

Auf einen Blick

TEIL I Vom Paragrafen zum Konzept:

IKS und Compliance im ERP-Umfeld

1	Gesetzliche Anforderungen im Bereich IKS-Compliance	37
2	Der Prüfer kommt: Wann, warum und wie man damit umgeht	57
3	IKS-Anforderungen und ERP-Systeme: Grundsätze, Frameworks, Struktur	79
4	Wie geht SAP mit dem Thema Compliance um?	105

TEIL II Vom Konzept zum Inhalt:

Revisionsleitfaden für SAP ERP

5	Revisionsrelevante SAP-Basics	149
6	Generelle IT-Kontrollen in SAP ERP	193
7	Übergreifende Applikationskontrollen in SAP ERP	233
8	Kontrollen in der Finanzbuchhaltung	265
9	Kontrollmechanismen im SAP ERP-gestützten Procure-to-Pay-Prozess	325
10	Kontrollmechanismen im SAP ERP-gestützten Order-to-Cash-Prozess	355
11	Datenschutz-Compliance in SAP ERP Human Capital Management	377
12	Betrug im SAP-System	415
13	Exkurs: FDA-Compliance und Kontrollen in SAP	437

TEIL III Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsyste

14	IKS-Automatisierung: Wie bringt man den COSO-Cube ins Rollen?	457
15	IKS-Automatisierung mithilfe von SAP BusinessObjects Process Control	479
16	Umsetzung von automatisierten Test- und Monitoring-Szenarien im SAP ERP-Umfeld	559
17	Praxis- und Projekterfahrungen	603

Inhalt

Vorwort	21
Vertrauen ist gut, Kontrolle ist billiger: Einleitung	23

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

1.1 Begriffsdefinitionen und Abgrenzung	37
1.1.1 Der Begriff »Compliance«	37
1.1.2 Der Begriff »Internes Kontrollsysterm« (IKS)	39
1.2 Gesetzliche IKS-Anforderungen in Übersee – die vielen Gesichter von SOX	40
1.2.1 SOX in USA	40
1.2.2 SOX in Kanada (NI 52-109)	42
1.2.3 SOX in Japan	42
1.2.4 SOX in China	43
1.3 IKS-Anforderungen in Europa	44
1.3.1 Die 8. EU-Richtlinie	44
1.3.2 Deutschland	45
1.3.3 Schweiz	47
1.3.4 Österreich	48
1.3.5 Vereinigtes Königreich Großbritannien und Nordirland	49
1.3.6 Frankreich	49
1.3.7 Dänemark	50
1.3.8 Italien	50
1.3.9 Spanien	51
1.4 IKS-Anforderungen in der Finanzbranche	52
1.4.1 Solvency II im Versicherungswesen	52
1.4.2 Basel II im Bankwesen	53
1.5 Resümee	55

2.1	IKS im IT-Umfeld aus der Sicht der Wirtschaftsprüfung	58
2.1.1	Herausforderung durch die Informationstechnologie	59
2.1.2	Systemprüfung als Prüfungsansatz im IT-Umfeld	59
2.1.3	Ansätze bei der Systemprüfung: IKS im Fokus	61
2.1.4	IKS und die Systemprüfung als Pflicht	63
2.2	IKS-Assurance in der Praxis	67
2.2.1	Ausrichtungen der Prüfer	67
2.2.2	Ausgewählte Prüfungsgrundsätze	69
2.2.3	Arten der externen Prüfung im ERP-Umfeld	72
2.2.4	Empfehlungen zum Umgang mit dem Prüfer	75
2.3	Resümee	78
3.1	IKS-Inhalte im SAP ERP-Umfeld definieren	79
3.1.1	IKS-Grundsätze im ERP-Umfeld: Von GoB zu GoBS	80
3.1.2	Wer definiert die Spielregeln im SAP-Umfeld?	82
3.1.3	Kontroll-Identifizierungsprozess	83
3.1.4	Struktur des IKS-Frameworks im SAP-Umfeld	86
3.2	IKS-relevante Referenzmodelle und Standards	91
3.2.1	COSO	92
3.2.2	CobiT	93
3.2.3	ITIL	94
3.2.4	GAIT	95
3.2.5	ITAF	95
3.2.6	Risk IT	96
3.2.7	VAL IT	97

