

# Inhalt

Vorwort .....	25
Vertrauen ist gut, Kontrolle ist billiger: Einleitung .....	27

## TEIL I Vom Paragraphen zum Konzept: IKS und Compliance im ERP-Umfeld

<b>1 Gesetzliche Anforderungen im Bereich IKS-Compliance</b> .....	<b>41</b>
<b>1.1 Begriffsdefinitionen und Abgrenzung</b> .....	<b>41</b>
1.1.1 Compliance .....	41
1.1.2 Internes Kontrollsystem (IKS) und GRC .....	43
1.1.3 Gesetzliche IKS-Anforderungen in Übersee – die vielen Gesichter des SOX .....	45
1.1.4 SOX in den USA .....	45
1.1.5 SOX in Kanada (NI 52-109) .....	47
1.1.6 SOX in Japan .....	47
1.1.7 SOX in China .....	48
<b>1.2 IKS-Anforderungen in Europa</b> .....	<b>49</b>
1.2.1 8. EU-Richtlinie .....	49
1.2.2 Deutschland .....	50
1.2.3 Schweiz .....	52
1.2.4 Österreich .....	53
1.2.5 Frankreich .....	54
1.2.6 Dänemark .....	54
1.2.7 Italien .....	54
1.2.8 Spanien .....	55
<b>1.3 IKS-Anforderungen in der Finanzbranche</b> .....	<b>56</b>
1.3.1 Solvency II im Versicherungswesen .....	56
1.3.2 Basel II und III im Bankwesen .....	58
<b>1.4 Unternehmenserfolg durch IKS?</b> .....	<b>60</b>
<b>1.5 Resümee</b> .....	<b>62</b>

## **2 Der Prüfer kommt: Wann, warum und wie man damit umgeht** 63

---

<b>2.1</b>	<b>IKS im IT-Umfeld aus der Sicht der Wirtschaftsprüfung</b> .....	64
2.1.1	Herausforderung durch die Informationstechnologie .....	65
2.1.2	Systemprüfung als Prüfungsansatz im IT-Umfeld .....	65
2.1.3	Ansätze bei der Systemprüfung: IKS im Fokus .....	67
2.1.4	IKS und die Systemprüfung als Pflicht .....	69
<b>2.2</b>	<b>IKS-Assurance in der Praxis</b> .....	72
2.2.1	Ausrichtungen der Prüfer .....	73
2.2.2	Ausgewählte Prüfungsgrundsätze .....	74
2.2.3	Arten der externen Prüfung im ERP-Umfeld .....	77
2.2.4	Empfehlungen zum Umgang mit dem Prüfer .....	80
<b>2.3</b>	<b>Interessenskonflikte in der Wirtschaftsprüfung</b> .....	83
2.3.1	Prüfung von Interessenskonflikten .....	84
2.3.2	Wenn Prüfer selbst im Spannungsfeld agieren .....	85
<b>2.4</b>	<b>Resümee</b> .....	87

## **3 IKS-Anforderungen und SAP-ERP-Systeme: Grundsätze, Frameworks, Struktur** 89

---

<b>3.1</b>	<b>IKS-Inhalte im SAP-ERP-Umfeld definieren</b> .....	89
3.1.1	IKS-Grundsätze im SAP-ERP-Umfeld: Von GoB zu GoBS und GoBD .....	90
3.1.2	Wer definiert die Spielregeln im SAP-Umfeld? .....	92
3.1.3	Kontroll-Identifizierungsprozess .....	93
3.1.4	Struktur eines klassischen IKS-Frameworks im SAP-ERP-Umfeld .....	96
3.1.5	Struktur der effizienz- und wirtschaftlichkeits- orientierten Kontrollen im SAP-ERP-Umfeld .....	102
<b>3.2</b>	<b>IKS-relevante Referenzmodelle</b> .....	106
3.2.1	COSO .....	106
3.2.2	COBIT .....	107
3.2.3	ITIL .....	108
3.2.4	GAIT .....	109
3.2.5	ITAF .....	110
3.2.6	Risk IT .....	111

