process Control	559
16.3.2 IKS-Datenmodell in SAP Process Control ...	563
16.3.3 Zentrale vs. lokale IKS-Stammdaten	565
16.3.4 Zeitabhängigkeit der IKS-Stammdaten	566
16.3.5 Nachvollziehbarkeit der Änderungen	568
16.3.6 Konzept der objektbezogenen Sicherheit ...	569
16.3.7 Kundeneigene Felder	570
16.3.8 Multiple-Compliance-Framework-Konzept	572
16.4 Implementierung des IKS-Prozesses	574
16.4.1 IKS-Dokumentationsprozess	575
16.4.2 Scoping-Prozess	582
16.4.3 Planungsprozess, Tests und Bewertungen	586
16.4.4 Problembehebungsprozess	595
16.4.5 Reporting	606
16.5 IKS- und Compliance-Umsetzung: Rollen	609
16.5.1 Berechtigungsmodell in SAP Process Control	610
16.5.2 Objektbezogene Sicherheit in Aktion	612
16.5.3 First-Level- vs. Second-Level-Berechtigungen	613
16.5.4 Vordefiniertes Best-Practice-Rollenkonzept in SAP	614
16.5.5 Anpassung der Rollen	615

16.6	SAP Process Control als GRC-Bestandteil – Neuheiten und Entwicklungen	617
16.6.1	Policy Management und sonstige Neuheiten in Release 10.0	617
16.6.2	Integration mit SAP Access Control	618
16.6.3	Integration mit SAP Risk Management	620
16.7	Resümee	625

17 Umsetzung von automatisierten Test- und Monitoring-Szenarien im SAP ERP-Umfeld 627

17.1	Automatisierte Test- und Überwachungsszenarien im SAP-Umfeld	628
17.1.1	Offline-CAAT-Tools	628
17.1.2	Online-CAAT-Berichte und -Auswertungen	634
17.1.3	Compliance-Management-Software	635
17.2	Automatisierte Tests und Monitoring in den SAP-Lösungen für GRC-Release 10.0 – Einführung	637
17.2.1	Continuous Monitoring Framework	637
17.2.2	Continuous Monitoring Framework – Potenzial und Erwartungshaltung	639
17.3	Einrichtung von CMF-Szenarien in SAP Process Control	643
17.3.1	SAP-Lösungen für GRC mit Geschäfts- anwendungen verbinden	643
17.3.2	Datenquellen in SAP Process Control	647
17.3.3	Geschäftsregeln im CMF anlegen	653
17.3.4	Überwachung der Datenänderungen im CMF	656
17.3.5	Automatisierung mithilfe vordefinierter Best-Practice-Szenarien	659
17.3.6	Verbindung von Kontrollen mit Regeln	661
17.3.7	Und los geht's!	663
17.4	Potenzial von CMF-Szenarien in SAP Process Control	664
17.4.1	Verwendung von SAP NetWeaver Business Warehouse für das Continuous Monitoring	665

17.4.2 Überlegungen zum Thema SAP BusinessObjects	666
17.5 Resümee	669

18 Praxis- und Projekterfahrungen 671

18.1 Praxiserfahrungen: Projekte zur IKS- und Compliance-Automatisierung	671
18.1.1 Hilfsmittel bei der Implementierung	671
18.1.2 Best-Practice-Projektaufbau bei der IKS-Umsetzung	673
18.1.3 Business Blueprint	674
18.1.4 IKS-Content	677
18.1.5 Einflussfaktoren auf den Projektaufwand	679
18.1.6 Erfolgsfaktoren	682
18.2 Projektbeispiele zur IKS- und Compliance- Automatisierung	684
18.2.1 Abdeckung der Schweizer Compliance- Anforderungen bei KUONI	685
18.2.2 Integrierter GRC-Ansatz bei Tecan	689
18.3 SOX bei Ericsson	694
18.3.1 IKS-Framework bei Ericsson	695
18.3.2 SOX-Compliance-Prozess bei Ericsson	699
18.3.3 Erfahrungen aus vorhergehenden Projekten	702
18.3.4 Optimierungspotenzial	703
18.3.5 Schritte zur Optimierung	704
18.4 Rückblick auf die IKS-Evolutionsstufen und Fazit	707

Anhang 711

A Abkürzungsverzeichnis	713
B Literatur	717
C Der Autor	721
D Die Beiträge	723
Index	727

Vorwort

In den vergangenen Jahren haben Bilanzskandale, Betrugs- und Korruptionsfälle, Verletzungen des Datenschutzes und andere Rechtsverstöße zu zahlreichen Haftungsfällen, Schadensersatzforderungen und Reputationsverlusten geführt. Als Reaktion auf diese Entwicklungen wurden zahlreiche Vorschriften erlassen: Corporate Governance, Sarbanes-Oxley Act, IFRS, Basel II und III, Solvency II, BilMoG, um nur einige zu nennen. Die dahinter stehenden Anforderungen sind komplex und betreffen längst nicht mehr nur die international ausgerichteten, börsennotierten Unternehmen. Das Thema Compliance hat in den Managementtagen und bei den überwachenden Organen (wie Aufsichtsrat, interne Revision, Wirtschaftsprüfung) Einzug gehalten.

Unter *Compliance* wird allgemein die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes innerhalb eines Unternehmens verstanden. Für den Aufbau eines Compliance-Management-Systems stehen allgemein anerkannte Rahmenkonzepte zur Verfügung (zum Beispiel COSO, OECD-Grundsätze der Corporate Governance) sowie Rahmenkonzepte, die die Spezifika einzelner Branchen oder compliancerelevanter Bereiche in den Vordergrund rücken (zum Beispiel FDA-Compliance). Auch das Institut der Wirtschaftsprüfer hat in Deutschland mit dem Prüfungsstandard *Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen* bereits reagiert.

Der erste Schritt ist vielfach getan: Unternehmen haben auf die Flut nationaler und internationaler Compliance-Gesetze und -Richtlinien reagiert und Maßnahmen ergriffen, um Compliance sicherzustellen. Nun gilt es, die einzelnen Aktivitäten, wie beispielsweise das Interne Kontrollsystem, das Risikomanagementsystem, das Vertragsmanagement, die interne Revision etc., in ein Compliance-Management-System zu integrieren und – so weit möglich – zu automatisieren, um ein Gleichgewicht zwischen Compliance und Performance zu erreichen. Die Einhaltung von Compliance allein stellt einen zusätzlichen Kostenfaktor im Unternehmen dar; erst durch die Balance zwischen Compliance und Performance werden die Chancen aus der Umsetzung der regulatorischen Anforderungen genutzt. Im Rahmen der Einhaltung der regulatorischen Anforderungen können und sollten

daher auch die Verbesserungen der Prozesse, verbunden mit Effizienzgewinnen, realisiert werden. Eine Verbesserung und eine Standardisierung der Prozesse unter Berücksichtigung regulatorischer Anforderungen erfordern in der Regel die Einbeziehung der IT-Systeme; die SAP-Lösungen für GRC stellen hier eine Option dar.

Die derzeit verfügbare Literatur beschränkt sich in der Regel auf die Abbildung von Kontrollen in SAP ERP und die Prüfung von SAP-Systemen. Auch das vorliegende Buch bietet hier Hilfestellung, geht jedoch weit über diese Inhalte hinaus. Ausgehend von den Anforderungen an die Compliance (Teil I) werden nicht nur compliancerelevante Fragestellungen in Form eines Kontrollleitfadens für ein SAP ERP-System (Teil II) angesprochen und beantwortet, sondern es wird auch aufgezeigt, wie ein (automatisiertes) Compliance-Management-System in einem SAP ERP-System abgebildet werden kann (Teil III). Damit greift dieses Buch den aktuellen Bedarf an Lösungsansätzen zur Implementierung von Compliance-Management-Systemen in den Unternehmen auf. Darüber hinaus zeigt das Buch auch, welche Risiken und Kontrollen die interne Revision sowie die externe Wirtschaftsprüfung bei der Prüfung eines in SAP abgebildeten Internen Kontrollsystems sowie eines Compliance-Management-Systems im Blick haben sollten.

Die Einführung eines Compliance-Management-Systems in SAP ERP erfordert sowohl Kenntnisse der zugrunde liegenden Gesetze und Rechtsnormen als auch der technischen Möglichkeiten der Umsetzung. Bei der Arbeit an diesem Buch hat Maxim Chuprunov seine umfangreichen Erfahrungen aus beiden Gebieten eingebracht. Diese Erfahrungen resultieren aus seiner bisherigen beruflichen Laufbahn, während der er sich einerseits mit der Prüfung von IT-Systemen im Allgemeinen und von SAP-Systemen im Speziellen und andererseits mit der Implementierung von SAP ERP-Systemen und den SAP-Lösungen für GRC befasst hat.

Ich bin davon überzeugt, dass es gerade diese Kombination von theoretischem und praktischem Wissen ist, die den besonderen Nutzen dieses Buches ausmacht. Sowohl Entscheider und Umsetzer von Compliance und Compliance-Management-Systemen im Unternehmen als auch interne Revision und Wirtschaftsprüfer als überwachende Organe werden in ihrem jeweiligen Tätigkeitsfeld von diesem Buch profitieren.

Annett Nowatzki

Vorstand der DSJ Revision und Treuhand AG, Berlin

Vertrauen ist gut, Kontrolle ist billiger: Einleitung

Die Notwendigkeit, Risiken zu beherrschen und ein Internes Kontrollsystem (IKS) zu etablieren, steht ganz oben auf der Agenda des Topmanagements in Unternehmen und beschert Wirtschaftsprüfungs- und Beratungsgesellschaften seit Jahren ein gutes Geschäft.

Kann die Umsetzung der gesetzlichen Anforderungen einen tieferen Sinn und Nutzen haben, der über das simple »den-Paragrafen-Genüge-tun« hinausgeht? Sicherlich ja – wenn man es richtig macht. Die Praxis zeigt Folgendes:

Warum
Compliance?

- ▶ Oft wird übersehen, dass das Thema IKS aufgrund seiner traditionellen Orientierung auf Compliance auch die Überwachung der Geschäftsprozesse hinsichtlich Effizienz, Wirtschaftlichkeit und Performance umfassen kann. Es geht daher nicht nur um Paragrafen.
- ▶ Selbst wenn es nur um Compliance im Sinn der Gesetzeskonformität geht, ist diese generell (kosten-)günstiger, weil Nicht-Compliance teuer zu stehen kommen kann (wie zum Beispiel der durch die Presse gut bekannte Schmiergeldskandal bei SIEMENS im Jahr 2006 zeigt).
- ▶ Compliance als Spielregeln, die vom Staat in Ausübung seiner regulierenden Rolle aufgestellt wurden, schützt die Allgemeinheit vor vielen Übeln. Vielleicht erinnern Sie sich noch an die spektakulären Pleiten von ENRON, FLOWTEX etc.? Ihre Ursachen lagen unter anderem in der Manipulation der externen Finanzberichterstattung.
- ▶ Diverse Compliance-Initiativen fordern, die komplexen Prozesse in einem Unternehmen (oft erstmals) sauber aufzunehmen. Transparentere Abläufe sind besser steuerbar, und die identifizierten Kontrollen kommen auch dem operativen Bereich zugute.
- ▶ Ein ineffizienter Compliance-Management-Prozess bindet viele Ressourcen. Die Automatisierung dieses Prozesses kann die Unternehmensleitung spürbar entlasten.

- ▶ Und nicht zuletzt: Compliance kann direkte finanzielle Vorteile bringen, wie etwa eine geringere Kapitalbindung infolge einer genaueren bzw. risikospezifischen Eigenkapitalhinterlegung oder günstigere Kredite aufgrund einer besseren Bewertung durch Ratingagenturen.

Warum ist Compliance eine Herausforderung?

Es gibt demnach zahlreiche Gründe, Compliance-Anforderungen nicht ausschließlich als notwendiges Übel zu betrachten. Ihre effiziente Umsetzung und der Aufbau eines wirksamen IKS waren und bleiben jedoch nicht einfach:

- ▶ Das komplexe ERP-Umfeld erfordert ein spezifisches Know-how, und bei IT-gestützten Geschäftsprozessen weiß man nicht immer, welche Risiken sich darin verbergen und welche Kontrollmechanismen es gibt.
- ▶ Die Missachtung von Compliance-Anforderungen während der Implementierung eines SAP-Systems kann gravierende Folgen haben. Im Nachhinein ist man immer schlauer – im Fall nicht berücksichtigter Compliance-Anforderungen bei der SAP-Implementierung aber meist auch ärmer. Die SAP-Einführung ist ein kostspieliges Unterfangen und ein nachträgliches Redesign ist aufwendig und teuer.
- ▶ Kontrollen müssen gelebt werden: Nicht die Kontrollen sind wirksam, die richtig dokumentiert und geprüft werden, sondern vielmehr die, die ausgeführt werden. Ohne Prüfung ist Compliance allerdings undenkbar, dabei sorgt die in der Praxis oft noch fehlende Automatisierung für viel administrativen Aufwand. Microsoft Excel-Sheets, E-Mails und manuelle Systemauswertungen dominieren oft die IKS- und Revisionswelt, eine zeitnahe Berichterstattung ist häufig nicht möglich.
- ▶ Die Automatisierung eines IKS könnte Antworten auf viele der Fragen geben, die heutzutage die Welt der Compliance beschäftigen:
 - ▶ Wie bringt man operative und revisionsspezifische Sichten auf Kontrollmechanismen zusammen?
 - ▶ Ist ein Realtime-Reporting über den Stand der Compliance auf Knopfdruck möglich?
 - ▶ Wie kann man das IKS so abbilden, dass unterschiedliche Anforderungen von Risk Management, interner Revision, exter-

ner Jahresabschlussprüfung und branchenspezifische Kontrollanforderungen effizient erfüllt werden?

Um ein IKS richtig zu implementieren, müssen viele Puzzleteile zusammengefügt werden:

Wie macht man es richtig?

- ▶ unternehmensinterne IKS- und Compliance-Ziele bezüglich Effizienz, Wirtschaftlichkeit und Performance
- ▶ gesetzliche Anforderungen und deren Auswirkung auf die heutige Welt der ERP-gestützten Prozesse
- ▶ »Übersetzung« der Compliance-Anforderungen in die Sprache eines jeweiligen ERP-Systems – zum Beispiel SAP ERP
- ▶ Konzipierung und Aufbau eines IKS-Modells im IT-Umfeld
- ▶ Automatisierung eines IKS-Compliance-Prozesses
- ▶ Automatisierung der Test- und Überwachungsszenarien durch Integration
- ▶ Umgang mit der internen und externen Revision

Das hochaktuelle und spannende Gesamtbild bzw. die Vision der automatisierten IKS- und Compliance-Prozesse im SAP ERP-Umfeld eines gut geführten Unternehmens, zu dem sich die einzelnen Puzzleteile zusammenfügen lassen, hat mich dazu bewegt, dieses Buch zu schreiben.

Thema, Aufbau und Inhalt des Buches

Die große Welle von gesetzlich getriebenen IKS-Projekten wurde durch den Sarbanes-Oxley Act Anfang des letzten Jahrzehnts ausgelöst. Diese Welle hat auch in Europa alle in den USA börsennotierten Unternehmen erfasst. Nach und nach griffen die Anforderungen, Risiken etc. durch das IKS transparent zu halten und zu minimieren, durch EU-Richtlinien und weitere lokale gesetzliche Initiativen auch auf weitere Unternehmen in Europa über. Der weltweite Trend, ob man die bevorstehende Einführung von China-SOX oder Entwicklungen in anderen Emerging Markets berücksichtigt oder nicht, zeigt insgesamt, dass sich ein funktionierendes IKS als eine staatlich geforderte Compliance-Anforderung rasch durchsetzt.

Immer mehr Anforderungen

Das Thema Governance, Risk, and Compliance als einheitliches Konzept (man spricht von einem integrierten GRC-Ansatz) ist auf dem

Compliance als Teil von GRC

Markt vor nicht allzu langer Zeit angekommen, und das Zusammenführen von GRC mit den Themen Strategie und Performance ist ein ganz neuer Trend, der sich sowohl in den einschlägigen Softwarelösungen als auch in anerkannten Referenzmodellen widerspiegelt. Das Thema Compliance kann somit nicht mehr isoliert betrachtet werden.

IKS im IT-Umfeld In diesem Buch wird Compliance als der im Rahmen eines IKS abgebildete Prozess verstanden, der Konformität mit den gesetzlichen Anforderungen und mit den unternehmenseigenen Richtlinien und Zielen (vor allem Effizienz und Wirtschaftlichkeit) gewährleisten soll. Ein IKS war schon vor dem Computerzeitalter bekannt, aber erst mit dem Voranschreiten der Informationstechnologie haben sich neue Besonderheiten ergeben: Die Systemprüfung als Prüfungsansatz und insbesondere die Betrachtung von IKS und der softwarespezifischen Applikationskontrollen im Rahmen der externen Revision haben sich als Pflicht durchgesetzt. Die Antwort auf die Frage, was all das für Unternehmen bedeutet, deren Prozesse SAP ERP-gestützt ablaufen, muss klar strukturiert und beschrieben werden.

Compliance auf Knopfdruck In den letzten Jahren waren auf dem Markt immer mehr Softwareprodukte zu finden, die es erlauben, den IKS-Prozess – gegebenenfalls im Zusammenspiel mit dem Risikomanagement – effizient zu gestalten. Doch das Grundverständnis der Abläufe in einem IT-gestützten Compliance-Management-Prozess wird leider nicht mit der Software mitgeliefert.

Konzept dieses Buches Wie Sie gesehen haben, gibt es zahlreiche Puzzleteile rund um die hochaktuellen Themen IKS und Compliance, die es zusammenzufügen gilt, um einen guten Überblick zu haben. Dieses Buch berücksichtigt die Verbindung von Compliance mit den weiteren Bestandteilen von GRC – Corporate Governance und Risk Management –, soweit die Integrationsicht es erfordert, um die möglichen Synergien aufzuzeigen und den integrierten GRC-Ansatz zu erklären. Im Fokus dieses Buches steht jedoch die IKS-Compliance selbst. Dabei wird dieses Thema aus der Perspektive eines von SAP ERP dominierten IT-Umfelds betrachtet und konzeptionell in drei Schritten aufgearbeitet:

1. Vom Paragraphen zum Konzept
2. Vom Konzept zum Inhalt
3. Von Konzept und Inhalt zur Automatisierung

Idee und Aufbau dieses Buches zeigt Abbildung 1 noch einmal im Zusammenhang.

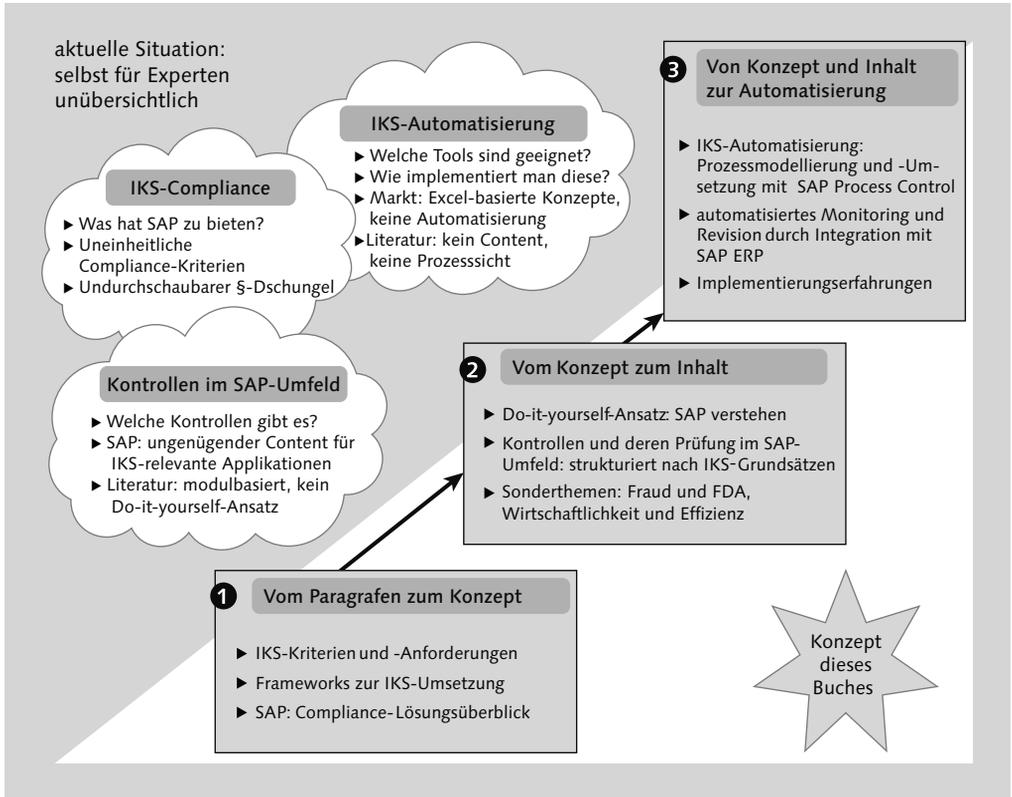


Abbildung 1 Konzept dieses Buches

Bei der vorliegenden zweiten Auflage des Buches wurden zwei wesentliche Anpassungen vorgenommen:

- ▶ Die IKS-Fokussierung auf Wirtschaftlichkeit und Effizienz wurde stärker hervorgehoben: Es wurden sowohl eine theoretische Grundlage in Form der Strukturierung eines IKS-Frameworks geschaffen als auch Praxisbeispiele aus dem SAP ERP-Umfeld ergänzt.
- ▶ Der integrierte GRC-Ansatz (basierend auf den neuen SAP-Lösungen für GRC) wurde näher erläutert. Im Zuge dessen wurden auch die Inhalte der Kapitel 16 und 17, die die Implementierung von SAP Process Control beschreiben, überarbeitet, um Spezifika des neuen Releases 10.0 wiederzugeben.