3.2.8	CMMI	99
3.2.9	MOF	100
3.2.10	ISO 27k	100
3.2.11	PCI-DSS	101
3.2.12	Zusammenfassende Sicht auf Referenzmodelle	102
3.3	Resümee	103
4.1	Softwarezertifizierung	105
4.1.1	SAP-Hinweis 671016	106
4.1.2	Zertifizierungsberichte	107
4.2	Compliance-relevante Leitfäden	110
4.2.1	SAP-Onlineressourcen	110
4.2.2	Sicherheitsleitfäden	113
4.2.3	DSAG-Leitfäden: Prüfleitfaden, Datenschutzleitfaden	119
4.3	Compliance-relevante Produkte	120
4.3.1	SAP BusinessObjects Access Control	122
4.3.2	SAP BusinessObjects Process Control	129
4.3.3	SAP BusinessObjects Risk Management	130
4.3.4	SAP Audit Management	131
4.3.5	SAP Audit Informationssystem	133
4.3.6	SAP Security Optimization Service	134
4.3.7	RSECNOTE-Tool	135
4.4	Compliance-relevanter Content	135
4.4.1	Direkter IKS-Content: Welche Kontrollen gibt es in SAP?	136
4.4.2	Content mit der IKS-Relevanz: Standard- geschäftsprozesse und -werteflüsse in SAP	141
4.5	Resümee	145

Teil II Vom Konzept zum Inhalt: Revisionsleitfaden für SAP ERP

5.1	Am Anfang war die Tabelle: SAP als tabellengesteuerte Applikation	150
-----	--	-----

5.1.1	Daten im SAP-System	152
5.1.2	Kontrollen im SAP-System	158
5.1.3	Tabellenbezogene Suche	160
5.1.4	Transaktionsbezogene Suche	166
5.1.5	Programmbezogene Suche	168
5.1.6	Beziehung zwischen Programmen und Transaktionen	169
5.1.7	Beziehung zwischen Programmen und Tabellen	171
5.1.8	Zusammenfassung der Suchmöglichkeiten in SAP	174
5.1.9	Organisationsstrukturen im SAP-System	174
5.2	Berechtigungen	176
5.2.1	Ablauf und Hierarchie der Berechtigungs- kontrollen	177
5.2.2	Berechtigungsobjekte	178
5.2.3	Ermittlung der Berechtigungsobjekte	181
5.2.4	Rollen im SAP-System	185
5.2.5	Benutzer im SAP-System	187
5.2.6	Benutzertypen in SAP	188
5.2.7	Beispiel für eine Berechtigungs- auswertung	189
5.3	Resümee	191
6.1	Organisatorische Kontrollen	193
6.1.1	IT-Organisation	194
6.1.2	IT-Outsourcing: Wer ist verantwortlich für die Kontrollen?	195
6.1.3	Richtlinien und Dokumentation	198
6.2	Kontrollen im Bereich Change Management und Entwicklung	200
6.2.1	SAP-Systemlandschaft	200
6.2.2	Korrektur und Transportwesen	202
6.2.3	Mandantensteuerung	206
6.2.4	Wartung und Updates	208
6.2.5	SAP Solution Manager	211
6.3	Sicherheitskontrollen beim Zugriff auf das SAP-System und der Authentifizierung	212
6.3.1	Identität und Lifecycle der Benutzer	213

6.3.2	Passwortschutz	215
6.3.3	Behandlung der Standard-User	217
6.3.4	Notfallbenutzerkonzept	219
6.4	Sicherheits- und Berechtigungskontrollen	
	innerhalb von SAP ERP	220
6.4.1	Schutz der Programme und Transaktionen	221
6.4.2	Schutz der Tabellen	225
6.4.3	Kontrollen in Steuerung der Berechtigungsprüfungen	226
6.4.4	Kritische Administrationstransaktionen	229
6.4.5	Berücksichtigung der Funktionstrennungsgrundsätze	230
6.5	Resümee	232
7.1	Der Grundsatz der Unveränderlichkeit	234
7.1.1	Schutz der Daten in Tabellen	234
7.1.2	Debugging	235
7.1.3	Änderbarkeit der Belege	237
7.2	Kontrollen für die datenbezogene Nachvollziehbarkeit	239
7.2.1	Änderungsbelege in SAP	239
7.2.2	Tabellenprotokollierung	241
7.2.3	Belegnummernvergabe	244
7.3	Nachvollziehbarkeit der Benutzeraktivitäten in SAP	246
7.3.1	Systemlog	246
7.3.2	Security Audit Log	248
7.3.3	Historie der Transaktionsaufrufe	250
7.3.4	Nachvollziehbarkeit der Systemänderungen im KTW	251
7.4	Prozessübergreifende Verarbeitungskontrollen	253
7.4.1	Überwachung der Verbuchungsabbrüche ...	254
7.4.2	Vollständigkeit der ALE- Schnittstellenverarbeitung	257
7.4.3	Remote-Function-Call-Verbindungen	259
7.4.4	Vollständigkeit der Batch-Input- Verarbeitung	261
7.5	Resümee	264