3.2.7	Val IT .....	112
3.2.8	CMMI .....	113
3.2.9	MOF .....	114
3.2.10	PCI-DSS .....	115
3.2.11	Zusammenfassende Sicht auf Referenzmodelle .....	115
<b>3.3</b>	<b>IKS und risikomanagementrelevante Standards und Modelle .....</b>	<b>116</b>
3.3.1	ISO-27k-Übersicht .....	117
3.3.2	ISO 27001: Informationssicherheits-Management-system .....	118
3.3.3	ISO 19600 – Compliance Management System .....	119
3.3.4	ISO 31000 – Risikomanagement .....	121
<b>3.4</b>	<b>Resümee .....</b>	<b>123</b>
<b>4</b>	<b>Wie geht SAP mit dem Thema Compliance um? .....</b>	<b>125</b>

---

<b>4.1</b>	<b>Softwarezertifizierung .....</b>	<b>125</b>
4.1.1	SAP-Hinweis 671016 .....	126
4.1.2	Zertifizierungsberichte .....	127
<b>4.2</b>	<b>Compliancerelevante Leitfäden .....</b>	<b>130</b>
4.2.1	SAP-Online-Ressourcen .....	131
4.2.2	SAP-Hinweise zur Behebung der Sicherheitsrisiken .....	131
4.2.3	SAP Security Whitepapers .....	132
4.2.4	SAP Secure Operations Map .....	133
4.2.5	DSAG-Leitfäden: Prüfleitfaden, Datenschutzleitfaden .....	135
4.2.6	SAP Security Optimization Services Portfolio .....	136
<b>4.3</b>	<b>SAP-Lösungen für Governance, Risk and Compliance (GRC) .....</b>	<b>138</b>
4.3.1	Übersicht über die GRC-Lösungen von SAP .....	138
4.3.2	SAP Process Control .....	142
4.3.3	SAP Access Control .....	147
4.3.4	SAP Policy Management (Richtlinienverwaltung) .....	155
4.3.5	SAP Risk Management .....	157
4.3.6	GRC-Werkzeuge in der Cloud .....	161
4.3.7	SAP Business Integrity Screening .....	163
4.3.8	SAP Business Partner Screening .....	166
4.3.9	SAP Tax Compliance .....	167
4.3.10	SAP Audit Management .....	168

4.3.11	SAP Enterprise Threat Detection .....	169
4.3.12	Audit-Informationssystem .....	169
<b>4.4</b>	<b>Resümee</b> .....	<b>170</b>

## **TEIL II Vom Konzept zum Inhalt: Kontrollen in SAP ERP**

### **5 Revisionsrelevante SAP-Basics** 175

---

<b>5.1</b>	<b>Am Anfang war die Tabelle:</b>	
	<b>SAP-System als tabellengesteuerte Applikation</b> .....	<b>176</b>
5.1.1	Daten im SAP-System .....	179
5.1.2	Kontrollen im SAP-System .....	185
5.1.3	Tabellenbezogene Suche .....	187
5.1.4	Transaktionsbezogene Suche .....	196
5.1.5	Programmbezogene Suche .....	199
5.1.6	Beziehung zwischen Programmen und Transaktionen ....	200
5.1.7	Beziehung zwischen Programmen und Tabellen .....	202
5.1.8	Zusammenfassung der Suchmöglichkeiten im SAP-System .....	206
5.1.9	Organisationsstrukturen im SAP-System .....	206
<b>5.2</b>	<b>Berechtigungen</b> .....	<b>208</b>
5.2.1	Ablauf und Hierarchie der Berechtigungskontrollen .....	209
5.2.2	Berechtigungsobjekte .....	210
5.2.3	Ermittlung der Berechtigungsobjekte .....	215
5.2.4	Rollen im SAP-System .....	219
5.2.5	Benutzer im SAP-System .....	221
5.2.6	Benutzertypen im SAP-System .....	223
5.2.7	Beispiel für eine Berechtigungsauswertung .....	224
<b>5.3</b>	<b>Resümee</b> .....	<b>227</b>

### **6 Generelle IT-Kontrollen in SAP ERP** 229

---

<b>6.1</b>	<b>Organisatorische Kontrollen</b> .....	<b>229</b>
6.1.1	IT-Organisation .....	230