TEIL I – Vom Paragrafen zum Konzept: Kontrollen im SAP ERP

IKS-Compliance im SAP ERP-Umfeld – selbst für einen Experten stellen sich bei diesem Stichwort viele Fragen: Welche Sicht auf Compliance ist gemeint? Welche gesetzlichen, aber auch unternehmensinternen Anforderungen stehen im Mittelpunkt? Wie sieht ein integrierter GRC-Ansatz basierend auf SAP-Software aus? Die Antworten auf diese grundlegenden Fragen gibt der erste Teil des Buches.

- ▶ In **Kapitel 1, »Gesetzliche Anforderungen im Bereich IKS-Compliance«**, erfahren Sie, was man unter einem IKS versteht und wie relevante gesetzliche Compliance-Anforderungen im internationalen und branchenübergreifenden Vergleich aussehen.
- ▶ **Kapitel 2, »Der Prüfer kommt: Wann, warum und wie man damit umgeht«**, erklärt die besonderen Rahmenbedingungen, denen die Revision im IT-Umfeld ausgesetzt ist, und fasst die wichtigsten Sachverhalte und Empfehlungen aus der Prüfungspraxis zusammen.
- ▶ In **Kapitel 3, »IKS-Anforderungen und ERP-Systeme: Grundsätze, Frameworks, Struktur«**, zeigen wir Ihnen, nach welchen Grundsätzen und wie der Inhalt eines IKS im SAP ERP-Umfeld definiert wird und welche international anerkannten Studien und Referenzmodelle Ihnen dabei behilflich sein können. Die Wichtigkeit des Continuous-Monitoring-Ansatzes wird dabei besonders hervorgehoben. Neu in dieser Auflage ist die Beschreibung, wie ein effizienz- und wirtschaftlichkeitsorientiertes IKS-Framework aufgebaut ist.
- ▶ **Kapitel 4, »Wie geht SAP mit dem Thema Compliance um?«**, fasst die wichtigsten Sachverhalte zusammen, damit Sie Ihre compliancerelevanten Prozesse effizienter gestalten können. Diese Sachverhalte reichen von der Zertifizierung der SAP-Softwarelösungen bis hin zu Dokumentationsquellen für Kontrollmechanismen in SAP und einer Aufstellung der Softwareprodukte. Zudem wird hier der integrierte GRC-Ansatz beschrieben, der auf den Komponenten der SAP-Lösungen für GRC Release 10.0 basiert.

TEIL II – Vom Konzept zum Inhalt: Kontrollen in SAP ERP

Wie werden die IKS-Compliance-Anforderungen in die SAP-Sprache übersetzt? Welche Risiken und Kontrollen gibt es dazu in SAP ERP-gestützten Prozessen? Und wie kann die Effizienz der SAP ERP-gestützten Prozessabläufe implementiert und überwacht werden? Die Antworten auf diese Fragen finden Sie im zweiten Teil des Buches.

- ▶ In **Kapitel 5, »Revisionsrelevante SAP-Basics«**, erläutern wir Ihnen die grundlegenden Zusammenhänge im SAP-System und vermitteln Ihnen das Handwerkszeug für eine eigenständige Suche nach kontroll- und revisionsrelevanten Informationen in SAP ERP.
- ▶ **Kapitel 6, »Generelle IT-Kontrollen in SAP ERP«**, behandelt sowohl allgemeine organisatorische Kontrollen als auch Themen rund um das Change Management, kritische Berechtigungen und die grundlegende Systemsicherheit.
- ▶ In **Kapitel 7, »Übergreifende Applikationskontrollen in SAP ERP«**, erfahren Sie, wie die generelle Einhaltung der Grundsätze der Nachvollziehbarkeit und Vollständigkeit bei der Verarbeitung in SAP ERP sichergestellt werden kann.
- ▶ Die Überschriften von **Kapitel 8, »Kontrollen in der Finanzbuchhaltung«**, **Kapitel 9, »Kontrollmechanismen im SAP ERP-gestützten Procure-to-Pay-Prozess«**, und **Kapitel 10, »Kontrollmechanismen im SAP ERP-gestützten Order-to-Cash-Prozess«**, sprechen für sich: In diesen SAP-gestützten Prozessen existieren Risiken, die die Einhaltung der Compliance unmittelbar gefährden. Die zugehörigen Kontrollmechanismen sind überlebenswichtig und werden in den genannten Kapiteln beschrieben.
- ▶ In **Kapitel 11, »Datenschutz-Compliance in SAP ERP Human Capital Management«**, lernen Sie, welche gesetzlichen Anforderungen den Umgang mit personenbezogenen Daten regeln und wie diese Anforderungen in SAP ERP umgesetzt werden.
- ▶ **Kapitel 12, »Betrug im SAP-System«**, ist dem Thema Fraud/Betrug gewidmet. Dort, wo die materiellen Werte und unmittelbar das Geld SAP-gestützt gehandhabt werden, ist immer die Gefahr doloser Handlungen gegeben. In diesem Kapitel zeigen wir Ihnen anhand von Beispielen, wie Sie mit dieser Gefahr umgehen können.

- ▶ **Kapitel 13, »Exkurs: FDA-Compliance und Kontrollen in SAP«,** betrifft direkt oder indirekt jeden Leser dieses Buches: Die vom Gesetz geforderten Kontrollmechanismen in der Pharma- und Nahrungsmittelindustrie, die primär auf die Qualität der hergestellten Produkte fokussiert sind, müssen in den SAP-Prozessen abgebildet sein. Auf die wichtigsten dieser Kontrollen wird hier eingegangen.
- ▶ **Kapitel 14, »Exemplarische effizienz- und wirtschaftlichkeitsorientierte Analyseszenarien in SAP ERP«,** gibt detaillierte Beispiele für jedes der vier Elemente eines effizienzorientierten IKS-Frameworks: prozessorientierte Analysen, Qualität von Stammdaten, manuelle Datenänderungen und Benutzereingaben sowie Erweiterung der Berichte. Der hohe Detaillierungsgrad der Darstellung dient dem Zweck, eine Do-it-yourself-Anleitung für die Einrichtung diverser Auswertungsszenarien zur Verfügung zu stellen und somit auch einen Eindruck davon zu vermitteln, welche Arbeit hinter der Implementierung von Continuous-Monitoring-Szenarien steckt.

TEIL III – Von Konzept und Inhalt zur Umsetzung: Automatisierung eines Internen Kontrollsystems

Compliance auf Knopfdruck ist ein realistisches Szenario. Auf dem Markt gibt es inzwischen Softwareprodukte, die helfen, ein IKS zu automatisieren. Was allerdings auf dem Markt noch recht spärlich vertreten ist, ist das Angebot der IKS-Prozesse sowie des IKS-Contents und deren softwarebasierter Umsetzung aus einer Hand. Einerseits werden IKS-Inhalte und »-Konzepte« von den Big-Four-Prüfungsgesellschaften sowie von diversen Compliance-Beratungshäusern meist Microsoft Excel-basiert angeboten; andererseits fehlt sowohl der existierenden Literatur über IKS- und GRC-Software als auch den Beratern aus den Softwarehäusern der konzeptuelle Compliance-Blick. Das Ziel dieses Teils ist es, sowohl eine konzeptionelle als auch eine technische Anleitung zur Implementierung von IKS- und Compliance-Management-Prozessen zu geben (basierend auf den SAP-Lösungen für GRC Release 10.0).

- ▶ In **Kapitel 15, »IKS-Automatisierung: Wie bringt man den COSO-Cube ins Rollen?«,** gehen wir auf die konzeptionelle Bedeutung der IKS-Automatisierung ein und erläutern die einzelnen

Bausteine, die bei der Modellierung der Automatisierung von IKS-Prozessen verwendet werden können. Dies geschieht in Form einer IKS-Umsetzungsmatrix.

- ▶ **Kapitel 16, »IKS-Automatisierung mithilfe von SAP Process Control«**, zeigt Ihnen, wie der Compliance- und IKS-Management-Prozess mithilfe von SAP Process Control implementiert werden kann. Sie erfahren auch, warum und mithilfe welcher Integrationszenarien SAP Process Control als Bestandteil eines integrierten GRC- sowie eines Strategie- und Performance-Management-Konzepts angesehen werden kann.
- ▶ In **Kapitel 17, »Umsetzung von automatisierten Test- und Monitoring-Szenarien im SAP ERP-Umfeld«**, wird erläutert, welche Optionen – unter anderem die Integration von SAP Process Control mit Ihren SAP ERP-Systemen – die große Vision eines »Tests auf Knopfdruck« möglich machen. Sie werden Schritt für Schritt durch die Einrichtung des Continuous-Monitoring-Ansatzes in SAP Process Control 10.0 geleitet.
- ▶ In **Kapitel 18, »Praxis- und Projekterfahrung«**, sind zahlreiche Projekterfahrungen dargestellt, die aufzeigen, wie Unternehmen aus unterschiedlichen Branchen ihre Compliance-Prozesse automatisiert haben. Dabei werden die wichtigsten Sachverhalte bezüglich der Projektgestaltung im Rahmen der Implementierung von SAP Process Control zusammengefasst und einige Beispiele für Implementierungsprojekte bei konkreten SAP-Kunden gegeben.

An wen richtet sich dieses Buch?

Welche Vorkenntnisse sollten Sie als Leser mitbringen? Während für Teil I des Buches nur gesunder Menschenverstand und etwas betriebswirtschaftliches Grundwissen benötigt werden, wäre insgesamt und insbesondere für die restlichen Teile dieses Buches SAP ERP-Erfahrung von Vorteil. Der Compliance- und IKS-Beratungshintergrund stellen ideale Voraussetzungen für dieses Buch dar.

An wen richtet sich dieses Buch?

- ▶ **IKS-Verantwortliche, Mitarbeiter interne Revision, externe Wirtschaftsprüfer, IT-Auditors, Compliance-Beauftragte**
Das ist Ihr Buch – vom ersten bis zum letzten Kapitel!

► **Leiter von SAP Competence Centern, Projektleiter, Data Governance Experts, Business-Analysten und Berater für die SAP ERP-Implementierungen**

Die Compliance-Anforderungen bei der Implementierung von SAP ERP zu berücksichtigen ist nicht einfach. Daher werden insbesondere Teil I und Teil II wichtige Hinweise für eine revisions- und IKS-konforme Gestaltung Ihrer Implementierungsprojekte und auch für den täglichen Betrieb der SAP ERP-Anwendungen geben.

► **SAP-Berater für die SAP-Lösungen für GRC**

Teil III sollte Ihre obligatorische Lektüre werden. In Ihren Implementierungsprojekten, bei denen die Prozesssicht auf das IKS im Fokus steht, sollten Sie den Bezug zum IKS-Inhalt niemals verlieren: Aus diesem Grund ist auch Teil II wichtig für Sie. Und nicht zuletzt: Das Verständnis der komplexen Zusammenhänge zwischen gesetzlichen Anforderungen und deren Umsetzung im IT-Umfeld muss ebenfalls zu Ihrem Rüstzeug gehören, um mit Kunden eine gemeinsame Compliance-Sprache zu finden. Aus diesem Grund wäre für Sie auch Teil I relevant.

► **MBA-, BWL- und Wirtschaftsinformatik-Studenten**

Für Sie sind vor allem Teil I und Teil II dieses Buches interessant: In Teil I gehe ich recht detailliert auf die gesetzlichen Anforderungen im internationalen Vergleich sowie auf die betriebswirtschaftliche Konzeption des IKS im IT-Umfeld ein. Die Übersicht über international anerkannte GRC-Referenzmodelle könnte für Sie ebenfalls interessant sein. Teil III können Sie entnehmen, was die Automatisierung von IKS konzeptionell bedeutet.

► **Senior Management**

Ob Sie ein CFO, CEO oder CIO in einem Unternehmen sind oder Ihren Pflichten in Vorstand oder Prüfungsausschuss nachgehen – die Compliance-Fragestellungen haben Sie sicherlich nicht umgangen. Selbst wenn Prozesse in Ihrem Unternehmen nicht SAP-gestützt ablaufen und eine richtige Definition des SAP-spezifischen Inhalts Ihres IKS für Sie irrelevant ist, haben Sie sich sicherlich Gedanken über dessen effiziente Gestaltung gemacht: Erfahrungen anderer Unternehmen im Umgang mit den IKS- und Compliance-Themen in Teil III werden gute Anhaltspunkte für Sie liefern. Darüber hinaus werden die gesetzlichen und sonstigen Compliance-Anforderungen, Empfehlungen zum Umgang mit der

externen Prüfung und die Übersicht der GRC-Rahmenkonzepte aus Teil I dieses Buches für Sie interessant sein. Die visionären und konzeptionellen Ausführungen zum Thema »Compliance auf Knopfdruck« in Teil III sollten Sie sich ebenfalls nicht entgehen lassen.

Hinweise zur Lektüre

In diesem Buch finden Sie mehrere Orientierungshilfen, die Ihnen die Arbeit erleichtern sollen.

In grauen Informationskästen sind Inhalte zu finden, die wissenschaftlich und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie die Informationen in den Kästen sofort einordnen können, haben wir die Kästen mit Symbolen gekennzeichnet:

Infokästen

► Die mit diesem Symbol gekennzeichneten *Tipps* und *Hinweise* geben Ihnen spezielle Empfehlungen, die Ihnen die Arbeit erleichtern können. Sie finden in diesen Kästen auch Informationen zu weiterführenden Themen oder wichtigen Inhalten, die Sie sich merken sollten.

[+]

► Das Symbol *Achtung* macht Sie auf Themen oder Bereiche aufmerksam, bei denen Sie besonders achtsam sein sollten.

[!]

► *Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen.

[zB]

Marginalien (Stichwörter am Seitenrand) ermöglichen es Ihnen, das Buch nach bestimmten, für Sie interessanten Themen zu durchsuchen oder Stellen wiederzufinden, die Sie bereits gelesen haben. Die Marginalien stehen neben dem jeweiligen Absatz, der die entsprechenden Informationen enthält.

Marginalien

Die Prüfungshandlungen, die in die Darstellung eingebunden sind, werden zum Beispiel über das ganze Buch hinweg durch die Marginalie »Prüfung:« kenntlich gemacht (jeweils ergänzt durch ein inhaltliches Stichwort).

Danksagung

Nun gilt es, mich bei all den Menschen zu bedanken, ohne deren Unterstützung ich dieses Buchprojekt nicht hätte bewältigen können.

Während der Zeit, in der ich neben meiner Hauptaufgabe als Geschäftsführer und Berater bei Riscomp GmbH und parallel zu vielen spannenden Projekten dieses Buch verfasst habe, mussten mich meine Freunde und Verwandten oft entbehren. Als Erstes möchte ich mich bei ihnen für ihr Verständnis und ihre Unterstützung bedanken.

Viele Menschen haben mir Anregungen, Ideen und Informationen zu vereinzelt gestellten Fragen gegeben: Großer Dank gebührt den SAP-Experten Herrn Jürgen Möller, Herrn Dominik Yow-Sin-Cheung, Herrn Daniel Welzbacher, Frau Jan Gardiner, Herrn David Ramsay und Herrn Atul Sudhalkar – für die Unterstützung bei »kniffligen« Fragen rund um die SAP-Lösungen für GRC. Ein herzlicher Dank geht an Herrn Dr. Karol Bliznak (SAP AG) für den Input bezüglich der Abbildung des »Risk-Intelligent-Strategic-Execution«-Ansatzes mit SAP-Produkten. Ebenso bedanke ich mich bei Herrn Jürg Kasper (Kanton Zürich) für seinen kreativen Input bezüglich der Automatisierung der Test- und Monitoring-Szenarien.

Hoch geschätzte Kollegen haben selbst Beiträge zu diesem Buch verfasst: Herr Gerhard Wasnick hat mir durch die hoch kompetente und in der Praxis mehrfach bewiesene Beschreibung der Kontrollmechanismen in den SAP ERP-gestützten Procure-to-Pay- und Order-to-Cash-Prozessen viel Arbeit abgenommen. Herr Günther Emmenegger (SAP Schweiz AG) hat das Kapitel zur Abbildung der FDA-Anforderungen im SAP-Umfeld geschrieben. Herr Volker Lehnert hat den größten Teil des Kapitels über datenschutzrelevante Kontrollen in SAP ERP HCM verfasst. Herr Marc Michely (PricewaterhouseCoopers) hat den Beitrag über Fraud-Szenarien in SAP beigesteuert. In enger Zusammenarbeit mit Herrn Jan Laurisjen (Ericsson) und Herrn Michele Poffo (Tecan) sind die Praxisberichte über die Abbildung von Compliance-Anforderungen entstanden. Herr Reto Bachmann hat Input für den Beitrag über effizienzorientierte Szenarien geliefert.

Für vielfältige Unterstützung, Hinweise und Hilfe danke ich Herrn Dr. Michael Adam (SAP AG), Herrn Dr. Gero Mäder, Herrn Thomas Schmale (SAP AG), Frau Evelyn Salie (SAP Schweiz AG), Herrn Arnold Babel (SAP Schweiz AG), Herrn Peter Heidkamp (KPMG),

Herrn Florian Köller (SAP AG), Herrn Walter Harrer (SAP Schweiz AG) und Herrn Christian Brunner (SAP Schweiz AG).

Vier oder sechs Augen sehen mehr als zwei: Frau Annett Nowatzki (DSJ Revision und Treuhand AG) sowie Frau Patricia Sprenger von Galileo Press haben erste Entwürfe, Vor- und Rohfassungen sowie den fertigen Text gelesen und durch ihre Anmerkungen verbessert. Herzlichen Dank für Ihre kompetenten Hinweise und Ihre Unterstützung!

Trotz der vielfachen Unterstützung, die mir zuteilwurde, bin ich allein für die verbliebenen Fehler verantwortlich.

Ich hoffe, dass Ihnen dieses Buch dabei hilft, Ihre Aufgaben rund um Compliance, Revision und IKS-Automatisierung mit SAP zu lösen, und wünsche Ihnen viel Erfolg und auch Freude bei der Lektüre.

Maxim Chuprunov

1. Werten Sie den Saldo des WE/RE-Kontos zum Ende eines Monats aus. Ist dieser ungleich null, klären Sie, ob die Rechnungsprüfung wareneingangsbezogen stattfindet. Falls nicht, klären Sie, wie der Saldo des WE/RE-Kontos im Rahmen der Abschlussarbeiten gehandhabt wird.
2. Prüfen Sie mittels Transaktion FBKP, ob für die Vorgänge BNG und GNB in der Kontenfindung die richtigen Sachkonten zugeordnet sind.

9.4 Kontrollen rund um das Thema Bestände

Von der Stammdatenpflege bis hin zur Bewertung – Bestände als Umlaufvermögen auf der Aktivseite der Bilanz stehen im Mittelpunkt der IKS-relevanten Themen im P2P-Prozess.

9.4.1 Pflege von Materialstammdaten

Wichtige Kontrollen im Stammdatenbereich mit P2P-Relevanz wurden unter anderem bereits in Abschnitt 8.6.1, »Richtigkeit der Abstimmkonten«, erläutert. Bleibt nun noch das Thema Materialstamm: Dessen Pflege hat Einfluss auf eine Vielzahl wichtiger Unternehmensprozesse. Außer dem P2P-Prozess ist auch der *Verkaufsprozess* (Order to Cash, O2C) betroffen. Aus Sicht des Internen Kontrollsystems (IKS) sind darüber hinaus auch die Bewertung des Umlaufvermögens und die Berechnung sowie der Ausweis der Vorsteuer (MwSt.) relevant. Aus diesem Grund sollte die Pflege von Materialstammdaten in einen IKS-konformen Änderungsprozess eingebunden sein.