8.1	Grundlegende Kontrollmechanismen im Hauptbuch	266
8.1.1	Grundsatz: Zeitnähe der Buchungen	266
8.1.2	Bilanz	269
8.1.3	Sachkontenstammdaten	270
8.1.4	Konsistenzcheck der Verkehrszahlen mit der großen Umsatzprobe	272
8.1.5	Ausgewählte Kontrollen bei Abschlussarbeiten	273
8.1.6	Abstimmarbeiten im Hauptbuch	274
8.2	Kontrollen über die Richtigkeit und Qualität der Daten im Hauptbuch	276
8.2.1	Richtigkeit der Kontenfindung	276
8.2.2	Feldstatusgruppen	278
8.2.3	Berechnung von Steuern bei manuellen Buchungen	279
8.2.4	Validierungen in SAP	280
8.2.5	Fremdwährungen	282
8.3	Vollständigkeit der Verarbeitung im Hauptbuch	284
8.3.1	Belegvorerfassung	285
8.3.2	Dauerbuchungen	287
8.3.3	Abstimmledger	288
8.4	Sicherheit und Schutz der Daten im Hauptbuch	290
8.4.1	Schutz der Buchungskreise	290
8.4.2	Toleranzgruppen	293
8.4.3	Schutz der Stammdaten	295
8.4.4	Kritische Transaktionen	298
8.4.5	Funktionstrennung im Hauptbuch	299
8.5	Kontrollen in der Anlagenbuchhaltung	300
8.5.1	Grundlagen der Anlagenbuchhaltung in SAP	301
8.5.2	Default-Werte bei Anlagenklassen	302
8.5.3	Kontenfindung in der Anlagenbuchhaltung	303
8.5.4	Konsistenzprüfung der Kontenfindung und der Konfiguration	305
8.5.5	Abschreibungen	306
8.5.6	Anlagengitter	309
8.5.7	Geringwertige Wirtschaftsgüter	310

8.5.8	Berechtigungssteuerung in der Anlagenbuchhaltung	311
8.5.9	Kritische Berechtigungen in der Anlagenbuchhaltung	313
8.6	Kontrollen in der Kreditoren- und Debitoren- buchhaltung	314
8.6.1	Richtigkeit der Abstimmkonten	315
8.6.2	Zahlungsfunktionen	316
8.6.3	Einmalkunden und -Lieferanten – Vorsicht!	319
8.6.4	Altersstruktur und Wertberichtigungen	321
8.6.5	Vier-Augen-Prinzip bei der Stammdatenpflege	322
8.7	Resümee	323
9.1	Bestellwesen	327
9.1.1	Berechtigungskonsistente Pflege der Organisationsstrukturen	327
9.1.2	Vier-Augen-Prinzip im Bestellwesen	328
9.2	Wareneingänge und Rechnungsprüfung	331
9.2.1	Wareneingänge: Kritische Bewegungsarten	331
9.2.2	3-Way-Match und Zahlungssperren bei der Logistik-Rechnungsprüfung	333
9.2.3	Prüfung auf doppelte Rechnungserfassung	336
9.3	WE/RE-Konto	336
9.3.1	Auszifferung des WE/RE-Kontos	337
9.3.2	Abschlussarbeiten und Ausweis des WE/RE-Kontos in der Bilanz	339
9.4	Kontrollen rund um das Thema Bestände	341
9.4.1	Pflege von Materialstammdaten	341
9.4.2	Unbewertetes Vorratsvermögen und getrennte Bewertung	343
9.4.3	Kontenfindung bei Materialbewegungen ...	345
9.4.4	Berichtigung des Vorratsvermögens: Inventur und Materialabwertungen	347
9.4.5	Freigabe von Verschrottungen	349