6.1.2	IT-Outsourcing: Wer ist verantwortlich für die Kontrollen? .....	231
6.1.3	IKS und Cloud .....	235
6.1.4	Zuständigkeit beim Outsourcing – Richtlinien und Dokumentation .....	238
<b>6.2</b>	<b>Kontrollen im Bereich Change Management und Entwicklung .....</b>	<b>240</b>
6.2.1	SAP-Systemlandschaft .....	240
6.2.2	Korrektur- und Transportwesen .....	242
6.2.3	Mandantensteuerung .....	246
6.2.4	Wartung und Updates .....	248
6.2.5	SAP Solution Manager .....	251
<b>6.3</b>	<b>Sicherheitskontrollen beim Zugriff auf das SAP-System und bei der Authentifizierung .....</b>	<b>252</b>
6.3.1	Identität und Lebenszyklus der Benutzer .....	252
6.3.2	Passwortschutz .....	254
6.3.3	Behandlung der Standardbenutzer .....	258
6.3.4	Notfallbenutzerkonzept .....	260
<b>6.4</b>	<b>Sicherheits- und Berechtigungskontrollen innerhalb von SAP ERP .....</b>	<b>261</b>
6.4.1	Schutz der Programme und Transaktionen – Grundlagen .....	262
6.4.2	Schutz der Programme und Transaktionen bei weitreichenden Entwicklungen .....	266
6.4.3	Schutz der Tabellen .....	272
6.4.4	Kontrollen bei der Steuerung der Berechtigungsprüfungen .....	273
6.4.5	Kritische Administrationstransaktionen .....	276
6.4.6	Berücksichtigung der Funktionstrennungsgrundsätze ....	277
<b>6.5</b>	<b>Resümee .....</b>	<b>279</b>

## **7 Übergreifende Applikationskontrollen in SAP ERP** 281

---

<b>7.1</b>	<b>Grundsatz der Unveränderlichkeit .....</b>	<b>282</b>
7.1.1	Schutz der Daten in Tabellen .....	282
7.1.2	Debugging .....	283
7.1.3	Änderbarkeit der Belege .....	286

<b>7.2</b>	<b>Kontrollen für die datenbezogene Nachvollziehbarkeit</b> .....	288
7.2.1	Änderungsbelege in SAP ERP .....	288
7.2.2	Tabellenprotokollierung .....	290
7.2.3	Belegnummernvergabe .....	294
<b>7.3</b>	<b>Nachvollziehbarkeit der Benutzeraktivitäten im SAP-System</b> .....	296
7.3.1	System-Log .....	296
7.3.2	Security Audit Log .....	299
7.3.3	Historie der Transaktionsaufrufe .....	300
7.3.4	Nachvollziehbarkeit der Systemänderungen im Korrektur- und Transportwesen .....	301
<b>7.4</b>	<b>Prozessübergreifende Verarbeitungskontrollen</b> .....	304
7.4.1	Überwachung der Verbuchungsabbrüche .....	304
7.4.2	Vollständigkeit der ALE-Schnittstellenverarbeitung .....	307
7.4.3	RFC-Verbindungen (Remote Function Call) .....	310
7.4.4	Vollständigkeit der Batch-Input-Verarbeitung .....	313
<b>7.5</b>	<b>Resümee</b> .....	315

## **8 Kontrollen in der Finanzbuchhaltung** 317

---

<b>8.1</b>	<b>Grundlegende Kontrollmechanismen im Hauptbuch</b> .....	318
8.1.1	Grundsatz: Zeitnähe der Buchungen .....	318
8.1.2	Bilanz .....	321
8.1.3	Sachkontenstammdaten .....	322
8.1.4	Konsistenzcheck der Verkehrszahlen mit der großen Umsatzprobe .....	324
8.1.5	Ausgewählte Kontrollen bei Abschlussarbeiten .....	325
8.1.6	Abstimmarbeiten im Hauptbuch .....	327
<b>8.2</b>	<b>Kontrollen zur Richtigkeit und Qualität der Daten im Hauptbuch</b> .....	328
8.2.1	Richtigkeit der Kontenfindung .....	329
8.2.2	Feldstatusgruppen .....	331
8.2.3	Berechnung von Steuern bei manuellen Buchungen .....	332
8.2.4	Validierungen im SAP-System .....	334
8.2.5	Fremdwährungen .....	335
<b>8.3</b>	<b>Vollständigkeit der Verarbeitung im Hauptbuch</b> .....	338
8.3.1	Belegvorerfassung .....	338