In einigen Unternehmen wird eine Kombination von Berechtigungen in Verbindung mit der SAP Business Workflow-Funktion eingesetzt. Dabei stellt die Einschränkung von Berechtigungen für Buchungskreise, Werke, Materialstammsichten und Pflegestatus sicher, dass die Materialien nur von den autorisierten Benutzern gepflegt werden können. Die Workflow-Funktionalität informiert die autorisierten Benutzer, welche Materialstämme zur Pflege bereitstehen.

Die Initiierung des Workflows erfolgt durch sogenannte *Ereignisse*. Das Ereignis ist in dem Fall die Erstellung eines neuen Materialstammsatzes, das heißt die Pflege der Grunddaten 1 und 2. In der

Wichtige Rolle der Materialstammdaten

Kontrollen rund um den Materialstamm

SAP Business Workflow

Folge wird ein Änderungsauftrag (Change Order) erzeugt, ein Beispiel sehen Sie in Abbildung 9.8.

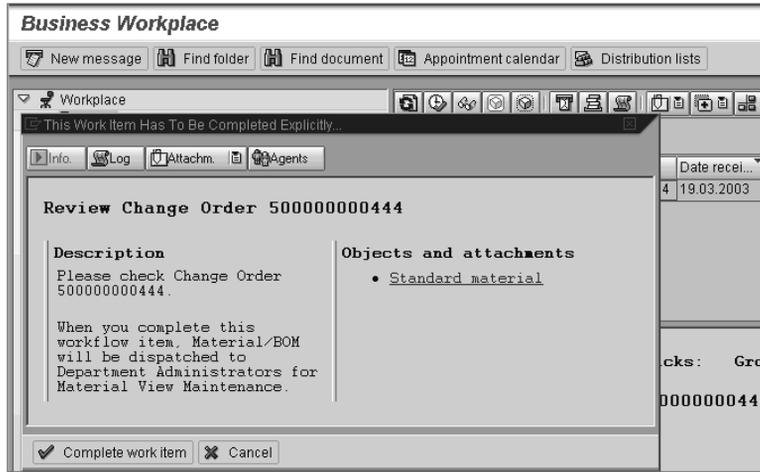


Abbildung 9.8 Änderungsauftrag für den Materialstamm

Dieser Änderungsauftrag wird an einen lokalen Materialstammverwalter geschickt. Nach der Freigabe wird der Antrag an alle lokalen Organisationseinheiten zur Pflege der relevanten Materialstamm-sichten weitergeleitet (siehe 1 in Abbildung 9.9).

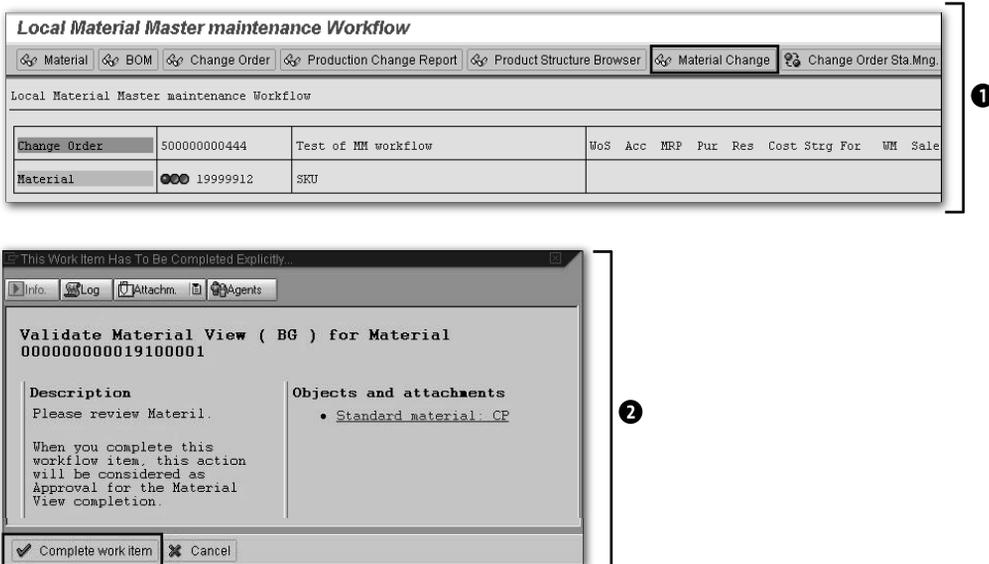


Abbildung 9.9 Workflowbasierte Bearbeitung von Materialstammdaten

Der Materialstammverwalter hat dabei jederzeit die Möglichkeit, den Fortschritt der Materialstammpflege zu verfolgen. Pro Sicht im Materialstamm erfolgt abschließend eine Freigabe, um eine angemessene Funktionstrennung sicherzustellen. Der Materialstamm kann über den Button MATERIAL CHANGE angezeigt werden. Die Materialstammänderung wird durch die Bestätigung der Workflow-Aufgabe COMPLETE WORK ITEM abgeschlossen ②.

Standard-SAP-Workflows werden über den Menüpfad SAP MENÜ • TOOLS • BUSINESS WORKFLOW • ADMINISTRATION konfiguriert.

Folgende Auswertungen sind im Zusammenhang mit der Behandlung der Materialstammdaten zu empfehlen:

Prüfung: Pflege
Materialstammdaten

1. Verschaffen Sie sich einen Überblick über die Prozesse und Verfahrensanweisungen zur Materialstammpflege in Logistik, Einkauf und Vertrieb.
2. Prüfen Sie, wie die Materialstammpflege im Berechtigungskonzept abgebildet ist. Wichtig für eine angemessene Funktionstrennung sind unter anderem folgende Berechtigungsobjekte:
 - ▶ M_MATE_STA für die Änderung des Pflegestatus
 - ▶ M_MATE_WRK für die Einschränkung auf Werksebene
 - ▶ M_MATE_MAR für die Materialart
 - ▶ M_MATE_VKO für die Pflege innerhalb definierter Verkaufsorganisationen

9.4.2 Unbewertetes Vorratsvermögen und getrennte Bewertung

Die Bestandsverwaltung in SAP erlaubt für das Vorratsvermögen mehrere Möglichkeiten einer gesonderten Bewertung. Das Vorratsvermögen besteht aus Roh-, Hilfs- und Betriebsstoffen, unfertigen und fertigen Erzeugnissen oder Leistungen. Materialien in SAP können trotz gleicher Materialnummer einen unterschiedlichen buchhalterischen Wert besitzen. So wird zum Beispiel Material mit abgelaufenem Mindesthaltbarkeitsdatum meist *unbewertet* geführt. In den folgenden Fällen wird das Material zwischen bewertetem und unbewertetem Bestand umklassifiziert:

Bewerteter vs.
unbewerteter
Bestand

- ▶ Wareneingänge erfolgen erst in der Qualitätssicherung, und erst nach Freigabe der Qualitätssicherung erfolgt eine Freigabe in den unbeschränkten Lagerbestand.

- ▶ (Un-)fertige Erzeugnisse überschreiten ihr Haltbarkeitsdatum, oder Materialien werden als unbewerteter Projektbestand geführt.
- ▶ Materialien werden durch Umlagerung oder Umbuchung zwischen bewertetem und unbewertetem Bestand verschoben.

Bei der Klassifizierung des Vorratsvermögens besteht das Risiko eines fehlerhaften Ausweises in der Bilanz, das heißt der Über- oder Unterbewertung.

Konfiguration zur Umklassifizierung des Bestandes

Die SAP-Funktionalität *Chargenverwaltung* kann bei aktivierter Prüfung des Mindesthaltbarkeitsdatums (MDH) im Bestand eine Veränderung des Status FREI auf NICHT FREI einschließlich der Erstellung eines Materialbelegs automatisch bewirken. Mithilfe der Kontenfindung kann die relevante Bewegungsart so eingestellt werden, dass der gesamte Buchwert der Charge in den Aufwand gebucht wird. Die Aktivierung der Prüfung des Mindesthaltbarkeitsdatums (MDH) erfolgt mit der Transaktion OMJE (Tabelle T159L sowie pro Bewegungsart in der Tabelle T156). Zusätzlich ist die Bewegungsart 341 (unfertige Leistungen, frei an nicht frei in der Kontenfindung, Tabelle T156 ff.) zu pflegen.

Handhabung der getrennten Bewertung

Neben der Chargenverwaltung können Materialien bei manuellen Materialbewegungen auch unterschiedlich bewertet werden. Dies ist für Unternehmen relevant, die Rohmaterialien, unfertige Erzeugnisse oder Fertigerzeugnisse sowohl fremd beziehen als auch selbst fertigen und lagern. Da Anschaffungs- und Herstellkosten der Materialien in diesem Fall unterschiedlich sind, müssen die Bestände *getrennt bewertet* werden.

Das Risiko bei der getrennten Bewertung ist vergleichbar mit dem Bewertungsrisiko bei unbewertetem Bestand.

Konfiguration der getrennten Bewertung

Die Einstellung der getrennten Bewertung erfolgt im Customizing unter MATERIALWIRTSCHAFT • BEWERTUNG UND KONTIERUNG • GETRENNTE BEWERTUNG • GETRENNTE BEWERTUNG AKTIVIEREN/EINSTELLEN oder mithilfe der Transaktion OMWO/OMWC. Mithilfe dieser Konfigurationseinstellungen werden beispielsweise Bewertungstypen konfiguriert (ob ein Eigen- oder Fremdbezug vorliegt etc.).

Prüfung: Bewertung des Vorratsvermögens

Folgende Prüfungshandlungen sind im Zusammenhang mit der Materialbewertung zu empfehlen:

1. Verschaffen Sie sich einen Überblick, ob die getrennte Bewertung und die Chargenverwaltung aktiviert sind.

2. Die Aktivierung der Prüfung auf das Mindesthaltbarkeitsdatum im Rahmen der Chargenverwaltung kann in den Tabellen T159L und T156 überprüft werden.
3. Prüfen Sie die Einstellungen zur getrennten Bewertung von Vorratsvermögen im Customizing mit den Transaktionen OMWO (MM-IV Steuerung Bewertung) und OMWC (MM-IV Getrennte Materialbewertung).

9.4.3 Kontenfindung bei Materialbewegungen

Die logistischen Prozesse in der Lagerverwaltung (Warehouse Management) sind den Hauptprozessen Einkauf, Produktion und Verkauf untergeordnet. Die notwendigen Materialbewegungen müssen einerseits die Mengen in den Lagerorten und andererseits die entsprechenden Werte in der Buchhaltung aktualisieren. Dies erfolgt im SAP-System mithilfe der *Bewegungsarten*. Jede Materialbewegung besitzt eine Bewegungsart im Materialbeleg.

Material-
bewegungen
in SAP

Eine Bewegungsart steuert unter anderem, ob nur Mengen, nur Werte oder beides im System aktualisiert werden. So müssen bei einem Wareneingang zu einer Bestellung die Materialbestände in den Lagerorten erhöht und das Vorratsvermögen angepasst werden. Im Gegensatz dazu erfordert eine *Umbuchung* innerhalb eines Werks oder eines Bewertungskreises meist nur die Aktualisierung der Mengen, nicht aber der Buchwerte. Die Richtigkeit der Kontenfindung ist dabei essenziell, weil bei fehlerhaften Einstellungen die korrekte Anweisung der Bestandswerte in der Bilanz und GuV beeinträchtigt werden kann.

Bewegungsarten
und Konten-
findung

Die Richtigkeit der Kontenfindung sowie die systemtechnische Einschränkung, dass Sachkonten bei Bewegungen manuell nicht ausgewählt werden können, sind auch aus IKS-Gesichtspunkten sehr wichtig. Die Kontenfindung in der SAP-Materialwirtschaft besteht aus folgenden Elementen:

Konfiguration der
Kontenfindung

- ▶ Bewertungssteuerung
- ▶ Bewertungskreis
- ▶ Bewertungsklasse
- ▶ Kontomodifikation

Während in der Bewertungssteuerung und im Bewertungskreis festgelegt wird, welche Werke mit oder ohne Anpassung der Kontierung

(Kontomodifikation) angelegt werden, wird in der Bewertungsklasse festgelegt, welches Konto abschließend bebucht wird. Über die *Bewertungsklasse* ist eine materialabhängige automatische Kontenfindung möglich. Beispielsweise können so die Zugänge für Rohstoffe auf andere Bestandskonten gebucht werden als die Zugänge für Halbfabrikate, obwohl in beiden Fällen der gleiche Vorgang erfasst wird. Die *Kontenklassenreferenz* verknüpft Bewertungsklassen mit Materialarten und legt damit fest, welche Bewertungsklassen für ein Material zulässig sind, das selbst immer einer bestimmten Materialart zugeordnet ist.

Um Erfassungsfehler bei Materialbewegungen zu verhindern, sollte das Prüfkennzeichen in der Kontomodifikation (Tabelle: T156X bis XPKON) *nicht* gesetzt sein. Durch diese Einstellung wird verhindert, dass Sachkonten, die im Erfassungsbild eingegeben werden, für den Buchhaltungsbeleg verwendet werden.

Prüfung: Kontenfindung bei Materialbewegungen

Folgende Handlungen empfehlen wir im Zusammenhang mit der Kontenfindung bei Materialbewegungen sowie für die Abstimmung des Hauptbuchs mit den Werten in MM:

1. Verschaffen Sie sich einen Überblick über die Systemeinstellungen zur Kontenfindung, insbesondere der Kontomodifikation für Bewegungsarten, sowie über die Anbindung der Kontenpläne (Transaktion OMWD oder mithilfe der Fixkontentabelle T030).
2. Kontrollieren Sie in Stichproben die Kontierung der Bewegungsarten für wichtige Materialarten. Wählen Sie dazu die Transaktion OMWB (Simulation der Kontenfindung), und klicken Sie anschließend auf den Button SIMULATION ODER SACHKONTEN.
3. Hinweis: Das Programm RM07MMFI führt einen Saldenabgleich zwischen der SAP-Materialwirtschaft und -Finanzbuchhaltung durch. Zusätzlich gleicht das Programm RM07MBST summarisch den Lagerbestand mit dem Bestandskonto in der Finanzbuchhaltung ab. Eine Konsistenzprüfung der Bestände sollte regelmäßig mithilfe des Programms RM07K001 durchgeführt werden.

9.4.4 Berichtigung des Vorratsvermögens: Inventur und Materialabwertungen

Werte anpassen – wann und warum?

Im Rahmen der Monats-, Quartals- oder Jahresabschlussaktivitäten ist das Vorratsvermögen nach allen Rechnungslegungsvorschriften auf eventuellen Abwertungsbedarf hin zu prüfen. Die Bewertungs-

maßstäbe können sich von Land zu Land unterscheiden. So wird zum Beispiel nach IAS 2 eine Bewertung zu niedrigeren, historischen Kosten oder zum Nettoverkaufswert (zum Nettoverkaufspreis, zu den Nettovertriebskosten etc.) verlangt. Abweichungen von Mengen infolge der Inventurergebnisse oder die Notwendigkeit einer Wertberichtigung (Erfassung zusätzlicher Anschaffungs- oder Herstellkosten, AHK) stellen weitere mögliche Ursachen für Wertkorrekturen dar.

SAP unterstützt unterschiedliche Inventurverfahren. Dies ist beispielsweise die *permanente, stichtagsbezogene oder Stichtagsinventur*. Alle Verfahren verfolgen dabei nur das Ziel, Differenzen zwischen den Mengen im SAP-System und den tatsächlichen Mengen im Lager zu finden. Diese Inventurdifferenzen werden im System erfasst (Rückmeldung der Zählung) und anschließend ausgebucht.

Inventur

Um eine Abweichung durch Materialbewegungen während der Inventur zu verhindern, sollten während der Inventur die Bestände durch eine Sperre der Lagerorte fixiert werden. Diese Sperre kann im Customizing aktiviert werden (MATERIALWIRTSCHAFT • BESTANDSFÜHRUNG UND INVENTUR • INVENTUR • BUCHBESTAND FIXIEREN IM LAGERORT ERLAUBEN im Einführungsleitfaden).

Inventurkontrolle:
Sperre der
Lagerorte

Eine weitere wichtige Kontrolle im Rahmen der Inventur ist die Funktionstrennung zwischen der Zählung und der Erfassung der Zählergebnisse einerseits und der Berechtigung zum Ausbuchen der Inventurdifferenzen andererseits. Für die Erfassung der Zählung ist das Berechtigungsobjekt M_ISEG_WDB in der Aktivität 01 erforderlich. Die Berechtigung zum Ausbuchen der Inventurdifferenz wird durch das Berechtigungsobjekt M_ISEG_WDB vergeben. Im Customizing des Systems können auch Obergrenzen für die Pflege von Inventurdifferenzen festgelegt werden.

Inventurkontrolle:
Funktionstrennung

Um die Vollständigkeit der Inventur sicherzustellen, sollten die angelegten Inventuren nach Abschluss auch wieder geschlossen werden.

Anpassungen des Buchwertes können laufend auftreten, wenn zum Beispiel Transportrechnungen als zusätzliche Anschaffungs- und Herstellkosten (AHK) erfasst werden. Im Rahmen von eigengefertigten Materialien für Anlagen im Bau erfolgt die Erfassung der Kosten indirekt am Monatsende. Entsprechende Kontrollen über die Materialien, die mit dem *Standardpreis* bewertet werden, sowie die Umlage der

AHK-bezogene
Wertberichtigung

Herstellkosten sind in Abschnitt 9.4.6, »Produktkostenrechnung«, aufgeführt.

Abwertung des Vorratsvermögens

Für Handelsware oder fremdbezogene Materialien (diese werden meist mit *gleitendem Durchschnittspreis* bewertet) ist jedoch zu ermitteln, ob ein Abwertungsbedarf des Vorratsvermögens besteht. SAP bietet zu diesem Zweck mehrere Verfahren an, die im System eingestellt werden müssen. Neben der Preissteuerung (S/V) kann ein Niederstwerttest auch auf Basis des periodisch gleitenden Durchschnittspreises, des mittleren Zugangspreises, durch die Ermittlung niedrigster Marktpreise, von Verbrauchsfolgeverfahren (LIFO/FIFO), der Reichweite oder der Lagerreichweite durchgeführt werden.

Die Bewertung des Vorratsvermögens enthält einen signifikanten Spielraum bei dem Ausweis der Werte in der Bilanz. Deshalb empfehlen sich folgende Kontrollen:

► **Prüfungshandlungen zur Abwertung**

Wichtige Parameter zur Berechnung der Niederstwertermittlung müssen zum Zeitpunkt des Programmstarts im Customizing richtig gesetzt sein:

- Reichweitenabschläge bei der Niederstwertermittlung im Customizing (Transaktionen OMW5 und OMW5W)
- Selektion der Beleg- und Bewegungsarten, die bei der Niederstwertermittlung nach Marktpreisen für die Berechnung der Zugangspreise berücksichtigt werden (Transaktion OMWI für Bewegungsarten/Transaktion OMWJ für Belegarten)
- Abschlagswerte für die Niederstwertermittlung nach Gängigkeit (Transaktionen OMW5 und OMW5W)
- Bewertungsebene für LIFO/FIFO (Transaktion OMWL) sowie die Definition der LIFO/FIFO-relevanten Bewegungsarten

► **Kontrollen zur Funktionstrennung**

Zusätzlich sollte eine angemessene Funktionstrennung sichergestellt sein. SAP ermöglicht die Erstellung einer Batch-Input-Mappe sowie die direkte Aktualisierung der Bewertungspreise im Materialstamm. Eine angemessene Funktionstrennung kann auf zwei unterschiedliche Arten erreicht werden.

► *Präventive Kontrolle*

Die Wertberichtigung wird ausschließlich mithilfe der Batch-Input-Mappe durchgeführt. Der Benutzer, der die Bewertung

vorbereitet und durchführt, darf keine Berechtigungen zur Aktualisierung des Materialstamms besitzen. Außerdem sollte der Benutzer auch keine Berechtigungen für die Verarbeitung der Batch-Input-Mappen haben.

► *Detektive Kontrolle*

Die Änderungen der Preise im Materialstamm werden nach der Aktualisierung mithilfe der Transaktionen MRN9 (Anwendungs-Log) und CKMPCD (Anzeige der Preisänderungsbelege) ausgewertet.

Wichtig für die Transaktion CKMPCD

Wählen Sie die Option BELEGPOSITIONEN PRO MATERIAL aus, anderenfalls werden die Wertänderungen nicht ausgegeben.

【!】

Abschließend ist die Festlegung der Schritte der Niederstwertermittlung wichtig. Diese sind jedoch organisatorisch festzulegen, bevor die Transaktionen MRN0 (Marktpreise), MRN1 (Reichweite), MRN2 (Gängigkeit) und MRN3 (Verlustfreie Bewertung) etc. zur Niederstwertermittlung gestartet werden können.