9.4.6	Produktkostenrechnung	350
9.4.7	Ausgänge von unbewertetem Bestand	353
9.5	Corporate Governance	353
9.6	Resümee	354
10.1	Kontrollen in der vorbereitenden Vertriebsphase	356
10.1.1	Kontrollen bei der Auftragserfassung	356
10.1.2	Qualität der Kundenstammdaten	358
10.1.3	Funktionstrennung bei der Stammdatenpflege	360
10.1.4	Kreditlimitvergabe und -kontrolle	361
10.2	Kontrollen bei der Auftragserfüllung und Umsatzlegung	363
10.2.1	Kontrollen rund um die Warenauslieferung	363
10.2.2	Preisfindung und Umsatzsteuerermittlung ..	364
10.2.3	Rücklieferungen und Gutschriften	368
10.2.4	Fakturavorrat	369
10.2.5	Vollständigkeit der buchhalterischen Erfassung von Fakturen	370
10.2.6	Mahnwesen	372
10.3	Resümee	375
11.1	Gesetzliche Datenschutzanforderungen	378
11.1.1	Datenschutz	378
11.1.2	Grundlagen: Richtlinie der Europäischen Union	380
11.1.3	Mitbestimmung und Arbeitnehmer- datenschutz	389
11.2	Datenschutzrelevante übergreifende Kontroll- mechanismen in SAP	392
11.2.1	Änderungen von personenbezogenen Daten nachvollziehen	393
11.2.2	Protokollierung der Reportaufrufe in SAP ERP HCM	395

11.2.3	Daten löschen und unkenntlich machen	396
11.2.4	Personenbezogene Daten außerhalb von SAP ERP HCM	397
11.3	Besondere Anforderungen an SAP ERP HCM	398
11.4	Berechtigungen und Rollen in SAP ERP HCM	399
11.4.1	Differenzierende Attribute in SAP ERP HCM	400
11.4.2	Personalmaßnahmen	402
11.4.3	Strukturelle Berechtigungen	405
11.4.4	Berechtigungshauptschalter	410
11.5	Resümee	413
12.1	Einführung in das Thema »Betrug«	415
12.1.1	Betrugsarten	416
12.1.2	Betrag und das SAP-System	418
12.2	Betragsszenarien in der SAP-Basis	420
12.2.1	»Write-Debugging«-Berechtigungen	420
12.2.2	Abspielen einer Batch-Input-Mappe unter einem anderen Benutzernamen	421
12.3	Betragsszenarien im Hauptbuch	422
12.3.1	Betrügerische manuelle Belegbuchungen im Hauptbuch	423
12.3.2	Identifizierung und Analyse von manuellen Journaleinträgen	424
12.4	Betragsszenarien im Vertriebsbereich	426
12.4.1	Fiktive Rechnungen an fiktive Kunden stellen	426
12.4.2	Gewährung nicht ordnungsgemäßer Gutschriften oder Boni	428
12.4.3	Übermäßiger Einsatz von Gratiswaren	429
12.4.4	Nicht ordnungsgemäße Abschreibung offener Kundenforderungen	431
12.5	Betragszenarien in der Personalbuchhaltung	431
12.5.1	Fiktive Angestellte	432
12.5.2	Limitierter Zugang zu eigenen HR-Daten	433
12.5.3	Vier-Augen-Prinzip bei vertraulichen Daten	434
12.6	Resümee	435

13.1	Gesetzliche Anforderungen im Bereich Arznei- und Lebensmittelherstellung	437
13.1.1	FDA-relevante gesetzliche Anforderungen im internationalen Vergleich	438
13.1.2	GxP – die FDA-Grundsätze	439
13.1.3	IT aus der Sicht von FDA-Compliance	441
13.2	Validierung der IT-Systeme	442
13.2.1	Vorgehensweise bei der Validierung	442
13.2.2	Kontrollen in Implementierungsprozessen ..	445
13.3	FDA-Compliance in IT-gestützten Geschäfts- prozessen	446
13.3.1	Beispiele: Kontrollen in der Beschaffung	446
13.3.2	Beispiele: Kontrollen im Produktionsmanagement	447
13.3.3	Beispiele: Kontrollen im Qualitäts- management	447
13.3.4	Beispiele: Kontrollen in der Instandhaltung	448
13.3.5	Beispiele: Kontrollen zur Chargenrückverfolgbarkeit	449
13.3.6	Beispiele: Kontrollen in Lagerverwaltungsprozessen	450
13.4	FDA-Compliance bei Systempflege, -aktualisierung und -änderung aufrechterhalten	451
13.5	Resümee	452

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

14.1	Grundidee der IKS-Automatisierung	457
14.1.1	Der COSO-Cube in Aktion	458
14.1.2	Idee der IKS-Automatisierung	459
14.2	IKS-relevante Objekte und Dokumentation	462
14.2.1	Organisationseinheiten	462
14.2.2	Prozesse	463