8.3.2	Dauerbuchungen .....	341
8.3.3	Abstimm-Ledger .....	342
<b>8.4</b>	<b>Sicherheit und Schutz der Daten im Hauptbuch .....</b>	<b>344</b>
8.4.1	Schutz der Buchungskreise .....	344
8.4.2	Toleranzgruppen .....	347
8.4.3	Schutz der Stammdaten .....	349
8.4.4	Kritische Transaktionen .....	353
8.4.5	Funktionstrennung im Hauptbuch .....	353
<b>8.5</b>	<b>Kontrollen in der Anlagenbuchhaltung .....</b>	<b>355</b>
8.5.1	Grundlagen der Anlagenbuchhaltung im SAP-System .....	355
8.5.2	Default-Werte bei Anlagenklassen .....	357
8.5.3	Kontenfindung in der Anlagenbuchhaltung .....	358
8.5.4	Konsistenzprüfung der Kontenfindung und der Konfiguration .....	359
8.5.5	Abschreibungen .....	362
8.5.6	Anlagengitter .....	364
8.5.7	Geringwertige Wirtschaftsgüter .....	366
8.5.8	Berechtigungssteuerung in der Anlagenbuchhaltung .....	367
8.5.9	Kritische Berechtigungen in der Anlagenbuchhaltung .....	369
<b>8.6</b>	<b>Kontrollen in der Kreditoren- und Debitorenbuchhaltung .....</b>	<b>370</b>
8.6.1	Richtigkeit der Abstimmkonten .....	370
8.6.2	Zahlungsfunktionen .....	371
8.6.3	Einmalkunden und -lieferanten – Vorsicht! .....	374
8.6.4	Altersstruktur und Wertberichtigungen .....	376
8.6.5	Vier-Augen-Prinzip bei der Stammdatenpflege .....	377
<b>8.7</b>	<b>Resümee .....</b>	<b>378</b>

## **9 Kontrollmechanismen im SAP-ERP- gestützten Procure-to-Pay-Prozess** 379

---

<b>9.1</b>	<b>Bestellwesen .....</b>	<b>381</b>
9.1.1	Berechtigungskonsistente Pflege der Organisationsstrukturen .....	381
9.1.2	Vier-Augen-Prinzip im Bestellwesen .....	382
<b>9.2</b>	<b>Wareneingänge und Rechnungsprüfung .....</b>	<b>385</b>
9.2.1	Wareneingänge: Kritische Bewegungsarten .....	386

9.2.2	3-Way-Match und Zahlungssperren bei der Logistik-Rechnungsprüfung .....	387
9.2.3	Prüfung auf doppelte Rechnungserfassung .....	390
<b>9.3</b>	<b>WE/RE-Konto</b> .....	390
9.3.1	Auszifferung des WE/RE-Kontos .....	391
9.3.2	Abschlussarbeiten und Ausweis des WE/RE-Kontos in der Bilanz .....	393
<b>9.4</b>	<b>Kontrollen rund um das Thema Bestände</b> .....	395
9.4.1	Pflege von Materialstammdaten .....	395
9.4.2	Unbewertetes Vorratsvermögen und getrennte Bewertung .....	397
9.4.3	Kontenfindung bei Materialbewegungen .....	399
9.4.4	Berichtigung des Vorratsvermögens: Inventur und Materialabwertungen .....	400
9.4.5	Freigabe von Verschrottungen .....	403
9.4.6	Produktkostenrechnung .....	404
9.4.7	Ausgänge von unbewertetem Bestand .....	406
<b>9.5</b>	<b>Corporate Governance</b> .....	406
<b>9.6</b>	<b>Resümee</b> .....	407