Folgendes müssen Sie im Zusammenhang mit Wertberichtigungen in der Materialwirtschaft prüfen:

1. Verschaffen Sie sich einen Überblick über die verwendeten Inventurverfahren, und klären Sie, ob Lagerorte während der Inventur gesperrt werden. Werten Sie entsprechende Änderungsbelege aus. Prüfen Sie, ob Funktionstrennungsanforderungen über Berechtigungen umgesetzt sind.
2. Prüfen Sie unter Berücksichtigung der rechnungslegungsrelevanten Bewertungsmaßstäbe die Vorgehensweise für die Abwertungen, und analysieren Sie gegebenenfalls die relevanten Konfigurationseinstellungen. Prüfen Sie, ob Funktionstrennungsanforderungen berücksichtigt werden.

Prüfung:
Berichtigung des
Vorratsvermögens

9.4.5 Freigabe von Verschrottungen

Die meisten Unternehmen führen regelmäßige Kontrollen ihres Lagerbestandes durch. Bestände, die nicht mehr benötigt oder verkauft werden können, werden bei »Verschrottungsaktionen« als Warenausgang aus dem Bestand in den Aufwand der GuV ausgebucht. Zu diesem Zweck sind im SAP-Standard die Bewegungsarten

IKS-konform
Bestände
ausbuchen

551, 553 und 555 definiert. Werden die Verschrottungsaktionen nicht durchgeführt, besteht Korrekturbedarf bei der Menge des Vorratsvermögens.

Kontrolle: Kritische Bewegungsarten

Hinsichtlich der Verwendung kritischer Bewegungsarten sollte die Kontrolle in zwei Teilen erfolgen:

1. Die Vorabkontrolle besteht in der restriktiven Vergabe der Berechtigungen.
2. Da eine effektivere Kontrolle auf Prozessebene (vorgelagerte Freigabe von Verschrottungen) leider nicht vom SAP-Standard unterstützt wird, kann nachträglich manuell geprüft werden, ob die kritischen Bewegungsarten autorisiert genutzt wurden.

Prüfung:
Freigabe von Verschrottungen

Bezüglich der Behandlung der Verschrottungen prüfen Sie Folgendes:

1. Die Einschränkung der Bewegungsarten erfolgt mit den Berechtigungsobjekten M_MSEG_BWA, M_MSEG_BMB, M_MSEG_BWE, M_MSEG_BMF und M_MSEG_LGO. Prüfen Sie, ob die Bewegungsarten 551, 553 und 555 restriktiv gehandhabt werden.
2. Materialbewegungen mit bestimmten Bewegungsarten können mithilfe der Transaktion MB51 (Materialbelegliste) analysiert werden. Werten Sie die Materialbelege mit den Verschrottungsbewegungsarten 551, 553 und 555 aus, und vergleichen Sie das Ergebnis mit den freigegebenen Verschrottungsaktionen.

9.4.6 Produktkostenrechnung

Wertefluss für Eigenerzeugnisse in SAP

Die Bewertung des Vorratsvermögens innerhalb der Wertschöpfungskette von Unternehmen wird in vielen Fällen mit dem SAP-Modul Controlling (CO) und dessen Komponenten Produktkostencontrolling (CO-PC) und Profitability-Analysis (CO-PA) durchgeführt. Als Kostenträger bzw. Kostensammler fungieren unterschiedliche Typen von Aufträgen, zum Beispiel Innen- oder Fertigungsaufträge. Diese Kostensammler werden durch die einzelnen Transaktionen im Geschäftsprozess belastet, zum Beispiel durch Rohmaterialentnahme. Am Ende des Fertigungsprozesses werden diese Kostensammler dann durch die Rückmeldung (Fertigmeldung) des Materials entlastet und beispielsweise der Bestand bei Lagerfertigung bzw. der Kundenauftrag belastet.

- ▶ durch die Wiederverwendung der Test-, Umfrage- und Bewertungsergebnisse für Prozesse und Kontrollen, die eine domänenübergreifende Relevanz haben (zum Beispiel Testergebnisse für IT General Controls im Rahmen von SOX ❶ und BilMoG ❷)

Eigenschaften von Auflagen

Die einzelnen *Auflagen* können gleiche Stammdaten verwenden (Objekte), sich aber hinsichtlich der Funktionalität unterscheiden (zum Beispiel enthält die Auflage »FDA« einen spezifischen Prozess der Problembehandlung, in dem CAPA-Funktionalität (CAPA = Corrective And Preventive Actions) und die E-Signatur zum Einsatz kommen, siehe hierzu Abschnitt 16.4.4, »Problembehebungsprozess«).

Begriffe »Auflage« und »Compliance-Initiative«

Die Begriffe *Auflage* und *Compliance-Initiative* sind Synonyme. Während Compliance-Initiative meist in Zusammenhang mit dem älteren GRC-Release 3.0 verwendet wird, wird Auflage meist in Bezug zum GRC-Release 10.0 verwendet.

Technische Details und Konfiguration

Die funktionalen Unterschiede und die Prozessunterschiede lassen sich durch die Gestaltung von spezifischen *Aktionen* und *Rollen* implementieren. In der Standardauslieferung von SAP Process Control sind zwei Auflagen vorkonfiguriert: SOX und FDA.

Neue Auflage anlegen

Um eine neue Auflage anzulegen, müssen folgende Schritte unternommen werden:

1. SAP GUI: neue auflagenspezifische Rollen (via PFCG) anlegen
2. SAP GUI: neue Auflage anlegen und konfigurieren (im IMG)
3. SAP GUI: neue Rollen der neuen Auflage zuweisen (im IMG)
4. Frontend: neue Auflage innerhalb einer bestehenden oder neuen Auflagengruppe anlegen

16.4 Implementierung des IKS-Prozesses

Wie Sie bereits aus Abschnitt 4.3 wissen, kann ein IKS-Prozess vereinfacht als Abfolge der IKS-Aktivitäten dargestellt werden. In Abbildung 16.14 sehen Sie ein Beispiel für eine solche Abfolge.

Nachdem Sie in Abschnitt 15.3 die Grundszenarien der IKS-Aktivitäten kennengelernt haben, werden Sie in diesem Abschnitt erfahren, wie das IKS-Standardszenario in SAP Process Control aussieht, was

die Inhalte einzelner Prozessschritte sind und wie diese technisch umgesetzt und gegebenenfalls angepasst werden können. Dabei werden wir uns auf die wesentlichen Fragestellungen beschränken, die sich erfahrungsgemäß bei der Implementierung von SAP Process Control ergeben.

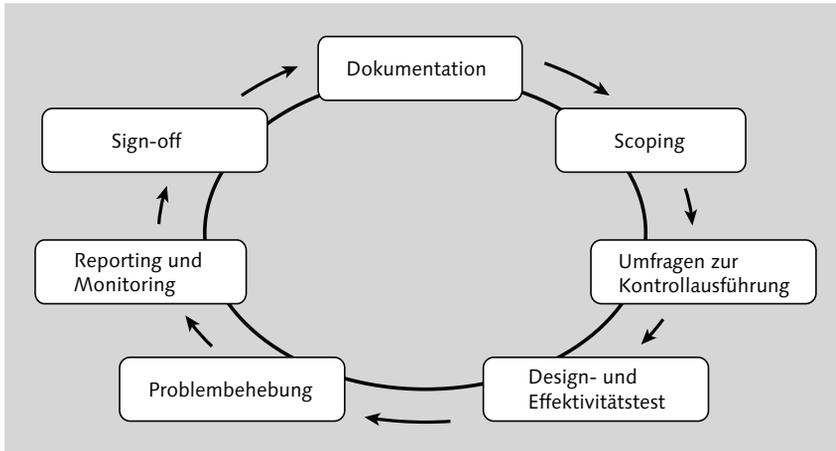


Abbildung 16.14 IKS-Zyklus – vereinfachte Darstellung

16.4.1 IKS-Dokumentationsprozess

Wie setzt man das IKS-Framework im System um? Diese Frage ist nicht nur während der Implementierungsphase relevant, während der die IKS-Stammdaten in SAP Process Control initial hochgeladen werden müssen, sondern auch während des Betriebs von SAP Process Control.

Betriebs-
wirtschaftliche
Sicht

Die Organisationsstrukturen, Geschäftsprozesse, Kontrollmechanismen und Zuständigkeiten befinden sich ständig im Wandel, und die IKS-Stammdaten müssen in regelmäßigen Abständen aktualisiert werden. Die Pflege in SAP Process Control ist intuitiv, dank der Weboberfläche. Eine wichtige Voraussetzung für die Pflege ist die Kenntnis des Datenmodells (siehe Abschnitt 16.3.2, »IKS-Datenmodell in SAP Process Control«).

In Abbildung 16.15 ist der Ablauf der Pflege der IKS-Stammdaten im zentralen Katalog (Schritte ❶ bis ❺, Arbeitsbereich STAMMDATEN in der deutschen Sprachversion) dargestellt.

Pflege im zentralen
Katalog

Schritt 4 ist optional und hängt von den IKS-Dokumentationsanforderungen im Unternehmen ab; zwingend sind dagegen die übrigen Pflegeschritte.

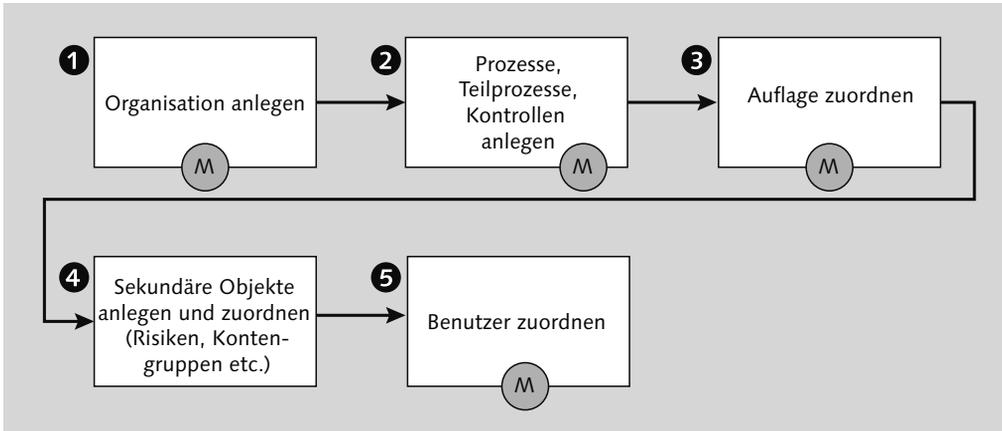


Abbildung 16.15 Ablauf der IKS-Stammdatenpflege

Der wesentliche Unterschied bei Release 10.0 im Vergleich zu Release 3.0 besteht darin, dass die manuelle Pflege der Stammdaten durch ein angepasstes Datenmodell wesentlich vereinfacht wurde. Während in Release 10.0 die einzelnen Auflagen als Werte innerhalb von einzelnen Objekten (Teilprozesse oder Kontrollen) gepflegt werden, stellten Auflagen (oder die in früheren Releases sogenannten *Compliance-Initiativen*) in Release 3.0 eigenständige Arbeitsbereiche dar. Das bedeutete beispielsweise, dass eine Kontrolle in unterschiedlichen Auflagen gegebenenfalls mehrfach bearbeitet werden musste.

Technische Details und Konfiguration

Für einen Massen-Upload der Stammdaten kann das MDUG-Tool (MDUG = Master Data Upload Generator) verwendet werden. Dieses Tool bietet SAP als Bestandteil der SAP-Lösungen für GRC 10.0 an. Die Benutzerdokumentation sowie Verweise auf weitere Informationsquellen sind in SAP-Hinweis 1563286 zu finden.

Vier-Augen-Prinzip bei der Pflege des IKS-Frameworks

Betriebswirtschaftliche Sicht

Bei der Pflege der IKS-Stammdaten ist es oft erforderlich, zum Beispiel aus Qualitäts- oder Zuständigkeitsgesichtspunkten, in die Änderungen eine weitere Person zu involvieren (wie beim Anlegen einer

neuen Kontrolle, der Zuordnung eines Risikos, der Änderung der Prozessbeschreibung etc.).

Vier-Augen-Prinzip bei der Kontrolldokumentation

[zB]

Im IKS-Alltag ist ein Szenario denkbar, bei dem ein Prozessverantwortlicher die Beschreibung des Designs einer Kontrolle ändern möchte. Ein IKS-Verantwortlicher muss diese Änderung genehmigen, zumindest sollte er über die Änderung in Kenntnis gesetzt werden.

Beide Optionen sind in SAP Process Control möglich, wie in Abbildung 16.16 dargestellt wird.

Beim ersten Szenario ❶ wird ein Genehmigungsprozess angestoßen, bevor eine Änderung an den Objekten erfolgen kann. Es kann aber auch die zweite Option zum Einsatz kommen ❷, bei der bei Änderungen an den Objekten eine Benachrichtigung an die zuständigen Personen gesendet wird.

Um die beschriebenen Optionen zu ermöglichen, müssen Workflows für Stammdatenänderungen aktiviert sein. Dies nehmen Sie im Einführungsleitfaden über den Pfad GRC • GEMEINSAME STAMMDATEN-EINSTELLUNGEN • WORKFLOW FÜR STAMMDATENÄNDERUNGEN AKTIVIEREN VOR.

Technische Details und Konfiguration

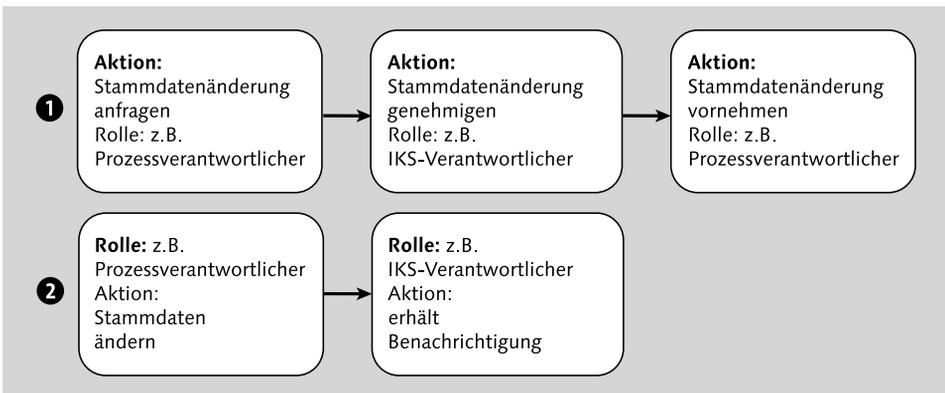


Abbildung 16.16 Zwei Optionen zur Abbildung des Vier-Augen-Prinzips

Zentralisierte vs. dezentralisierte Dokumentation des IKS

Man unterscheidet in der Praxis zwischen einem dezentralisierten und einem zentralisierten Ansatz im Rahmen der IKS-Dokumentation. Dabei ist nicht nur der Prozess an sich gemeint; im Rahmen des

Betriebswirtschaftliche Sicht

IKS-Prozessen können auch manche der IKS-Aktionen, wie zum Beispiel Scoping, Planung, unabhängige Effektivitätstests etc., zentral (auf der Corporate-Ebene) oder dezentral (in den einzelnen Einheiten) durchgeführt werden. Darüber hinaus ist die Verwaltung von IKS-Stammdaten relevant: wie die obligatorische Verwendung von einem vorgeschriebenen Mindestumfang an zentral dokumentierten Kontrollen.

[+] FEI-Survey-Ergebnisse

Laut einer Umfrage, die von Financial Executives International (FEI, www.fei.org) 2007 durchgeführt wurde, betragen die durchschnittlichen Compliance-Kosten bei einem dezentral organisierten IKS 1,9 Millionen €, während Unternehmen mit einem zentral organisierten IKS wesentlich weniger – 1,3 Millionen € im Schnitt – aufwenden mussten.

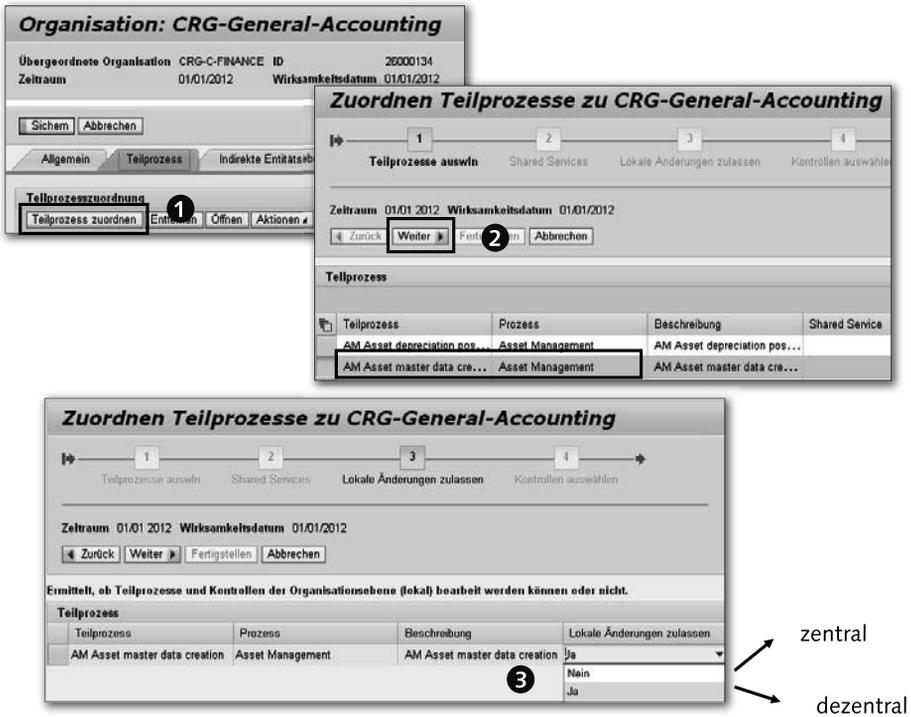


Abbildung 16.17 Voraussetzungen für die Realisierung eines zentralisierten vs. dezentralisierten Ansatzes bei der Stammdatenverwaltung

Optionen bei der Zuordnung von Subprozessen

Während eine Zentralisierung der Aktivitäten in SAP Process Control mithilfe der Rollen gewährleistet werden kann, besteht auf der

Stammdatenseite die Option, Subprozesse den Organisationseinheiten entweder als Referenz oder als Kopie zuzuordnen, wie in Abbildung 16.17 dargestellt ist. Die Zuordnung erfolgt innerhalb einer Organisation. Im Bereich TEILPROZESSE müssen Sie hierzu den Button TEILPROZESS ZUORDNEN ❶ anklicken und anschließend den benötigten Subprozess aus dem zentralen Katalog auswählen ❷. Die Auswahl der Zuordnungsmethode ist ein separater Schritt ❸.

In Abbildung 16.18 sind alle bestehenden Optionen beschrieben, die in SAP Process Control bezüglich der Kontrollpflege zur Verfügung stehen:

- ▶ Wurde ein Subprozess aus dem Zentralkatalog als Referenz zugeordnet ❶, können die zugehörigen Kontrollen nicht mehr geändert werden.
- ▶ Wurde dagegen ein Subprozess als Kopie zugeordnet ❷, können die bestehenden Kontrollen geändert ❸ oder neue angelegt ❹ werden.

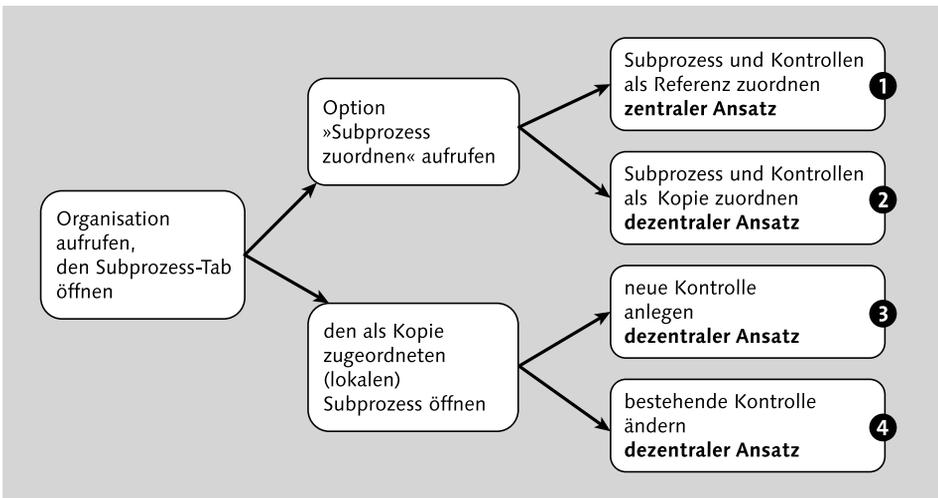


Abbildung 16.18 Zentralisierter vs. dezentralisierter IKS-Dokumentationsansatz in Aktion

In Abschnitt 16.3.3, »Zentrale vs. lokale IKS-Stammdaten«, wurde das Konzept der lokalen vs. globalen Stammdaten beschrieben. Die lokalen Stammdaten entstehen, wenn die Subprozesszuordnung erfolgt ist.