14.2.3	Kontrollen	464
14.2.4	Kontrollziele	466
14.2.5	Risiken	467
14.2.6	Kontengruppen	467
14.2.7	Beispiel eines IKS-Datenmodells	469
14.3	Grundszenarien der IKS-Aktivitäten	470
14.3.1	Dokumentation	471
14.3.2	Selektion und Priorisierung von Kontrollaktivitäten	471
14.3.3	Kontrolldurchführung	472
14.3.4	Designtest	473
14.3.5	Effektivitätstest	473
14.3.6	Umfrage	475
14.3.7	Risikobewertung	475
14.3.8	Behebung	476
14.3.9	Sign-Off	476
14.3.10	Reportauswertung	477
14.3.11	Personen als Bindeglied zwischen IKS-Objekten und Aktionen	477
14.4	Resümee	478

15.1	Einleitung: IKS-Umsetzung mit SAP BusinessObjects Process Control	480
15.2	Technischer Implementierungsteil	482
15.2.1	Technische Architektur und Installation	483
15.2.2	Initiale Konfiguration der Standardfunktionen	484
15.2.3	Informationsquellen zu Implementierung, Betrieb und Upgrade von Process Control ..	487
15.3	Datenmodell	488
15.3.1	IKS-Stammdaten in Process Control	489
15.3.2	IKS-Datenmodell in Process Control	492
15.3.3	Zentrale vs. lokale IKS-Stammdaten	494
15.3.4	Zeitabhängigkeit der IKS-Stammdaten	496
15.3.5	Nachvollziehbarkeit der Änderungen	497
15.3.6	Konzept der objektbezogenen Sicherheit ...	498
15.3.7	Kundeneigene Felder	500
15.3.8	Multiple-Compliance-Framework-Konzept	502

15.4	Implementierung des IKS-Prozesses	504
15.4.1	IKS-Dokumentationsprozess	505
15.4.2	Scoping-Prozess	512
15.4.3	Planungsprozess, Tests und Bewertungen ...	516
15.4.4	Problembehebungsprozess	526
15.4.5	Reporting	537
15.5	IKS- und Compliance-Umsetzung: Rollen	540
15.5.1	Berechtigungsmodell in Process Control	541
15.5.2	Objektbezogene Sicherheit in Aktion	543
15.5.3	First-Level- vs. Second-Level-Berechtigungen	544
15.5.4	Vordefiniertes Best-Practice-Rollenkonzept in SAP	545
15.5.5	Anpassung der Rollen	546
15.6	SAP BusinessObjects Process Control als GRC-Bestandteil	548
15.6.1	Policy Management und sonstige Neuheiten in Release 10.	548
15.6.2	Integration mit Access Control	550
15.6.3	Integration mit Risk Management	552
15.6.4	Zusammenführung von GRC-, Strategie- und Performance-Themen	555
15.7	Resümee	558
16.1	Automatisierte Test- und Überwachungsszenarien im SAP-Umfeld	559
16.1.1	Offline-CAAT-Tools	560
16.1.2	Online-CAAT-Berichte und -Auswertungen	565
16.1.3	Compliance Management Software	567
16.2	Automatisiertes Testen und Monitoring	568
16.2.1	Automated Rules Framework	568
16.2.2	Anbindung	578
16.2.3	Kontrollen	582
16.2.4	Kontrollautomatisierung: Beispiele	586
16.2.5	... Und los geht's!	597
16.3	Ausblick auf künftige ARF-Szenarien in Process Control	598

16.3.1	Release-Unterschiede 3.0 vs. 10.	598
16.3.2	Überlegung zum Thema SAP BusinessObjects	599
16.4	Resümee	602
17.1	Praxiserfahrungen: Projekte zur IKS- und Compliance-Automatisierung	603
17.1.1	Hilfsmittel bei der Implementierung	603
17.1.2	Best-Practice-Projektaufbau bei der IKS-Umsetzung	605
17.1.3	Business Blueprint	606
17.1.4	IKS-Content	609
17.1.5	Einflussfaktoren auf den Projektaufwand	611
17.1.6	Erfolgsfaktoren	613
17.2	Projektbeispiele zur IKS- und Compliance-Automatisierung	616
17.2.1	Abdeckung der Schweizer Compliance- Anforderungen bei KUONI	616
17.2.2	SAP BusinessObjects Process Control 2.5 – Implementierung in den Niederlanden	621
17.3	SOX bei Ericsson	625
17.3.1	IKS-Framework bei Ericsson	625
17.3.2	SOX-Compliance-Prozess bei Ericsson	629
17.3.3	Erfahrungen aus vorherigen Projekten	632
17.3.4	Optimierungspotenzial	634
17.3.5	Schritte in Richtung Optimierung	635
17.4	Rückblick auf die IKS-Evolutionsstufen und Fazit	637
A	Abkürzungsverzeichnis	643
B	Literatur	649
C	Der Autor dieses Buches	653
D	Beiträger zu diesem Buch	655
Index	657