## **10 Kontrollmechanismen im SAP-ERP-gestützten Order-to-Cash-Prozess** 409

---

<b>10.1</b>	<b>Kontrollen in der vorbereitenden Vertriebsphase</b> .....	410
10.1.1	Kontrollen bei der Auftragserfassung .....	410
10.1.2	Qualität der Kundenstammdaten .....	412
10.1.3	Funktionstrennung bei der Stammdatenpflege .....	414
10.1.4	Kreditlimitvergabe und -kontrolle .....	415
<b>10.2</b>	<b>Kontrollen bei der Auftragserfüllung und Umsatzlegung</b> .....	417
10.2.1	Kontrollen rund um die Warenauslieferung .....	417
10.2.2	Preisfindung und Umsatzsteuerermittlung .....	418
10.2.3	Rücklieferungen und Gutschriften .....	422
10.2.4	Fakturavorrat .....	423
10.2.5	Vollständigkeit der buchhalterischen Erfassung von Fakturen .....	424
10.2.6	Mahnwesen .....	426
<b>10.3</b>	<b>Resümee</b> .....	430

# 11 Datenschutz-Compliance in SAP ERP Human Capital Management 431

---

<b>11.1 Gesetzliche Datenschutzanforderungen</b> .....	432
11.1.1 Rechtliche Datenschutzgrundlagen und Grundsätze .....	432
11.1.2 Grundlagen der DSGVO .....	436
11.1.3 Mitbestimmung und Arbeitnehmerdatenschutz .....	446
<b>11.2 Datenschutzrelevante übergreifende Kontrollmechanismen im SAP-System</b> .....	449
11.2.1 Änderungen von personenbezogenen Daten nachvollziehen .....	450
11.2.2 Protokollierung der Reportaufrufe in SAP ERP HCM .....	451
11.2.3 Daten löschen und unkenntlich machen .....	452
11.2.4 Personenbezogene Daten außerhalb von SAP ERP HCM ...	453
<b>11.3 Besondere Anforderungen an SAP ERP HCM</b> .....	454
<b>11.4 Berechtigungen und Rollen in SAP ERP HCM</b> .....	455
11.4.1 Differenzierende Attribute in SAP ERP HCM .....	456
11.4.2 Personalmaßnahmen .....	458
11.4.3 Strukturelle Berechtigungen .....	461
11.4.4 Berechtigungshauptschalter .....	466
<b>11.5 Datenlöschung und Datensperrung</b> .....	468
<b>11.6 Resümee</b> .....	469

# 12 Betrug im SAP-System 471

---

<b>12.1 Einführung</b> .....	471
12.1.1 Betrugsarten .....	472
12.1.2 Betrug und das SAP-System .....	474
<b>12.2 Betrugsszenarien in der SAP-Basis</b> .....	476
12.2.1 Write-Debugging-Berechtigungen .....	476
12.2.2 Abspielen einer Batch-Input-Mappe unter einem anderen Benutzernamen .....	477
<b>12.3 Betrugsszenarien im Hauptbuch</b> .....	478
12.3.1 Betrügerische manuelle Belegbuchungen im Hauptbuch .....	479

12.3.2	Identifizierung und Analyse von manuellen Journaleinträgen .....	479
<b>12.4</b>	<b>Betrugsszenarien im Vertriebsbereich .....</b>	<b>482</b>
12.4.1	Fiktive Rechnungen an fiktive Kunden stellen .....	482
12.4.2	Gewährung nicht ordnungsgemäßer Gutschriften oder Boni .....	484
12.4.3	Übermäßiger Einsatz von Gratiswaren .....	485
12.4.4	Nicht ordnungsgemäße Ausbuchung offener Kundenforderungen .....	487
<b>12.5</b>	<b>Betrugsszenarien in der Personalbuchhaltung .....</b>	<b>488</b>
12.5.1	Fiktive Angestellte .....	488
12.5.2	Limitierter Zugang zu eigenen HR-Daten .....	489
12.5.3	Vier-Augen-Prinzip bei vertraulichen Daten .....	490
<b>12.6</b>	<b>Resümee .....</b>	<b>491</b>