Technische Details
und Konfiguration

Shared-Services-Konzept im IKS

Betriebs-
wirtschaftliche
Sicht

Die Quintessenz des in SAP Process Control abgebildeten Shared-Services-Konzepts besteht in der mehrfachen Wiederverwendung der gleichen Prozess- und Kontrollhierarchie und insbesondere in der mehrfachen Wiederverwendung der Test- und Bewertungsergebnisse innerhalb einer Auflage.

Aus betriebswirtschaftlicher Sicht kann die Wiederverwendung von Prozess- und Kontrollhierarchien sowie von Test- und Bewertungsergebnissen bei den folgenden beiden IKS-Szenarien – Outsourcing und generellen IT-Kontrollen – erforderlich sein.

[zB]

Outsourcing oder zentralisierte Dienstleistungen

Wurden bestimmte Dienstleistungen im Unternehmen ausgegliedert oder innerhalb von sogenannten Shared Services hausintern zentralisiert, beinhaltet das die folgende Herausforderung für den IKS-Prozess: Bei den zentralisierten Prozessen werden die Kontrollen zwar de facto »aus einer Hand« abgewickelt, bleiben aber weiterhin formell in Verantwortung aller Einheiten, die sich der entsprechenden Prozesse bedienen (siehe Abschnitt 6.1.2, »IT-Outsourcing: Wer ist verantwortlich für die Kontrollen?«).

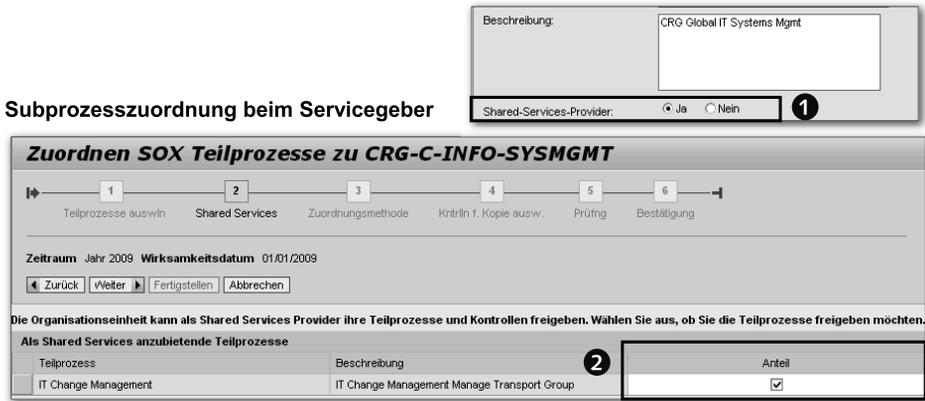
Nicht nur organisatorische, sondern auch IKS-spezifische Herausforderungen führen in einem Umfeld, in dem Geschäftsprozesse IT-gestützt ablaufen, zu einer ähnlichen Situation.

[zB]

IT-General-Controls-Szenario

Angenommen, dieselbe IT-Anwendung wird von mehreren Einheiten innerhalb eines Unternehmens genutzt. Jede Einheit kann dabei unterschiedliche geschäftsprozessspezifische Kontrollmechanismen in eigener Zuständigkeit haben. Dabei sind die IT General Controls zentralisiert, deren Verantwortliche in der Regel einer IT-Abteilung angehören. Diese IT General Controls haben Gültigkeit für die ganze Anwendung und dementsprechend auch für alle Einheiten, die diese Anwendung einsetzen.

In beiden beschriebenen Fällen besteht der Bedarf, die Ergebnisse der Tests und Bewertungen für gleiche Kontrollen für mehrere Organisationen verfügbar zu machen. Die Herausforderung, diesen Ansatz technisch umzusetzen, wird in SAP Process Control mithilfe der Shared-Services-Funktion gelöst.



Subprozesszuordnung beim Servicennehmer

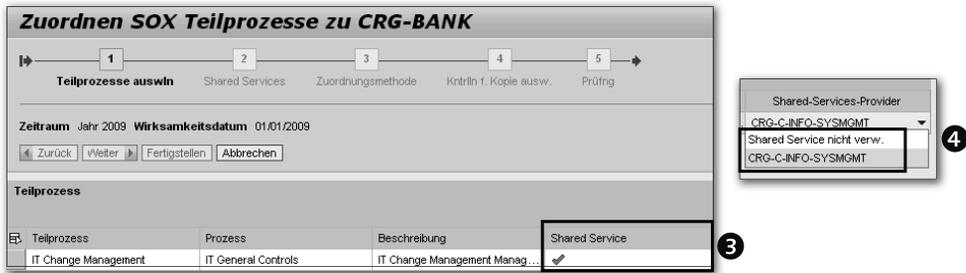


Abbildung 16.19 Abbildung des Shared-Services-Szenarios

Wie Sie in Abbildung 16.19 sehen, müssen folgende Voraussetzungen für die Verwendung der Shared-Services-Funktionalität gewährleistet sein: Voraussetzungen

- ▶ Die Auswahl der entsprechenden Option muss in einer Servicegeber-Organisation ① getroffen werden.
- ▶ Des Weiteren müssen die in der Servicegeber-Organisation verwendeten Subprozesse für die Wiederverwendung von den Servicennehmer-Organisationen freigegeben sein ②.
- ▶ Bei der Zuordnung von Subprozessen zu einer Servicennehmer-Organisation werden die freigegebenen Subprozesse als solche gekennzeichnet ③.
- ▶ Im weiteren Schritt ④ ist die Servicegeber-Organisation in einer Drop-down-Liste auszuwählen.

Sie haben nun einen Eindruck davon erhalten, wie die Dokumentation eines IKS-Frameworks in SAP Process Control abgebildet wird.

16.4.2 Scoping-Prozess

In Abschnitt 1.2.1, »SOX in den USA«, wurde der Prozess der Kontrollauswahl (Top-down Risk Based Scoping) erstmals erwähnt. Das Ziel dieses Prozesses ist es, Kontrollbereiche zu priorisieren. Da dieser Prozess vom Gesetzgeber nicht als zwingend vorgeschrieben ist und es nur eine allgemeine Anleitung gibt, haben sich in der Praxis diverse Szenarien etabliert. Einige dieser Szenarien werden in SAP Process Control angeboten.

Wesentlichkeitsbasierter Scoping-Prozess

Betriebs-
wirtschaftliche
Sicht

In Abschnitt 15.3.2, »Selektion und Priorisierung von Kontrollaktivitäten«, wurde Scoping als eines der Grundszenarien der IKS-Aktivitäten erläutert. Dabei kommt eine wesentlichkeitsbasierte Beurteilung zum Einsatz, die sich an der Höhe der Salden von einzelnen Konten oder deren Gruppen orientiert – manchmal initial beim Aufsetzen eines Kontroll-Frameworks, bei einigen Unternehmen findet dieser Prozess aber auch regelmäßig statt, zum Beispiel jährlich.

Kontengruppen in
SAP Process
Control

Der wesentlichkeitsbasierte Auswahlprozess wird in SAP Process Control unterstützt. Dabei spielen *Kontengruppen* als Verbindung zwischen Finanzberichterstattung und den Prozessen eine zentrale Rolle (siehe hierzu auch Abschnitt 15.2.6). Die Hierarchie der Kontengruppen wird im Arbeitsbereich STAMMDATEN und hier in der Menügruppe KONTEN angelegt. In Abschnitt 16.4.1, »IKS-Dokumentationsprozess«, ist die Rolle der Kontengruppen im Datenmodell von SAP Process Control beschrieben.

Zwei Optionen

Abbildung 16.20 zeigt, wie der wesentlichkeitsbasierte Scoping-Prozess in SAP Process Control realisiert ist. Über den Pfad STAMMDATEN • KONTEN sind zwei Optionen zu finden:

- ▶ KONSOLIDIERTE SALDEN (Consolidated Balances and Significance)
- ▶ ORGANISATIONSBIANZEN (Organization-Level Balances and Significance)

Durchführung

Bei beiden Scoping-Optionen müssen folgende Schritte durchgeführt werden:

1. Die Salden der einzelnen Kontengruppen werden entweder in einer Microsoft Excel-Form ❶, die herunter- und hochgeladen werden kann, oder direkt in der Anwendung manuell gepflegt ❷.

2. Anschließend wird ein Schwellenwert für die Wesentlichkeit festgelegt und angewendet ③.
3. Als Ergebnis werden sowohl die relevanten Kontensalden ④ als auch Organisationen und Subprozesse automatisch markiert (dies kann aber auch manuell vorgenommen werden).
4. Die Scoping-Ergebnisse werden per Default pro Jahr gespeichert, können aber flexibel konfiguriert werden.

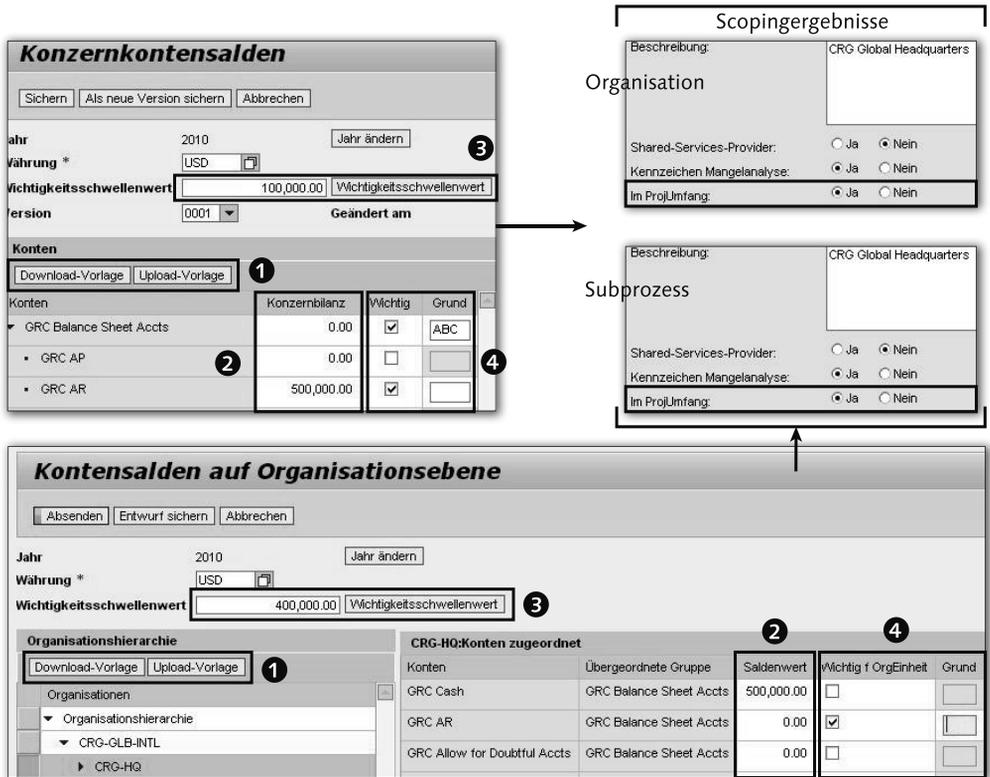


Abbildung 16.20 Wesentlichkeitsbasierter Scoping-Prozess

Der Unterschied zwischen den zwei beschriebenen Ansätzen besteht darin, dass bei der zweiten Option die Kontensalden pro Organisation gepflegt werden können. Bei der ersten Option kommt eine Kontengruppe dagegen nur einmal vor, und deren Saldo stellt einen konsolidierten Wert dar.

Unterschied der Optionen

Risikobasierter Scoping-Prozess

Workflowbasierte Risikobeurteilung

Die Inhalte eines Scoping-Prozesses variieren in der Praxis: Während die Wesentlichkeitsanalyse ein mehr oder weniger einheitliches und weit verbreitetes Scoping-Verfahren ist, gestalten Unternehmen die Folgeschritte im Rahmen der top-down-risikobasierten Kontrollauswahl sehr unterschiedlich. SAP bietet hierfür in SAP Process Control zwei Szenarien an:

- ▶ qualitative Bewertung der Risiken
- ▶ Risikoeinstufung von Kontrollen

Szenarien Beide Szenarien sind workflowbasiert, das heißt, der Benutzer erhält in seiner Inbox eine Aufgabe zur Abarbeitung.

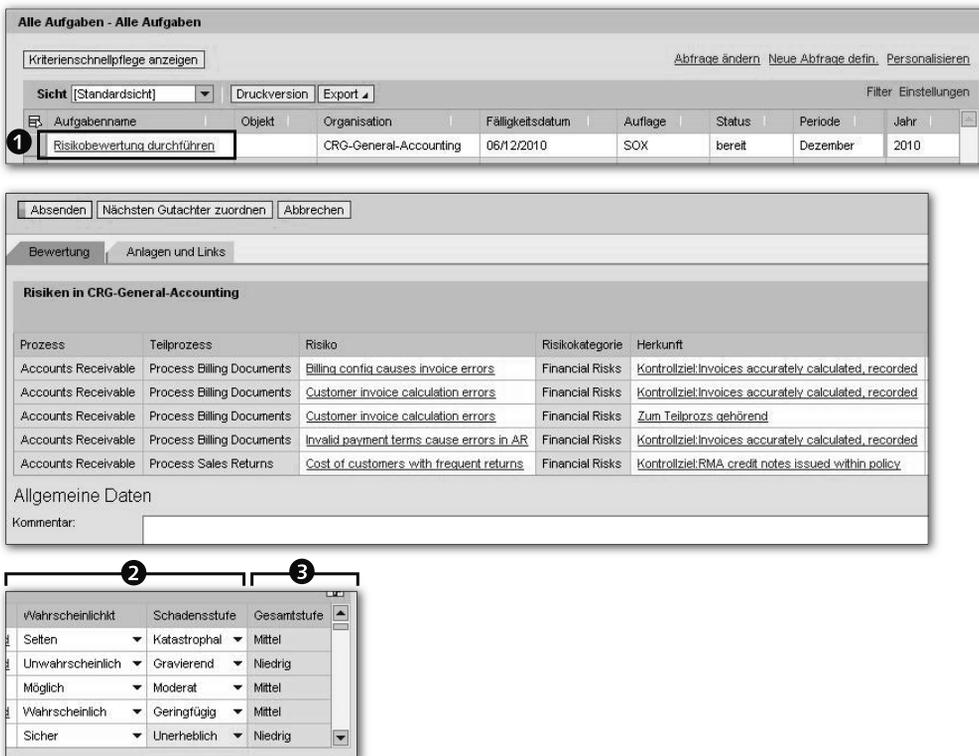


Abbildung 16.21 Risikobewertung als Teil des Scoping-Prozesses

Qualitative Bewertung der Risiken

In Abbildung 16.21 sehen Sie den Ablauf der Risikobewertung. Nachdem der Benutzer eine Aufgabe per Workflow in der Inbox erhalten hat ①, müssen zwei Risikodimensionen bewertet werden ②:

zum einen die Eintrittswahrscheinlichkeit (Probability) und zum anderen eine mögliche Schadenshöhe (Impact). Das Endergebnis dieser Bewertung ist die qualitative Einstufung der Risiken ③ entsprechend der hinterlegten Entscheidungsmatrix. Der Benutzer hat bei der Bewertung die Möglichkeit, Einzelheiten zu den Risiken und deren Herkunft im Datenmodell einzusehen (es gibt drei Optionen, siehe Abschnitt 16.3.2, »IKS-Datenmodell in SAP Process Control«).

Gültigkeit der Bewertungsergebnisse

[+]

Es ist wichtig zu wissen, dass die Bewertungsergebnisse nur für einen bestimmten Zeitraum gelten. Dieser Zeitraum wird bei der Planung festgelegt (siehe Abschnitt 16.4.3, »Planungsprozess, Tests und Bewertungen«) und ist zum Beispiel im Reporting sichtbar (siehe Abschnitt 16.4.5).

Arbeitseingang

Aufgabenname	Objekt	Organisation	Fälligkeitsdatum	Auflage
Kontrollrisikobewertung durchführen	IT Acquire and maint apps software	CRG-General-Accounting	06/14/2010	SOX
Kontrollrisikobewertung durchführen	IT Back up and recovery	CRG-General-Accounting	06/14/2010	SOX
Kontrollrisikobewertung durchführen	IT Change Management	CRG-General-Accounting	06/14/2010	SOX

↓

Kontrollrisikobewertung durchführen: CRG-General-Accounting

Organisation: CRG-General-Accounting Teilprozess: IT Acquire and maint apps software Bewertungszeitraum: Jahr 2010

Absenden Nächsten Gutachter zuordnen Abbrechen Weiter

Bewertung Anlagen und Links

Kontrolle	SchwSt. letzt. Jahr	Mangel Vorjahr	Komplexität	Historie der Kontrollfehler	Attributwert	Attributwert	Gesamteinstufung
IT org uses SDLC methodology	0		Einstufung 2	Niedrig	Niedrig	Niedrig	Niedrig
IT SDLC includes devel and changes	0		Einstufung 4	Mittel	Hoch	Hoch	Mittel

Allgemeine Daten
Kommentar:

↓

Scopingergebnisse

Name: * IT SDLC includes devel and changes

Beschreibung: The organization's SDLC policies and procedures consider the development and acquisition of new systems and

Kontroll- oder Prozessschritt: Kontrolle Prozessschritt

Kontrollkategorie: Allgemeine Kontrolle iEEK-Test

Wichtigkeit: Hauptkontrolle

Nachweisebene: Empfohlenes System verwenden Stufe 3: Kontrolldesign-Bewertung und Kontrollwirksamkeit

Kontrollrisiko: Empfohlenes System verwenden Mittel

Abbildung 16.22 Kontrollrisikobewertung als Teil des Scoping-Prozesses

In Abbildung 16.22 sehen Sie den Ablauf des zweiten Scoping-Szenarios, bei dem die Kontrollen einer Risikoeinstufung unterzogen wer-

Risikoeinstufung von Kontrollen

den. Bei der Bearbeitung eines Tasks (diese werden pro Subprozess generiert) haben Sie die Möglichkeit, die Einzelheiten zu den Kontrollen sowie die bestehenden Problemfälle einzusehen ❶. Die zu bewertenden Kriterien sind flexibel konfigurierbar, die Werte sind per Dropdown auswählbar ❷. Das Endergebnis ist die Risikoeinstufung der Kontrollen ❸, entsprechend der hinterlegten Entscheidungsmatrix, die in die Stammdaten der jeweiligen Kontrollen übertragen wird ❹. Die Ergebnisse der Risikoeinstufung werden in das Kontrollattribut KONTROLLRISIKO übernommen; dieses Attribut kann bei Bedarf auch manuell gepflegt werden (falls die Konfiguration dies erlaubt).

Vergleich Während bei der Risikobewertung zwei Kriterien – Eintrittswahrscheinlichkeit und Schadenshöhe – vorgegeben sind und nur die möglichen Werte angepasst werden können, können bei der Risikoeinstufung der Kontrollen beliebige Bewertungskriterien definiert werden. In beiden Fällen kann die Ableitungslogik in einer Matrix hinterlegt werden. Die jeweiligen Einstellungen sind im Einführungsleitfaden über GRC • PROCESS CONTROL • UMFANGSERMITTLUNG zu finden.

Ableitung der kombinierten Risikobewertungsergebnisse

Das Feld NACHWEISEBENE stellt eine weitere Option dar, um einen risikobasierten Ansatz im IKS einzurichten. In diesem Feld können Werte entweder manuell eingetragen oder automatisiert ermittelt werden (als Kombination der Werte für Kontrollrisikolevel und Risikolevel). Die Ableitungsregeln – *Kontrollrisikolevel + Risikolevel = Nachweisebene* – werden im IMG gepflegt: GRC • PROCESS CONTROL • UMFANGSERMITTLUNG • NACHWEISEBENE SETZEN.

16.4.3 Planungsprozess, Tests und Bewertungen

Mithilfe der Planungsfunktion werden in SAP Process Control workflowbasierte IKS-Aktionen angestoßen. Diese Funktion ist im Arbeitsbereich BEWERTUNGEN und hier in der Menügruppe BEWERTUNGSPLANUNG unter PLANER zu finden.

In der Planungsfunktion sind aufgrund der Harmonisierung von Funktionen einzelner Komponenten im GRC-Release 10.0 erstmalig Aktivitäten aller GRC-Komponenten zu finden, das heißt nicht nur Aktivitäten für SAP Process Control.