## **13 Exkurs: FDA-Compliance und Kontrollen in SAP** 493

---

<b>13.1</b>	<b>Gesetzliche Anforderungen im Bereich Arznei- und Lebensmittelherstellung .....</b>	<b>493</b>
13.1.1	FDA-relevante gesetzliche Anforderungen im internationalen Vergleich .....	494
13.1.2	GxP – die FDA-Grundsätze .....	495
13.1.3	IT aus der Sicht von FDA-Compliance .....	497
<b>13.2</b>	<b>Validierung der IT-Systeme .....</b>	<b>498</b>
13.2.1	Vorgehensweise bei der Validierung .....	498
13.2.2	Kontrollen in Implementierungsprozessen .....	500
<b>13.3</b>	<b>FDA-Compliance in IT-gestützten Geschäftsprozessen .....</b>	<b>501</b>
13.3.1	Beispiele: Kontrollen in der Beschaffung .....	502
13.3.2	Beispiele: Kontrollen im Produktionsmanagement .....	502
13.3.3	Beispiele: Kontrollen im Qualitätsmanagement .....	503
13.3.4	Beispiele: Kontrollen in der Instandhaltung .....	504
13.3.5	Beispiele: Kontrollen zur Chargenrückverfolgbarkeit .....	504
13.3.6	Beispiele: Kontrollen in Lagerverwaltungsprozessen .....	505
<b>13.4</b>	<b>FDA-Compliance bei Systempflege, -aktualisierung und -änderung aufrechterhalten .....</b>	<b>506</b>
<b>13.5</b>	<b>Resümee .....</b>	<b>508</b>

## **14 Exemplarische effizienz- und wirtschaftlichkeitsorientierte Analyseszenarien in SAP ERP** 509

---

<b>14.1</b>	<b>Prozessbezogene Datenauswertungen</b> .....	510
14.1.1	Vergleich von Einkaufsbestelldatum mit dem Wareneingangsdatum .....	511
14.1.2	Fristgerechte Freigabe bzw. Anlage von Bedarfsanforderungen und Bestellungen .....	516
14.1.3	Zeitspanne zwischen Bestelleingang und Bestätigung des Kundenauftrags .....	525
14.1.4	Zehn weitere Beispiele möglicher datenbasierter Prozessanalysen .....	527
<b>14.2</b>	<b>Analyse der Stammdatenqualität</b> .....	527
14.2.1	Qualität der Kundenstammdaten .....	528
14.2.2	Produzierte Materialien ohne Stückliste .....	530
14.2.3	Abstimmung von Materialkosten innerhalb eines Buchungskreises .....	532
14.2.4	Zehn weitere Beispiele möglicher Stammdatenanalysen .....	534
<b>14.3</b>	<b>Manuelle Datenänderungen</b> .....	535
14.3.1	Veränderungen von Bedarfsanforderungen .....	536
14.3.2	Veränderungen von Einkaufsbelegen .....	538
14.3.3	Veränderungen von Verkaufsbelegen .....	543
14.3.4	Zehn weitere Beispiele für manuelle Datenänderungen .....	546
<b>14.4</b>	<b>Ergänzung von SAP-ERP-Standardreports</b> .....	547
14.4.1	Bestandsanalysen um Planungsparameter erweitert .....	547
14.4.2	Kreditmanagementanalyse um Kundenstammdaten erweitert .....	548
<b>14.5</b>	<b>Resümee</b> .....	550

## **15 Risk und Compliance in SAP S/4HANA** 551

---

<b>15.1</b>	<b>SAP S/4HANA im Überblick</b> .....	551
15.1.1	Universal Journal als Innovationstreiber .....	553
15.1.2	Neue Reporting-Optionen .....	554

15.1.3	Die neue Benutzeroberfläche SAP Fiori .....	555
15.1.4	SAP HANA und die In-Memory-Technologie .....	557
15.1.5	Data Aging .....	557
<b>15.2</b>	<b>Finanzbuchhaltung</b> .....	<b>558</b>
15.2.1	Risk und Compliance in SAP S/4HANA: Das Wichtigste auf einen Blick .....	558
15.2.2	Kontrollmöglichkeiten bei der Migration .....	561
15.2.3	FI-Kontrollen in SAP S/4HANA .....	563
15.2.4	Das neue Datenmodell in der Finanzbuchhaltung .....	565
15.2.5	Änderungen in der Anlagenbuchhaltung .....	566
15.2.6	Geschäftspartnerstammdaten .....	567
15.2.7	Parallele Rechnungslegung .....	568
<b>15.3</b>	<b>Controlling</b> .....	<b>569</b>
15.3.1	Das Zusammenwachsen von FI und CO .....	569
15.3.2	Echtzeitintegration .....	570
15.3.3	Material-Ledger .....	571
15.3.4	Buchhalterische Ergebnisrechnung .....	571
<b>15.4</b>	<b>Resümee</b> .....	<b>572</b>