Harmonisierter Planer in Release 10.0

Wie Sie in Abbildung 16.23 sehen, beginnt die Planung mit der Auswahl der durchzuführenden Aktivität, der Periode, des Startdatums und eines Fälligkeitsdatums (Deadline) ❶.

Index

- 3-Way-Match 363
 - 8. EU-Richtlinie 49
 - Artikel 39 bis 41 49
 - interne Revision 50
 - Kontroll- und Risikomanagementsystem 49
 - strategisches Risiko 50
-
- ## A
-
- ABAP Code Security 248
 - ABAP Command Injection 252
 - ABAP Editor 189
 - ABAP-Programm 189
 - Abgleich Haupt- und Nebenbuch 305
 - Abschlussarbeit 303, 369
 - Abschlussprüfer 66
 - Abschlussrichtlinie → 8.EU-Richtlinie 49
 - Abschreibung für Abnutzung (AfA) 334
 - Abschreibung offener Forderung, nicht ordnungsgemäße 459
 - Abschreibungsschlüssel 333, 338
 - Abstimmarbeit 304
 - Abstimmkonto 345, 501, 502
 - Abstimm-Ledger 319
 - Abweichung 363
 - Abwertung 352
 - Accelerated SAP (ASAP) 471, 673
 - Access Risk Management (ARM) 133, 138
 - Funktionstrennungsverletzungen 139
 - kompensierende Kontrollen 138
 - Organizational Rules 138
 - ACL 151, 488
 - Administration
 - BI-Mappe 259
 - Nummernkreisintervall 259
 - Profilparameter 259
 - RFC-Verbindung 259
 - SAP-Instanz 259
 - Transport Management System 259
 - Administrationsberechtigung 129
 - Aktiengesetz (AktG) 50
 - Altersstruktur 352
 - Analyse
 - Datenänderung 507, 518
 - Kreditmanagement 520
 - Kundenstammdaten 520
 - Stammdaten 506
 - Stammdatenqualität 499
 - Änderungsbeleg 265, 269, 491, 569
 - konfigurieren 423
 - löschen 259
 - Programm RSSCD100 491
 - Änderungsprotokoll 184
 - Anlage 332
 - Anlagenbuchhaltung 331
 - Bewegungsart 342
 - Konsistenzprüfung 336
 - Kontenfindung 334
 - Rechenmethode 338
 - Vorschlagswert 333
 - zurücksetzen 344
 - Anlagengitter 339
 - Anlagengitterreport 332
 - Anlagenklasse 332, 333
 - Anonymisierung von Daten 425
 - Anschaffungs- und Herstellkosten (AHK) 341
 - Anti-Fraud-Kontrolle 446
 - Anti-Fraud-Kontrolle, automatisierte 446
 - Anti-Virus-Software 127
 - Application Link Enabling (ALE) 288
 - ALE-Audit 179
 - Auditing 288
 - Application Security 123
 - Applikationskontrolle 121
 - Applikationslebenszyklus 130
 - Arbeitnehmerdatenschutz 419
 - ARF/CMF-Szenarien
 - Aufwand 681
 - Implementierung 691
 - Arznei- und Lebensmittelherstellung 465
 - Arzneimittelzulassungsbehörde 465
 - Assertion 90, 294
 - asynchroner RFC 290
 - Audit 126
 - Audit and Assurance Faculty Standard (AAF), 01/06 219
 - Audit Committee 45, 51
 - Audit Standards Committee, Report No. 18 219
 - Audit-Informationssystem (AIS) 150, 649
 - Auditing and Assurance Standards Board (AASB) 219
 - Aufbewahrung von Daten 421
 - Auflage 574
 - auftrags- und lieferbezogene Fakturierung 395
 - Auftragsdatenverarbeitung 413
 - Auftragserfassung 386, 387
 - Auftragskontrolle 419
 - Ausgangssteuer 310
 - Ausgleichsdatum 176
 - Auskunftsrecht 415
 - Auswertung
 - gemerkter Beleg 304
 - vorerfasster Beleg 304
 - Auswertungsweg 435
 - Auszifferung 368
 - Automated Controls Framework (ACF) → Continuous Monitoring Framework
 - Automated Monitoring Framework (AMF) → Continuous Monitoring Framework

automatische Buchung 307
 automatische Verkaufspreiser-
 mittlung 396

B

Bankstammdatenänderung
 304
 Bankverbindung 389
 Basel II 58
 Basel III 60
 Basisberechtigung 258
 Batch-Input-Mappe 293
 Batch-Input-Verfahren 292
 Batch-Job-Log-File 450
 Batch-where-used-Liste 477
 BC-Set 473, 555, 672, 676
 Beanstandung 48
 Deficiency 48
 Material Weakness 48
 Significant Deficiency 48
 Bedarfsanforderung 488, 508
 Bedarfsanforderung, Verände-
 rung 508
 Befehl
 AUTHORITY-CHECK 244
 CALL TRANSACTION 244
 Behebung 545
 Beleg
 Änderbarkeit 267
 Änderung 269
 Änderungsregel 268
 Archivierung 275
 Nichtveränderlichkeit in SAP
 ERP 90
 Stammdaten 326
 Substitution 311
 Validierung 311
 Vorerfassung 275, 315
 Belegdaten analysieren (Haupt-
 buch) 453
 Belegdatum 175
 Belegkopf 174
 Belegnummernkreisintervall
 276
 Belegnummernpufferung 275
 Belegnummernvergabe 274
 Belegsegment 174
 Benutzer 208
 anonymer Benutzer-Account
 237
 Attribut 208
 Benutzergruppe 260
 Benutzerinformationssystem
 202, 237
 Benutzermenü 189
 Benutzertyp *Kommunika-*
 tion 210
 Benutzertyp *Service* 210
 Benutzertyp *System* 210
 Benutzerverwaltung 236
 Benutzerverwaltungskon-
 zept 221
 Berechtigungsauswertung
 211
 Berechtigungsvergabe 261
 Dialogbenutzer 209
 Eigenschaft *Benutzertyp* 210
 Identität 235
 Lebenszyklus 235
 Notfallbenutzer-Konzept 242
 Referenzbenutzer 210
 SAP-System 208, 209
 Standardbenutzer 240
 Standardkennwort 241
 Toleranzgruppe 324
 Berechtigung
 Berechtigung in AA 343
 Berechtigungsgruppe 246,
 302
 Berechtigungshauptschalter
 440, 441
 Berechtigungskontrolle 198
 Berechtigungskonzept 221
 Berechtigungsverwaltung
 128
 Berechtigungskonzept 129
 Berechtigungsobjekt 199, 432
 Aktivität 200
 Dokumentation 202
 Ermittlung 203
 F_BKPF_BUK 200, 201,
 204, 212
 F_BKPF_KOA 204, 213
 F_KNA1_APP 390
 F_KNA1_BUK 390
 *M_BAN_** 358
 *M_BES_** 358
 M_BEST_WRK 205
 M_ISEG_WDB 377
 M_MATE_MAR 373
 M_MATE_STA 373
 M_MATE_VKO 373
 M_MATE_WRK 373
 M_MSEG_BMB 380
 M_MSEG_BMF 380
 M_MSEG_BWA 362, 380,
 393
 M_MSEG_BWE 380
 M_MSEG_LGO 380
 P_ORGIN 432, 434, 440,
 441, 462
 P_ORGINCON 441
 P_ORGXX 441, 462
 P_ORGXXCON 439
 P_PCLX 432
 P_PERNR 432, 434, 440,
 461
 PLOG 432
 Prüfung ausschalten 256
 S_BCD_MONI 258
 S_BDC_MONI 294
 S_BTCH_NAM 450
 S_PRO_PAGE 258
 S_PROGRAM 246
 S_RFC 258
 S_SCDO 271
 S_TCODE 199, 204, 212
 strukturelle Berechtigung
 439
 Tabelle USOBT 205
 V_KNA1_BRG 390
 V_KNA1_VKO 390
 V_KNKK_FRE 390
 V_VBRK_FKA 400
 V_VBRK_VKO 400
 V_VBUK_FRE 390
 Vorschlagswert für Profilage-
 erator 205
 Wertefeld 199
 Berechtigungsobjektebene
 256
 Berechtigungsprüfung 256
 Berechtigungsprüfung, Profil-
 parameter 257
 Bericht direkt aufrufen 246
 Beschaffungskennzeichen
 502, 504

- Beschaffungsprozess 488
 Bestand
 bewerteter 373
 getrennte Bewertung 374
 unbewerteter 373, 383
 Bestätigungsvermerk 76
 Bestellanforderung, fristgerechte Freigabe 489
 Bestellbestätigung 514, 517
 Bestelleingang 497
 Bestellung 358, 488
 Bestellung fristgerecht anlegen 495
 Bestellwesen 357
 Best-Practice-Rollenkonzept 614
 Betriebssystemkommando 277
 Betriebsverfassungsgesetz (BetrVG) 410
 Betrug 443
 Batch-Input-Mappe 449
 betrügerische Belegbuchung 451
 betrügerische Finanzberichterstattung 444
 Betrugsart 444
 betrugsbegünstigender Faktor 445
 manueller Journaleintrag 452
 zum Missbrauch genutzte Funktion 448
 Betrugsmöglichkeit 446
 SAP-Basis 448
 SAP-Hauptbuch 450
 SAP-Personalbuchhaltung 459
 SAP-Vertriebsbereich 454
 Bewegungsart 342, 361, 375, 393
 501 362
 561 362
 Bewegungsdaten 272
 bewertete Warenbewegung 399
 Bewertungsbereich 332
 Bewertungsdifferenz 505
 Bewertungsplan 332
 Bewertungsverfahren 421
 Big Four 80
 Bilanz 299
 Bilanzbetrug/-fälschung 451
 Bilanzgliederung 536
 Bilanzstruktur 299
 Bilanzrechtsmodernisierungsgesetz (BilMoG) 51
 Bonus 456
 BRG → Business Role Governance (BRG)
 BS 7799 112
 Buchhaltungsbelegänderung 304
 Buchung
 beschränken 451
 Sperre 451
 Buchungskreis 196, 321
 Buchungskreis, Produktivkennzeichen 321
 Buchungsperiode 296, 299
 Buchungssatz, abgebrochener 303
 Bundesamt für Gesundheit (BAG) 466
 Bundesamt für Sicherheit in der Informationstechnik (BSI) 119, 121
 Bundesamt für Umwelt (BAFU) 468
 Bundesdatenschutzgesetz (BDSG) 132, 410, 420
 Bundesministerium für Gesundheit und soziale Sicherung (BMGS) 466
 Business Blueprint 222, 674
 Business Performance Management (BPM) 625
 Business Process Change Analyzer 480
 Business Process Repository 163
 Business Role Governance (BRG) 133, 140, 142
 Business Rule 642
C
 CAAT-unterstützte Abfrage 454
 Canada, NI 52-109 46
 Canadian Institute of Chartered Accountants (CICA), 5970 219
 Capability Maturity Model Integration (CMMI) 111
 CEA 133, 144
 CEAVOP → Assertion
 Centralized Emergency Access (CEA) 133, 144
 Change Log Tool 658
 Change Management
 Audit 82
 Change-Management-Richtlinie 221
 FDA 473
 Charge 477
 Chargenverwaltung 374
 Chief Compliance Officer 546
 China 48
 Basic Standard for Enterprise Internal Control 48
 Business Management IT-Systems 48
 Cisco-Sona-Prüfregel 650
 C-Level-Management 115
 Cluster-Tabelle 489
 Code of Federal Regulations (CFR) 466
 Codeanalyse-Tool 254
 CO-FI-Integration 382
 Committee of Sponsoring Organizations of the Treadway Commission 104
 Competence Center 216
 Compliance 25, 41
 auf Knopfdruck 28
 Automatisierung 528
 GRC 27
 Herausforderung 26
 Compliance/Automatisierung, Projekterfahrungen 671
 Compliance-Initiative 574
 Compliance-Management-Software (CMS) 635
 compliancerelevanter Leitfaden 122
 Computer Aided Test Tool (CAT) 229
 Computer Assisted Auditing Techniques (CAAT) 151, 628

- Computer Center Management System (CCMS) 280
 Conference-Room-Pilot 674
 Content 153, 161
 Content Lifecycle Management (CLM) 135, 156
 Content Lifecycle Management → CLM
 Continuous Compliance & Monitoring 694
 Continuous Control Monitoring 136, 692
 Continuous Monitoring Framework 146, 152, 155, 488, 601, 638, 648, 680
Analyse der Änderung 656
Analyseregeln 653
Aufbau in SAP GRC 10.0 641
BW-Skript 665
Change Log Tool 658
Effizienz 488
Erwartungshaltung 639
GRC Integration Framework 641, 644
Kontrolle 661
Potenzial 639
Protokollierung 658
Regel 642
Skripttyp 649
Teilszenario 648
vordefinierte Regel 660
Wirtschaftlichkeit 488
 Continuous Monitoring Framework, Teilszenario
Business-Warehouse-Abfrage 648
Ereignis 648
Funktionsstrennungintegration 648
konfigurierbares 648
programmiertes 648
Prozessintegration (PI) 648
Reportprogramm 648
SAP-Abfrage 648
 Continuous Rules Monitoring (CRM) 637
 Conto pro Diverse (CpD) 180, 350
 Control Design Assessment 587
 Control Objectives for Information and Related Technologies 104
 Control Risk Assessment 587
 Corporate Governance 383, 534
 Corporate Governance Kodex 48
 COSO-Cube 526, 528
 Critical Action Risk 619
 Cross-Client Database Access 252
 Cross-Site 252, 253
 Custom Field 676, 680
 Customizing-Verteilung 233
- D**
-
- Dänemark 54
Auditors' Act 55
Financial Statements Act 54
 Data Browser 181
 Data Consistency Cockpit 159
 Data Retention Tool (DART-Tool) 631
 DataSource 642
 Daten
anonymisieren 425
lokal speichern 427
 Daten im SAP-System
Bewegungsdaten 173
Datumfeld 175
Konfigurationsdaten 176
Stammdaten 172
Suche 180
 Datenänderung 507
 Datenauswertung 482
Effizienz 482
Grundvoraussetzung 482
Wirtschaftlichkeit 482
 Datenextraktion 631
 Datenschutz 81, 280, 409
Datenschutzbeauftragter 416
Datenschutzkommission 416
datenschutzrelevanter übergreifender Kontrollmechanismus 422
Datenverarbeitung 411
Gesetzgebung Deutschland 410
personenbezogene Daten 411
Schweiz 411
sensitive Daten 411
 Datenschutzrichtlinie
Richtlinie 95/46/EG 408, 410
Safe-Harbor-Grundsatz 417
 Datensicherung 221
 Datenübermittlung
an Dritten 413
Drittland 416
 Dauerbuchung 318
 Dauerbuchungsurbeleg 269, 304
 Debitorenstammdatenänderung 304
 Debugging 265, 277
 Designtest 542
 Deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 58
 Deutscher Corporate Governance Kodex (DCGK) 50
 Deutschland 50
AktG 50
BaFin 58
BilMoG 51
Cromme Code 51
DCGK 50
HGB 50
KonTraG 50
MaRisk (VA) 58
 Deutschsprachige SAP-Anwendergruppe (DSAG) 122, 125
 Directory 253
 Dokumentation 220
 Dokumentationsmanagementsystem (DMS) 471, 472
 doppelte Rechnungserfassung 366
 Dreiecksgeschäft 396
 DSAG-Leitfäden 131
- E**
-
- EarlyWatch Alert 131, 231
 Effektivitätstest 542, 591

- Eigenentwicklung 244
 Eingabekontrolle 419
 Einkaufsbeleg, Kontierung 514
 Einkaufsbelegart 358
 Einkaufsbestelldatum 483
 Einkaufsorganisation 196
 Einkaufsprozess 355
 Einkaufsprozess, dezentraler/zentraler 357
 Einmalkunde 350
 Einmallieferant 350
 Einverständniserklärung 414
 Einzelpostenanzeige 303
 E-Learning 234
 E-Mail-Sicherheit 127
 England 53
 Combined Code on Corporate Governance 53
 Turnbull Guidance 54
 Enterprise Asset Management (EAM) 476
 Entity-Level Control 46, 99, 587, 594
 Entwicklerrichtlinie 221, 254
 Entwicklerschlüssel 259
 Entwicklungssystem 223
 Ergebnisbereich 196
 Ericsson 694
 Erweiterungspaket 230
 EU-GCP Note for Guidance 469
 EU-Kommission 408
 European Medicines Agency (EMA) 466
 Euro-SOX 49
 extended CATT (eCATT) 229
 externe Belegnummernvergabe 274
- F**
-
- Faktura
 erfassen 401
 Statusliste 402
 überleiten 401
 Fakturavorrat 400, 459
 Fakturierung, auftrags- und lieferbezogene 395
- Fälligkeit analysieren 454
 Fälligkeitsdatum 176, 352
 FDA-Compliance 465, 466
 IT 469
 Systempflege 479
 Federal Register 466
 fehlerhafte Rechnung 395
 Feldstatusgruppe 302, 308, 500
 Fertigerzeugnis 381
 Feuerschutz 221
 fiktive Rechnung 454
 fiktiver Angestellter 460
 File Upload 253
 FIMPRCH_05T1_01_A 661
 Financial Instruments and Exchange 46
 Financial Services Agency (FSA) 47
 Financial Systems Integration Office 120
 Finanzberichterstattung 66
 Finanzbranche
 Basel II 58
 Basel III 60
 EU-Richtlinie 58
 EU-Richtlinie 2006/48/EG 58
 EU-Richtlinie 2006/49/EG 58
 MaRisk 58
 MRC 60
 Solvency II 57
 First expired – First out (FEFO) 478
 First-Level-Berechtigung 614
 Flow Chart 550
 Food and Drug Administration (FDA) 155, 465
 Bestimmung 465
 Change Management 473, 479
 Compliance automatisieren 528
 Configuration Management 479
 Prozess 528
 risikobasierte Validierung 471
 Validierung 469, 470
- Foreign Practice Act 383
 Forensik 452
 formelle Ordnungsmäßigkeitsanforderung 89
 Frankreich 54
 AMF 54
 Loi de Sécurité Financière 54
 Fraud-Audit 81
 Freigabekennzeichen 359
 Freigabestrategie 358
 mit Klassifizierung 358
 ohne Klassifizierung 359
 Werteingabe 361
 Fremdwährung 313
 Fremdwährungsdifferenz 314
 Funktionstrennung 55, 260, 329
 Basis 260
 Benutzerpflege 260
 Controlling 381
 Designtest vs. Umfrage 544
 Dokumentation 261
 Entwicklung 260
 Ericsson 698
 Finanzbuchhaltung 330
 Hauptbuch 329
 IKS-Applikation 542
 Kontrolle 696
 mangelnde 535
 Matrix 261
 Profilgenerator 260
 Stammdatenpflege 390
 Transportauftrag 260
 überwachen 663
- G**
-
- Geldwäsche 384
 gemerkter Beleg 304
 Generally Accepted Accounting Principles (GAAP) 73
 Generic Module Execution 252
 geringwertige Wirtschaftsgüter (GWG) 341
 Geschäftsbereich 196
 Geschäftsjahresvariante 296
 Geschäftspartner, Toleranzgruppe 324

- Gesetz zur Kontrolle und
 Transparenz im Unterneh-
 mensbereich (KonTraG) 50
 Gesetzeskonformität 42
 gesetzliche Datenschutzerfor-
 derung 408
 getrennte Bewertung 373
 Gewinn- und Verlustrechnung
 (GuV) 299
 gleitender Durchschnittspreis
 378
 globaler Roll-out 233
 globales System-Log 278
 Good Automated Manufactu-
 ring Practice (GAMP) 467
 Good Manufacturing Practice
 (GMP) 467
 Governance, Risk, and Compli-
 ance → GRC
 Gratisware 457
 GRC 132
 Integration Framework 641,
 644, 677
 Integration mit Audit
 Management 149
 Integrationszenarien 148
 Policy Management 145
 SAP Access Control 138
 SAP Process Control 133
 SAP Risk Management 147
 Upload Tool 673
 Grundsätze ordnungsmäßiger
 Buchführung (GoB) 72, 73
 Grundsätze ordnungsmäßiger
 Buchführungssysteme
 (GoBS) 88, 118
 formelle 89
 IT-spezifische 88
 materielle 89
 Grundsätze zum Datenzugriff
 und zur Prüfbarkeit digitaler
 Unterlagen (GDPdU) 81,
 120, 631
 Guidance Statement (GS), 007
 219
 Guide to the Assessment of IT
 Risk (GAIT) 107
 gute Arbeitspraxis 468
 gute klinische Praxis 468
 gute Laborpraxis 468