## **16 Berechtigungen in SAP S/4HANA** 573

---

<b>16.1</b>	<b>Berechtigungen für SAP Fiori</b> .....	<b>574</b>
16.1.1	Berechtigungen in SAP ERP und SAP S/4HANA im Vergleich .....	577
16.1.2	Gestaltung der SAP-Fiori-Berechtigungsrollen .....	578
16.1.3	Berechtigungsprüfung in SAP S/4HANA .....	586
<b>16.2</b>	<b>Berechtigungen für das SAP-S/4HANA-Backend</b> .....	<b>587</b>
16.2.1	Vereinfachung der Stammdatenpflege .....	588
16.2.2	Vereinfachungen im Rechnungswesen (FI/CO) .....	589
<b>16.3</b>	<b>Funktionstrennung in SAP S/4HANA</b> .....	<b>590</b>
<b>16.4</b>	<b>Berechtigungen in SAP HANA</b> .....	<b>593</b>
16.4.1	Pflege von Benutzern und Rollen in SAP HANA .....	596
16.4.2	Berechtigungen für Administratoren in SAP HANA .....	597
16.4.3	Berechtigungen für Schemas in SAP HANA .....	599
<b>16.5</b>	<b>Erfahrungswerte aus SAP-S/4HANA-Berechtigungsprojekten</b>	<b>602</b>
<b>16.6</b>	<b>Resümee</b> .....	<b>605</b>

# 17 Unified Connectivity: Wirksamer Schutz der SAP-ERP-Umgebungen

607

---

<b>17.1</b>	<b>Schnittstellenbezogene Risiken in SAP ERP</b> .....	608
<b>17.2</b>	<b>Die Funktionsweise von UCON</b> .....	612
<b>17.3</b>	<b>Phasen der UCON-Einführung</b> .....	613
17.3.1	Protokollierungsphase (Logging) .....	613
17.3.2	Auswertungsphase (Evaluation) .....	614
17.3.3	Finale Phase (Final) .....	614
17.3.4	Unterschied zwischen der Protokollierungs- und der Auswertungsphase .....	615
<b>17.4</b>	<b>Konfigurationsschritte</b> .....	615
17.4.1	Profilparameter für UCON festlegen .....	615
17.4.2	UCON-Batch-Job einplanen .....	616
17.4.3	UCON-Set-up ausführen .....	616
17.4.4	Virtuelle Hosts für RFCs konfigurieren .....	619
17.4.5	Geeignete Dauer für Protokollierungs- und Auswertungsphasen wählen .....	620
17.4.6	RFMs der Standard-Communication-Assembly zuordnen	621
17.4.7	Funktionsbausteine der Auswertungsphase zuordnen ....	623
17.4.8	Funktionsbaustein der finalen Phase zuordnen .....	624
17.4.9	Durch UCON-Monitorvorlagen im Computer Center Management System navigieren .....	624
17.4.10	»Secure by Default« auswählen .....	625
<b>17.5</b>	<b>Bereitstellungsszenarien für UCON</b> .....	625
17.5.1	Szenario A: Produktive Nutzung des lokalen RFC-Basisszenarios .....	626
17.5.2	Szenario B: Testnutzung des lokalen RFC-Basisszenarios .....	627
17.5.3	Szenario C: Das Produktivsystem ist Teil der RFC-Basisszenario-Landschaft .....	629
17.5.4	Szenario D: Das Entwicklungssystem ist Teil der RFC-Basisszenario-Landschaft .....	631
17.5.5	Szenario E: UCON ausschließlich mit Protokollierung .....	631
17.5.6	Szenario F: Der UCON-RFC ist vollständig ausgeschaltet ...	632
17.5.7	Szenario G: UCON-Rollenbau-Szenario .....	632
17.5.8	Vergleich des Sicherheitsgrades sämtlicher Szenarien .....	634
<b>17.6</b>	<b>FAQ zu UCON</b> .....	635
<b>17.7</b>	<b>Resümee</b> .....	637