 Gutschrift 398, 399, 456
 Gutschrift/Bonus, nicht ord-
 nungsgemäße/r 456

H

 Halbfabrikat 381
 Handelsgesetzbuch (HGB) 50
 Hauptbuch 296
 Belegdaten analysieren 453
 Betrug 450
 betrügerische Belegbuchung
 451
 Kontrollbericht 303
 Health Insurance Portability
 and Accountability Act
 (HIPAA) 81
 Health Products and Food
 Branch (HPFB) 466
 Herstellmaterial, Kalkulation
 502
 Hilfsmittel
 Dokumentation 673
 Stammdaten 673
 Hilfstransaktion 344
 Historie, Transaktionsaufruf
 280
 HKSA-Statement, Auditing
 Practice Note 860.2 219
 HR-Berechtigung
 Auswertungsweg 435
 Berechtigungshauptschalter
 441
 Berechtigungslevel 434
 Berechtigungsobjekt 432,
 434
 Kontextlösung 438
 strukturelle 436
 strukturelles Profil 436
 HR-Daten, Zugang limitieren
 461
 Human Capital Management
 231, 407, 430

I

 ICH-GCP-Guidelines 469
 IDEA 151

 Identität 235
 Identitätsprinzip 235, 236
 Identity Management 236
 IKS- und Compliance-Automa-
 tisierung 684
 IKS-Aktion, Matrix 675
 IKS-Automatisierung, Business
 Blueprint 674
 IKS-Framework in Japan 46
 IKS-Inhalt 91
 Applikationskontrolle 97
 *automatisierte Überwa-
 chung* 97
 Entity-Level Controls 99
 *halb automatisierte Kon-
 trolle* 97
 IT General Controls 95
 manuelle Kontrolle 98
 *übergreifende Applikations-
 kontrolle* 96
 Implementierung SAP Process
 Control 671
 Improper Authorization 252
 Incoterm 502, 521
 Information Technology Assu-
 rance Framework (ITAF)
 107
 Information Technology Infra-
 structure Library (ITIL) 106
 Information Technology Secu-
 rity Evaluation Criteria
 (ITSEC) 121
 Informationsmissbrauch 428
 Informationsrecht 415
 Infotyp 423, 430, 433, 564
 Initialkennwort 241
 Injection-Schwachstelle 253
 In-Memory Technologie 62
 Inner-Join 485
 Inspektionsintervall 475
 Instandhaltung 476
 Instandhaltungsmaßnahme
 476
 Institut der Wirtschaftsprüfer
 (IDW) 73
 Intermediate Document (IDoc)
 288
 International Conference on
 Harmonization (ICH) 466

- International Financial Reporting Standards (IFRS) 58, 73
 International Framework for Assurance Engagements 219
 International Organization for Standardization → ISO
 International Society for Pharmaceutical Engineering (ISPE) 467
 International Standard on Assurance Engagements (ISAE) 127
 International Standards of Auditing (ISA) 73
 interne Belegnummernvergabe 274
 interne Revision 76
 Internes Kontrollsystem (IKS) 42
 Aktivität 538
 Anforderung an ERP-System 87
 automatisierte Kontrolldurchführung 541
 Automatisierung 135, 525
 Begriff 43
 Bestätigung der Kontrolldurchführung 541
 Content 677, 683
 Datenmodell 537, 563, 565, 572, 575
 Domäne 533
 Finanzbranche 56
 Funktionstrennung 542
 IKS-bezogenes Audit 81
 IKS-Grundsatz 88
 IKS-Testat 117
 Merkmale der Automatisierung 137
 Modellierung 675
 Multidomänenprinzip 533
 Objekt 530
 Organisationseinheit 530
 Planung 135
 Problembhebungsprozess 595
 Prozess 532
 Prozessdefinition 675
 Risikoorientierung 52
 Rolle 546
 Scoping 540
 Sign-off 545
 Struktur 99
 Umsetzungsmatrix 551
 Verantwortlicher 546
 Vier-Augen-Prinzip 599
 zentral organisiertes 578
 Ziel 43
 Inventur 376
 Inventurkontrolle 377
 Inventurverfahren 377
 ISAE 3402 127, 219
 ISO 238
 ISO 17799 112
 ISO 27k 112
 ISO 9000 218
 IT Security Evaluation Manual (ITSEM) 121
 Italien 55
 Comply-or-Explain-Prinzip 56
 Preda Code 55
 IT-Organisation 216
- J**
-
- Jahresabschluss 66
 Jahresabschlussprüfung 81
 Japan
 Financial Instruments and Exchange 46
 Financial Services Agency 47
- K**
-
- Kalkulationsschema 396
 Key Performance Indicator (KPI) 624
 Key Risk Indicator (KRI) 147, 668
 Klimatisierung 221
 Kombinationsverbot 419
 Kommunikationsbenutzer 291
 Kommunikationssicherheit 127
 kompensierende Kontrolle 139, 620
 Konditionsart 397
 Konditionsart konfigurieren 456
 Konditionstechnik 395
 Konfigurationskontrolle 179
 Konfigurationstabelle 178
 Konsistenzcheck 309
 Konsistenzprüfung 336
 Konsistenzprüfung der Bestände 376
 Kontenfindung 307, 334, 375
 Kontengruppe 297, 501, 536, 537
 Kontextlösung 438
 Kontierung 514
 Kontrollauswahl → Scoping
 Kontrollbericht, Hauptbuch 303
 Kontrolldesign-Bewertung 594
 Kontrolldurchführung bestätigen 541, 550
 Kontrolle 232, 236, 239, 241, 532
 Attribut 532
 Auftragserfassung 387
 Auftragserfüllung und Umsatzlegung 393
 Bestand 371
 Bestellwesen 357
 Bewertung Vorratsvermögen 378
 Bezeichnung des Transportauftrags 224
 FDA/Beschaffung 474
 FDA/Chargenrückverfolgbarkeit 476
 FDA/Implementierungsprozess 472
 FDA/Instandhaltung 476
 FDA/Lagerverwaltungsprozess 477
 FDA/Produktionsmanagement 474
 FDA/Qualitätsmanagement 475
 Funktionstrennung 227
 HR-Daten sperren 461

- im Produktivsystem angelegter Transportauftrag* 227
integrative Funktion 534
Inventurkontrolle 377
Konfigurationskontrolle 179
Kundenstammdaten 388
Mahnprozess 403
Mandanteneinstellung 230
Mandanteneinstellung ändern 230
Materialstammdaten 371
Notfallproduktionskorrektur 227
Paketierung der Transportaufträge 225
*Profilparameter zur Handhabung von SAP** 241
Prozesskontrolle 96, 97
Rücklieferung 399
Sicherheitsrichtlinie 237
Stammdatenkontrolle 179
Standardform und Testdokumentation 226
Transaktionskontrolle 180
übergreifende Applikationskontrolle 96
Verwendung kritischer Bewegungsart 380
Warenauslieferung 393
- Kontroll-Identifizierungsprozess 91
 Kontrollmatrix umsetzen 639
 Kontrollverantwortlicher 546
 Kontrollziel 534
 Korrektur- und Transportwesen (KTW) 281
 KTW-Parameter 282
 KTW-Verzeichnis 282
 Steuerungsparameter 283
 Kostenrechnungskreis 196
 Kostenträger 380, 381
 Kreditausfallrisiko 59, 391
 Kreditkontrollbereich 391
 Kreditlimit 506, 520
 Kreditlimitdaten, Kundenstamm 392
 Kreditlimitkontrolle 391
 dynamische 391
 Pflege 392
 statische 391
- Kreditlimitpflege 388
 Kreditlimitvergabe 391
 Kreditmanagement 304, 520
 Kreditorenrechnung 384
 Kreditorenstammdatenänderung 304
 KRI → Key Risk Indicator
 kritische Administrationstransaktion 258
 kritische Transaktion 329
 Kundenauftrag 497, 517
 Bestätigung 497
 Position 517
 Kundenstamm 389
 Incoterm 521
 Zahlungsbedingung 520
 Kundenstammdaten 388, 500, 520
 Pflege 392
 Qualität 388, 500
 Kundenstammdatenpflege 388
 KUONI 685
- L**

 Lagerentnahmestrategie 477
 Lagerort 196
 Länderdelkredere 346
 Langzeitbeleg 424
 Lebensmittelüberwachung 465
 Lebenszyklus, Benutzer 235
 Leitfaden Datenschutz 131
 Lieferbedingung 520
 Liefertermin 517
 Lizenz 236
 logische Datenbank 185
 Logistik-Rechnungsprüfung 363
 lokales Speichern der Daten 427
- M**

Mahnwesen 402, 403
 Grundeinstellung 403
 Mahnbereich 404
 Mahnprozess 402
 Mahnschlüssel 404
 Mahnsperrrgrund 404
 Mahnverfahren 405
 Management Risk Controlling (MRC) 60
 Mandant 196, 228
 Produktivmandant öffnen 230
 Steuerungsfunktion 228
 Mandantenänderbarkeit pflegen 259
 Mappe 293
 Marktpreisrisiko 59
 Massenänderung 329
 Massenpflege 329
 Massenstorno 329
 Master Data Upload Generator (MDUG) 134, 673
 Material
 Beschaffungskennzeichen 504
 Bewertungsdifferenz 505
 Material Weakness 604
 Materialabwertung 376
 Materialbewegung 375
 Materialbewertung 306
 materielle Ordnungsmäßigkeitsanforderung 89
 Sonderbeschaffungsart 504
 Umlagerung 504
 Materialbewertung 504
 Materialstamm, Workflow 372
 Materialstammdaten pflegen 371
 MDUG → Master Data Upload Generator
 Medical Device Evaluation Committee (MDEC) 466
 Meldepflicht 416
 Metaschicht 668
 Microsoft Operations Framework (MOF) 112
 Mindestanforderungen an das Risikomanagement (MaRisk) 58
 Mindesthaltbarkeitsdatum 375
 minimale Rechtevergabe 244

Ministry for Health, Labour
and Welfare (MHLW) 467
Mitarbeiterdaten 426
Mitarbeitergruppe 196, 431
Mitarbeiterkreis 196, 431
Mitbestimmung von Betriebs-
und Personalrat 419
mobiles Endgerät 244
Modifikation, Überblick 233
Monitoring 158, 541
Multi Application Query Tool
(MQT) 646, 647
Multidomänenanforderung
480
Multidomänenprinzip 572
Multiple Compliance Frame-
work (MCF) 572

N

Nachrichtentyp 288
Nachvollziehbarkeit 422
National Institute of Standards
and Technology 238
National Institute of Standards
and Technology → NIST
National Pharmaceutical Con-
trol Bureau (NPCB) 466
Nettopreis 396
neues Hauptbuch 302, 320,
382
NI 52-109 46
Non-Routine Transaction 306
Notfallbenutzer-Konzept 144,
242
Notfallbenutzer-Prozess 242
Notfallkonzept 127

O

Object-related Security Con-
cept 551
objektbezogene Sicherheit
551, 569, 570, 610, 612
objektgenaue Protokollie-
rung 658
Objekttyp 430
Obligationsrecht (OR) 52

Offline-CAAT-Tool 628
Offline-Datenanalyse 628
Offline-Datenanalyse-Tool
631
Offline-Formular 592
Offline-Test 592
OM → Organisationsmanage-
ment
Online-CAAT-Bericht 634
Operational-Risk-Manage-
ment 147
operationelles Risiko 59
Oracle 153, 155
Order to Cash 385, 387
Organisationseinheit 196,
530
Organisationsmanagement
(OM) 140, 236, 435, 531
Organisationschlüssel 431
Organisationsstruktur 196
Finanzsicht 196
Logistik 196
Materialwirtschaft 196
Personalwirtschaft 196
technische Sicht 196
Vertrieb 196
OS Command 252
OSS-Fehlermeldung 232
Österreich 53
§ 22 *GmbHG* 53
§ 82 *Ak* 53
Art. 1 § 39 des Statuts der
Europäischen Gesellschaft
53
Österreichischer Corporate
Governance Kodex 53
Outer-Join 485
Outsourcing 126, 217, 580

P

parallele Rechnungslegung
300
Passwortschutz 237, 238
Payment Card Industry Data
Security Standard (PCI-DSS)
113
PCAOB-Standard 45
PeopleSoft 153, 155

Personalbereich 196, 431
Personalbeschaffung 426
Personalmaßnahme 432
Personalstammdaten 433
personenbezogene Daten
411, 415, 420
Änderung nachvollziehen
423
Schutznorm 428
verarbeiten 414
Verarbeitungsgrundsatz 415
Pflege der Buchungsperiode
329
Pharmaceutical and Medical
Safety Bureau (PMBS) 467
Pharmaceutical Inspection
Cooperation Scheme (PIC/S)
467
physische Sicherheit 221
Pilotprojekt 682
Plant Maintenance 476
Planungsfunktion 586
Planungsparameter 506, 508
Planungsprozess 508
Planungsstatus 431
Planvariante 430
PoC-Funktionstrennungs-
regel 691
Policy Management 145, 617
Praxiserfahrung 671
Preisabweichung 368
Preisfindung 395
Preissteuerung 378
Procure-to-Pay-Prozess 355
Produktivkennzeichen 321
Produktivsystem 223
Produktkostencontrolling (CO-
PC) 380
Produktkostenrechnung 380
Profilgenerator 260
Profilparameter 257, 278, 285
Profitability-Analysis (CO-PA)
380
Programm
ABAP-Quellcode 192
Berechtigungsgruppe 246
GRPCRTA_CHANGELOG-
GRC 658
Link zur Transaktion 190
modifizieren/entwickeln 259
RAABST01 337

- RAGITT01 332
 RFBABLO0 269
 RFDAUB00 318, 319
 RFDOPFW00 352
 RFDOPR00 352
 RFDOPR10 352
 RFDSLD00 305
 RFHABU00 305
 RFKABLO0 270
 RFKKBU00 305
 RFKSLD00 305
 RFPUEB00 317
 RFSABLO0 270
 RFSSLD00 305
 RFTMPBEL 317
 RFUMSV00 310
 RFUMSV10 310
 RFBVER00 287
 RM07CUFA 309
 RM07MSAL 370
 RS_ABAP_SOURCE_SCAN
 193
 RSBDCOSO 277
 RSPARAM 273, 279, 280,
 281, 283
 RSSCD100 491, 508, 515
 RSSTAT26 281
 RSTBHIST 298, 299
 RSTRFCQDS 292
 SAPF120 318
 SAPF124 367
 SAPF190 302
 Schutz 244, 248
 Suchmöglichkeit Tabelle 193
 TABLES 192
 TFC_COMPARE 302
 Verwendung der Tabelle 192
 Verwendungsnachweis 193
 Projektbeispiel 684
 Proof of Concept (PoC) 682
 Protokoll-Flag 273
 Protokollierung 274, 425, 658
 Provisionierungs-Tool 260
 Prozess 532
 Prozessanalyse 499
 Prozesskontrolle 98
 Prozessverantwortlicher 546
 Prüfer 75, 76, 77
 externer Wirtschaftsprüfer
 75
 Grundsatz 77
 industriespezifischer externer
 Prüfer 76
 interne Revision 76
 Nachweispflicht 79
 Objektivität 78
 professioneller Skeptizismus
 79
 steuerliche Außenprüfung 76
 Unabhängigkeit 78
 Prüferintervall 475
 Prüflleitfaden 131
 Prüfung 261, 320
 abgebrochene Verbuchung
 287
 Abschreibungsregel 338
 Abstimmkonto Geschäftspart-
 nerstammdaten 346
 AfA-relevanter Parameter in
 Anlagenklasse 334
 Änderungsbeleg 271
 Application Link Enabling
 (ALE) 288
 Arbeitnehmerdatenschutz
 422
 Batch-Input-Verarbeitung
 293
 Berechtigung für direktes Auf-
 rufen von Berichten 246
 Berechtigung zur Tabellen-
 pflege 255
 Berechtigungshauptschalter
 442
 Berechtigungsschutz eigenent-
 wickelter Programme 245
 Berichtigung des Vorratsver-
 mögens 379
 Betrugsaufdeckung beim Fäl-
 ligkeitsdatum 352
 Bewertung des Vorratsvermö-
 gens 374
 Buchungslogik und Kontenfin-
 dung 308
 CpD-Funktion und abwei-
 chende Bankdaten im Beleg
 351
 Daten anonymisieren 426
 datenschutzrelevante Daten in
 SAP ERP 427
 Debugging-Berechtigung 267
 Definition des sensiblen Feldes
 bei Stammdatenpflege 353
 doppelte Rechnungserfas-
 sung 366
 Einsatz der Belegvorerfas-
 sung 316
 Fakturavorrat 400
 Feld im Sachkontenstamm
 301
 Feldstatusgruppe 309
 Freigabe von Verschrottung
 380
 Freigabestrategie im Bestell-
 wesen 361
 Funktionstrennung im Haupt-
 buch 331
 Funktionstrennung/Entwick-
 lung/Berechtigungswesen
 260
 Grundsatz der zeitnahen
 Buchung 298
 GWG-Konfigurationskont-
 rolle 342
 Identität/Lebenszyklus der
 Benutzer 237
 Inhalt Infotyp 431
 Konsistenzcheck in AA 337
 Kontenfindung bei Material-
 bewegung 376
 Kontenfindung in AA 335
 Kontrolle beim SAP-Zahllauf
 349
 Kontrolle zur Rechnungsprü-
 fung 365
 Korrektur- und Transportwe-
 sen 228
 Kreditlimit im Vertrieb 392
 kritische Berechtigung in FI
 329
 kritische Bewegungsart 362
 Länderspezifikum 47
 lückenlose Belegnummernver-
 gabe 276
 Mahnprozess 404
 Mandanteneinstellung 230

- Nachvollziehbarkeit im Korrektur- und Transportwesen* 283
Notfallbenutzer 243
Organisation und Planung 82
Organisationsstruktur im Einkauf 357
Personalmaßnahme 434
Pflege 265
Pflege der Kundenstammdaten 390
Pflege des Währungskurses 314
Pflege Materialstammdaten 373
Preisermittlung bei Fakturierung 398
Produktkostenrechnung in P2P 382
Profilparameter 257
Protokollierung Infotyp 425
Protokollierung Reportaufruf 425
Remote Function Call (RFC) 291
sachliche Richtigkeit 415
SAP-Systemlandschaft 224
SAP-System-Log 278
Schutz der Stammdaten in FI 329
Schutz des Buchungskreises 323
Security Audit Log (SAL) 280
Statistikdatei 281
strukturelle Berechtigung 438
strukturelle Berechtigung – Kontextlösung 439
System-Trace eigenentwickelter Transaktionen 246
Tabellenprotokollierung 273
Toleranzgrenze 315
Umgang mit Dauerbuchung 319
Verarbeitung personenbezogener Daten 414
Verfahrens- und Systemdokumentation 222
Verkaufsdokument auf Tabellenebene 458
Vertriebsbeleg 387
Vollständigkeit Anlagengitter 340
Vorhandensein eines vorerfassten Belegs 317
Warenauslieferung 394
Wartung und Update 232
WE/RE-Konto ausziffern 369
Wert aus CO nach FI überleiten 320
Zweckbestimmung 414
Prüfungsansatz 67
Einzelfallprüfung 68
Systemprüfung 68
Prüfungsausschuss 51
Prüfungshandlung 68
Prüfungsrisiko 69
Entdeckungsrisiko 69
Fehlerrisiko 69
Prüfungsstandard 73, 120, 217
951 219
IDW PS 951 127
SAS 70 127
Public Company Accounting Reform and Investor Protection Act 45
Public Key Infrastructure (PKI) 127
Publizitätsgesetz (PublG) 66
- Q**

qualifizierter Lieferant 474
Qualitätssicherungssystem 223
Qualitätssicherungs-Tool 254
queued RFC 290
- R**

Rabatt 456
RAMS 156
Read-Debugging 448
Rechnungsprüfung 361
Rechnungsprüfung, Toleranzgrenze 364
Refresh 224
Reihengeschäft 396
Remote Function Call (RFC) 290
RFC-Anmeldeversuch 279
RFC-Benutzer 291
Remote-Zugriff 232
Reparatur 233
Reparaturkennzeichen 233
Reportauswertung 545
Repository Infosystem 186, 189
Retoure 383
Retourenabwicklung 400
Retourenbeleg 400
Revalidierung 480
Reversed Business Engineering (RBE) 280
RFC-Kommunikation
Art 290
asynchrone 290
Richtlinie
2006/43/EG 51
2006/46/EG 51
75/319/EWG 468
81/851/EWG 468
91/356/EWG 468
91/412/EWG 468
95/46/EG 410
Richtlinienverwaltung 145
Riscomp 673, 676
Automated-Monitoring-Szenarien 691
Automated-Monitoring-Szenarien 691
GRC Upload Tool 676
Risiko 69, 535
inhärentes 69
Kontrollrisiko 69
risikobasierte Validierung 471
risikobasiertes Scoping 584
Risikobewertung 544
Risikokategorie 544
Risikoregel 154
Risikoklasse 520
Risk Analysis and Remediation
 → Access Risk Management

- Risk Assessment 587
 - Risk IT 108
 - Risk Management 145, 534, 624
 - GRC340 160
 - Integration 147
 - Integration mit SAP Strategy Management 624
 - Operational Risk Management 147
 - Schulungen 160
 - Rolle 207
 - anpassen 615
 - Berechtigungsauswertung 207
 - Rollenverwaltung 261
 - Routine Transaction 306
 - RSECNOTE-Tool 152
 - Rücklieferung 398
 - Rückmeldung 381
 - Rückmeldung der Zählung 377
 - Rückstellung 403
- S**
-
- Sachkontenstammdaten 301
 - Sachkontenstammdaten ändern 303
 - Sachkonto 299
 - sachliche Richtigkeit 415
 - Safe-Harbor-Grundsatz 417
 - Saldenbestätigung 304
 - Sales & Distribution (SD) 385
 - SAP Access Control 133, 137, 153, 618
 - Content 153
 - Integration 618
 - Schulungen 160
 - SAP Audit Management 149
 - SAP Best Practice 161
 - SAP Business Workflow 359, 371
 - SAP Code Inspector 130
 - SAP Crystal Reports 554, 609
 - SAP GUI 244
 - SAP HANA 62
 - SAP Help Portal 123
 - SAP Process Control 134, 155, 473, 559, 672
 - Administration 556, 562
 - Aggregation von Mängeln 604
 - Analyseregeln 653
 - Änderungsbeleg 569
 - ASAP Roadmap 673
 - Automated Rules Framework (ARF) 680
 - BC-Set 672
 - Benachrichtigung 589
 - Benutzerauthentifizierung 611
 - Berechtigungsmodell 610, 614
 - Business Blueprint 674
 - Carryforward 606
 - Change Log Tool 658
 - Compliance-Initiative 574
 - Conference Room Pilot 674
 - Content 155
 - Continuous Monitoring Framework 155
 - Crystal Reports 609
 - Custom Field 571
 - Datenmodell 563, 565, 572, 575
 - Funktionsstrennungsintegration 649
 - GRC Integration Framework 641
 - GRC330 159
 - halb automatisierte Kontrolle 603
 - IKS-Stammdatenkonzept 565
 - Implementierung 672, 682
 - Implementierungsaufwand 679
 - Installation 558
 - Integration 147, 601
 - Integration mit Risk Management 147
 - Integration mit SAP Access Control 139, 618
 - kompensierende Kontrolle 620
 - Konfiguration 553, 555
 - Kontrollautomatisierung 152, 155
 - Kopie 579
 - Migration 558
 - Multiple Compliance Framework (MCF) 572
 - Object-related Security Concept 551
 - Objekt 560
 - objektbezogene Sicherheit 569, 610
 - Objekttyp 566
 - Offline-Formular 592
 - Offline-Test 592
 - Organisationshierarchie 559
 - Planungsfunktion 586
 - Projektaufwand 679
 - Referenz 579
 - Riscomp Automated Monitoring Scenarios 155
 - risikobasiertes Scoping 584
 - Rollenkonzept 614
 - Schulung 159
 - Schwachstelle 595
 - Scoping 582
 - Sign-off 605
 - Sizing 558
 - Stammdaten 559
 - Standardbericht 606
 - Standardkurs GRC330 559
 - technische Architektur 553
 - Upgrade 558
 - Vier-Augen-Prinzip 577, 599
 - vordefinierte Regel 155
 - wesentlichkeitsbasiertes Scoping 583
 - workflowbasierte Aktivität 587
 - Zeitabhängigkeit 560, 566
 - zentralisierte vs. dezentralisierte Dokumentation 577
 - SAP Quality Management 474
 - SAP Query 484, 495
 - Inner-Join 485
 - Outer-Join 485
 - SAP Query Painter 389
 - SAP Security Guide 123
 - SAP Service Marketplace 232
 - SAP Standard for Security 125
 - SAP-Betriebsaudit 82

- SAP-Hinweis 225
 112388 272
 1314345 659
 1320737 659
 1420281 265
 1916 272
 31875 303
 671016 118, 119
 77503 150
 863362 152
 888889 152
Tabellenprotokollierung 272
- SAP-Implementierungsaudit 81
- SAP-Middleware 244
- SAP-Schulung 159
- SAP-Systemlandschaft 222
- SAP-Verbuchungssystem 284
- Sarbanes-Oxley Act (SOX) 44, 45, 46
 China 48
 Euro-SOX 49
 Japan 46
 Kanada 46
 Scoping 46
 USA 45
- SAS 70 127
Bericht 218
Report 127
- Schutzmaßnahme
Auftragskontrolle 419
Eingabekontrolle 419
Kombinationsverbot 419
Verfügbarkeitskontrolle 419
Weitergabekontrolle 419
Zugangskontrolle 418
Zugriffskontrolle 418
Zutrittskontrolle 418
- Schweiz 52
 Art. 716a Ziff. 3 OR 52
 Art. 728a Ziff. 1 OR 53
 Obligationsrecht 52
 Prüfungsstandard PS 890 53
 SOX Light 52
- Schweizerisches Heilmittel Institut (SHI) 467
- Scoping 46, 540, 582
- Second-Level-Berechtigung 613
- Secure Area 232
- Secure Operations Map 125
- Securities and Exchange Commission 45
- Security 122
- Security Audit Log (SAL) 279, 427
- Security Notes 124
- Security Optimization Service (SOS) 131, 152
- Security-Audit 81
- Segregation of Duties 138
- Segregation of Duties Review 141, 142
- Segregation of Duties Risk 619
- Selbstpflege 428
- Self Assessment 587
- sensibles Feld 353
- sensitive Daten 411
Datenschutz 411
erheben 421
- Service Desk 234
- Service Level Agreement (SLA) 218
- Service Pack 232
- Serviceunternehmen 216
- Serviceverbindung 230
- Shared Service 216, 580
- Shared-Services-Organisation 531
- Shelf Life Expiration Date 478
- Sicherheitsleitfaden 125
- Sicherheitsstandard 238
- Sicherheitszertifikat 121
- Significant Deficiency 604
- Sign-off 545, 605
- Single Sign-on (SSO) 235, 611
- Sizing 558
- Skilldatenbank 421
- Skonto 44
- Skript 647
- SoD → Segregation of Duties
- Software Deployment Manager (SDM) 130
- Softwareaktualität 231
- Softwareauswahl 82
- Softwarebescheinigung 118
- Softwarezertifizierung 74, 117
Kriterium 118
sicherheitsbezogene 121
- Solution Manager 130, 157, 162, 226, 233, 480
Business Process Repository 163
Data Consistency Cockpit 159
Monitoring 159
- Solution Monitoring 234
- Solvency II 57
- Sonderbeschaffungsart 504
- Sonderperiode 296
- SOX-Compliance automatisieren 528
- SOX-Compliance-Prozess 529
- Sozialgesetzbuch (SGB) 409
- Spanien 56
Good Governance 56
Good Governance of Listed Companies 56
Securities Markets Commission 56
- Sparte 196
- Sperre
betragmäßige 365
stochastische 365
- Sperrgrund 364
- SPM → Superuser Privilege Management
- SQL-Injection 252
- SQL-Trace 427
- Stammdaten 172, 326
A-Segment 172
Berechtigungsobjekt 327
B-Segment 173
Schutz 325
Vier-Augen-Prinzip 353
- Stammdatenpflege 390
- Stammdatenqualität 499
- Standard Operation Procedures (SOP) 475
- Standardbenutzer 240
 DDIC 240
 EARLYWATCH 240
 SAP* 240, 241
 SAPCPIC 240
 TMSADM 240
 WF_BATCH 240
- Standardgeschäftsprozess 161
- Standardpreis 377
- Statistikdatei 280
- Steuer 309

Steuerkennzeichen 310
 Steuerprüfung 81
 Steuerungsdaten 271
 Strategie- und Performancemanagement 622
 Strategy Management 624
 strukturelle Berechtigung 435, 436
 strukturelles Berechtigungsprofil 436, 439
 Stückliste 502
 Substitutionsregel 311
 Subtyp 430
 Suche, SAP 195
 Superuser Privilege Management (SPM) 144
 Support 230
 Support Package 231
 synchroner RFC 290
 Systemadministration 129
 Systemkopie 425
 Systemlandschaft 232
 System-Log 266, 277
 Systemprüfung 67
 Systemprüfung, Outsourcing 74
 System-Trace 203, 246

T

Tabelle 170
 &SAP_EDIT 265
 Änderung 265
 Änderungsbeleg 265
 Anzahl 170
 Berechtigungsgruppe 256
 CDHDR 491, 494
 CDPOS 491, 494
 Data-Dictionary-Tabelle 181
 Debugging-Aktivität 265
 direkte Pflege 255
 EBAN 489, 510
 EKES 514
 EKET 495, 513
 EKKN 514
 EKKO 485, 512
 EKPO 485, 513
 Infotyp 431
 KNA1 500

KNB1 500
 KNVV 500
 LFA1 485
 logische Datenbank 185
 MARC 495, 502, 519
 MAST 502
 MBEW 505
 MKPF 485
 MSEG 485, 505
 Pflege 259
 Protokollierung 193, 271, 272
 Protokollierungsumfang 271
 SAP 170
 Schutz 255, 256
 Schutz der Daten 264
 Stichwortsuche 185
 Suche 180, 183
 Tabellenhandbuch 178
 Tabellensuche über Feld 183
 Umschlüsselungstabelle 193
 VBAK 516
 VBAP 517
 VBEP 517
 VBRK 457
 Verknüpfung 187
 Verwendungsnachweis 193, 195
 Vorteil aus Revisionssicht 171
 Test of Control Effectiveness 587
 Testmanagement 234
 Testplan 591
 Therapeutic Goods Administration (TGA) 466
 Toleranzgruppe 324, 368
 Transaktion 187
 AFAMA (Abschreibungs-schlüssel pflegen) 338
 AW01N (Asset Explorer) 332
 Basisberechtigung 259
 BD87 (Statusmonitor für ALE-Nachrichten) 288
 BDM2 (IDoc-Verfolgung) 289
 Benutzermenü 189
 CK24 (Preisfortschreibung mit Kalkulation) 661

CK40N (Kalkulationslauf bearbeiten) 661
 CKME (Aktivierung geplanter Preise) 661
 CKMLPC (Preisänderung) 661
 CKMPCD (Anzeige der Preisänderungsbelege) 379
 Einkaufsprozess 187
 F.15 (Dauerbuchungen listen) 318
 F.80 (Massenstorno) 329
 F110 (Parameter für maschinelle Zahlung) 347
 F-43 (Erfassung Kreditorenrechnung) 384
 FB04 (Belegänderungen) 269
 FB41 (Buchen von Steuer und Zahllast) 293
 FB60 (Erfassung eingehender Rechnungen) 200, 204, 206, 256, 326, 384
 FBKP (Konfiguration Buchhaltung pflegen) 307, 369
 FBL3N (Kreditoren) 405
 FBL5N (Debitoren) 405
 FD24 (Kreditlimitänderungen) 393
 FD32 (Debitor – Kreditmanagement ändern) 391
 FIBLAPOP 347
 FK02 (Kreditorenstammdaten ändern) 535
 FP22 (Massenstorno) 329
 FPVC (Massenstorno von Mahnungen) 329
 FS00 (Zuordnung zu einer Toleranzgruppe) 369
 FTXP (Steuerkennzeichen pflegen) 311
 GGB0 (Validierungsbearbeitung) 312
 GRFN_STR_CHANGE (Administration Process Control) 562, 568
 GRFN_STR_CREATE (Administration) 556
 GRFN_STR_DISPLAY (Anzeige Process Control) 562

- IDOC (Reparatur- und Prüfprogramme für IDocs und EDI) 289
 KALC (Meldung der Kostenflüsse) 319
 Kurzbeschreibung 188
 MASS (Massenänderungen) 329
 MB51 505
 MB51 (Materialbelegliste) 362, 380
 MC42 518
 MC43 518
 MC44 518
 MC46 518
 MIRO (Logistik Rechnungsprüfung) 535
 MR11 (Manuelle Pflege des WE/RE-Kontos) 367
 MR21 (Preisänderung) 661
 MRBR (Gesperrte Rechnungen freigeben) 364
 MRNO (Marktpreise) 379
 MRN2 (Gängigkeit) 379
 MRN3 (Verlustfreie Bewertung) 379
 MRN9 (Anwendungs-Log) 379
 OA79 (Pflege des Anlagengitters) 340
 OAAK und OAAQ (Jahresabschlussaktivitäten zurücknehmen) 344
 OABK (Anlagenklassen löschen) 344
 OABL (Buchungskreis zurücksetzen) 322, 329, 344
 OAMK (Konfiguration der Abstimmkonten pro Buchungskreis) 345
 OAY2 (Anlagenklasse GWG-Wertprüfung) 341
 OAYK (Geringwertige Wirtschaftsgüter) 341
 OAYR (Buchungsregeln Abschreibungen) 338
 OAYZ (Anlagenklassen) 333
 OB_GLACC11, OB_GLACC12 und OB_GLACC13 (Massenpflege Sachkonten) 329
 OB29 (Geschäftsjahresvarianten) 298
 OB32 (Pflege der Belegänderungsregeln) 268
 OBC4 (Pflege Tabelle T004V) 309
 OBL6 (Konsistenzprüfung Mahnverfahren) 403, 405
 OMJJ (Customizing neue Bewegungsarten) 362, 393
 OMR3 (MM-IV Vorschlag Kontenpflege) 369
 OMW0 (MM-IV Steuerung Bewertung) 375
 OMWB (Simulation der Kontenfindung) 376
 OMWC (MM-IV Getrennte Materialbewertung) 375
 OOAC (HR-Berechtigungs-hauptschalter) 438, 442
 OOSB (Benutzerberechtigungen ändern) 437
 OOSP (Berechtigungsprofil ändern) 437
 OVX3 502
 PA30 (Personalstammdaten) 432
 PA40 (Pflege über Personalmaßnahmen) 432
 PFCG (Profilgenerator) 261, 357, 435
 S_AHR_61016380 (Protokollierte Änderungen) 435
 S_ALR_87003642 (Pflege der Buchungsperioden) 329
 S_ALR_87012180 (Adressliste Debitoren) 389
 SA38 (ABAP-Programmausführung) 190
 SA38 (ABAP-Reporting) 239, 246
 SCC4 (Mandantenverwaltung) 228
 SDD1 (Doppelte Verkaufsbelege im Zeitraum) 387
 SE01 (Transport Organizer) 225
 SE11 (ABAP-Dictionary-Pflege) 194, 255
 SE14 (Verwaltung der Änderungsbelege) 265
 SE16 (Data Browser) 181, 188, 230, 396, 404, 631
 SE16N (Data Browser) 264
 SE38 (ABAP Editor) 190, 247
 SE84 (Repository Infosystem) 182, 188, 247
 SM13 (Monitor Verbuchungen) 286
 SM14 (Verbuchungsadministration) 286
 SM20 (Auswertung des Security Audit Logs) 280
 SM21 (Onlineauswertung des System-Logs) 277
 SM30 (Tabellenpflege) 255, 313, 314
 SM35 (Batch-Input) 294
 SM58 290
 SM59 (Pflege der RFC-Destinationen) 290, 291
 SMQ2 (Monitoreingang) 290
 SPAM (Support Package Manager) 231
 SPAU (Modifikationsabgleich) 233
 SQ01 484
 SQVI 484
 STMS (Transport Management System) 223
 SU01 (Benutzerpflege) 241, 260, 435, 610
 SU10 (Massenpflege der Benutzer) 260
 SU24 (Berechtigungsobjektprüfung unter Transaktionen) 256
 SU53 (Auswertung der eigenen Berechtigungsprüfung) 258
 Suche 187
 SUIM (Benutzerinformationssystem) 202, 207, 237, 357
 technischen Namen anzeigen 189
 V.02 (Liste unvollständige Aufträge) 387

- V.03 (*Liste unvollständiger Anfragen*) 163
 V.15 (*Anzeigen rückständige Aufträge*) 388
 VA11 (*Anfrage anlegen*) 163
 VA12 (*Anfrage ändern*) 163
 VA13 (*Anfrage anzeigen*) 163
 VA15 (*Liste anfragen*) 163
 VBKD 517
 VCHECKT683 (*Customizing-Check Kalkulations-schema*) 396
 VF03 (*Anzeigen Faktura*) 401
 VKM1 (*Anzeige gesperrter Vertriebsbelege*) 388
 VKM2 (*Anzeige entsperrter Vertriebsbelege*) 388
 VOV8 (*Pflege der Belegarten*) 394, 400
 WE05 (*IDoc-Liste*) 288
 XK99 (*Massenpflege*) 329
 transaktionaler RFC 290
 Transaktionsaufruf
 Historie 280, 427
 Transport Management System (TMS) 223, 224
 Transportauftrag 224, 260, 282
 Bezeichnung 226
 Freigabe 226
 Funktionstrennung 227
 Genehmigungsverfahren 226
 Import 226
 Transportweg 227
 trusted System 291
- U**
-
- UAM → User Access Management
 UAR → User Access Review
 UME → User Management Engine
 Umfrage 543
 Umlagerung 504
- Umrechnungskurs 312, 313
 mengennotierter 313
 preisnotierter 313
 Verschlüsselungslogik 314
 Umsatzprobe 302
 Umsatzsteuer 396
 Umsatzsteuerermittlung 395
 Umsatzsteuervoranmeldung 309
 Umsetzungsmatrix 551
 unbewertetes Material 383
 Universum 668
 Unkenntlichmachung von Daten 425
 Unmanaged SQL 252
 USA
 Paragraf 1107 46
 Paragraf 404 45
 Paragraf 802 46
 PCAOB-Standard 45
 Securities and Exchange Commission 45
 Standard AS 5 45
 US-Department of Commerce 417
 User Access Management (UAM) 133, 140
 User Access Review (UAR) 141
 User Management Engine (UME) 611
- V**
-
- V1-Vorgang 285
 V2-Vorgang 285
 Val IT 109
 Validierung 311
 verantwortliche Stelle 412, 421
 Verbindlichkeit 536
 Verbuchungsabbruch 276, 277, 284
 Verbuchungsadministration 259
 Verbuchungssystem 284
 Verfügbarkeitskontrolle 419
 Verkäufergruppe 196
 Verkaufsauftrag 497
- Verkaufsbeleg 497, 515
 Verkaufsbüro 196
 Verkaufsorganisation 196
 Verkaufspreisermittlung 396, 397
 Vermögensunterschlagung 444
 Versagungsvermerk 65
 Verschrottung freigeben 379
 Vertriebsauftrag 386
 Vertriebsbeleg 386
 Vertriebsbereich 196
 Vertriebsphase, vorbereitende 386
 Vertriebsprozess 385
 Vertriebsweg 196
 Verwendungsnachweis 193, 195
 Vier-Augen-Prinzip 315
 Bestellwesen 358
 IKS-Aktion 599
 Kontrolldokumentation 577
 Pflege IKS-Framework 576
 Stammdatenpflege 353
 vertrauliche Daten 462
 Virtual Forge CodeProfiler 254
 V-Modell 471
 vorbereitende Vertriebsphase 386
 vorerfasster Beleg 304
 vorkonfigurierter Workflow 672
 Vorratsvermögen 376
 Vorsteuerkennzeichen 309
- W**
-
- Warehouse Management 478
 Warenauslieferung 393
 Wareneingang 361
 kritische Bewegungsart 361
 ohne Bestellung 361
 Wareneingangsdatum 483
 Wartung 232
 WE/RE-Konto 366
 Ausweis am Monatsende 370
 ausziffern 367

- WE/RE-Verrechnungskonto 367
Web Dynpro 259
Webbrowser 244
Weitergabekontrolle 419
Werk 196
Werthaltigkeit von Forderung 403
wesentlichkeitsbasiertes Scoping 583
Whitepaper 125
Wiederanlaufverfahren 221
- Wirtschaftsprüfung 66
Work in Progress (WIP) 306
workflowbasierte Aktivität 587
Write-Debugging 449
- Z**
-
- Zahllauf 347, 348
Zahlung in SAP 347
Zahlungsbedingung 502, 520
- Zahlungsfristenbasisdatum 176, 352
Zahlungskondition 518
Zahlungsvorschlagsliste 348
Zertifizierung 218
Zugangskontrolle 418
Zugriffsfolge 397
Zugriffskontrolle 418
Zuordnungsnummer 368
Zutrittskontrolle 418
Zweckbestimmung 414, 422
Zweckbindung 420