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

<b>18 IKS-Automatisierung: Wie bringt man den COSO-Cube ins Rollen?</b>	641
<b>18.1 Grundidee der IKS-Automatisierung</b>	641
18.1.1 COSO-Cube in Aktion	642
18.1.2 Zielsetzung der IKS-Automatisierung	643
<b>18.2 IKS-relevante Objekte und Dokumentation</b>	646
18.2.1 Organisationseinheiten	646
18.2.2 Risiken	648
18.2.3 Prozesse	649
18.2.4 Kontrollen	649
18.2.5 Kontrollziele	651
18.2.6 Kontengruppen	652
18.2.7 Beispiel eines IKS-Datenmodells	653
<b>18.3 Grundszenarien der IKS-Aktivitäten</b>	655
18.3.1 Dokumentation	656
18.3.2 Selektion und Priorisierung von Kontrollaktivitäten	656
18.3.3 Kontrolldurchführung	657
18.3.4 Designtest	658
18.3.5 Effektivitätstest	659
18.3.6 Umfrage	660
18.3.7 Risikobewertung	661
18.3.8 Behebung	661
18.3.9 Sign-off	662
18.3.10 Reportauswertung	662
18.3.11 Personen als Bindeglied zwischen IKS-Objekten und Aktionen	662
<b>18.4 Resümee</b>	664

# 19 IKS-Automatisierung mithilfe von SAP Process Control

665

---

<b>19.1</b>	<b>Einleitung: IKS-Umsetzung mit SAP Process Control</b> .....	666
<b>19.2</b>	<b>Technische Implementierung</b> .....	668
19.2.1	Planung der SAP-GRC-Systemlandschaft .....	669
19.2.2	Initiale Konfiguration der Standardfunktionen .....	672
19.2.3	Informationsquellen zu Implementierung, Betrieb und Upgrade von SAP Process Control .....	674
<b>19.3</b>	<b>Datenmodell</b> .....	676
19.3.1	IKS-Stammdaten in SAP Process Control .....	676
19.3.2	IKS-Datenmodell in SAP Process Control .....	682
19.3.3	Zentrale vs. lokale IKS-Stammdaten .....	684
19.3.4	Zeitabhängigkeit der IKS-Stammdaten .....	686
19.3.5	Nachvollziehbarkeit der Änderungen .....	687
19.3.6	Konzept der objektbezogenen Sicherheit .....	689
19.3.7	Kundeneigene Felder .....	691
19.3.8	Multiple-Compliance-Framework-Konzept .....	693
<b>19.4</b>	<b>Implementierung des IKS-Prozesses</b> .....	696
19.4.1	IKS-Dokumentationsprozess .....	696
19.4.2	Scoping-Prozess .....	708
19.4.3	Planungsprozess, Tests und Bewertungen .....	713
19.4.4	Problembhebungsprozess .....	725
19.4.5	Reporting .....	736
<b>19.5</b>	<b>IKS- und Compliance-Umsetzung: Rollen</b> .....	741
19.5.1	Berechtigungsmodell in SAP Process Control .....	742
19.5.2	Objektbezogene Sicherheit in Aktion .....	743
19.5.3	First-Level- vs. Second-Level-Berechtigungen .....	745
19.5.4	Vordefiniertes Best-Practice-Rollenkonzept im SAP-System .....	746
19.5.5	Anpassung der Rollen .....	747
19.5.6	Gestaltung der Benutzeroberfläche .....	748
<b>19.6</b>	<b>Resümee</b> .....	752

## 20 Umsetzung von automatisierten Test- und Monitoring-Szenarien 753

---

<b>20.1 Automatisierte Test- und Überwachungsszenarien im SAP-Umfeld</b> .....	754
20.1.1 Offline-CAAT-Tools .....	754
20.1.2 Auswertungsmöglichkeiten in SAP-ERP-Systemen .....	760
20.1.3 GRC-Management-Software .....	762
20.1.4 Machine Learning im Dienst von GRC .....	763
<b>20.2 Automatisierte Tests und Monitoring in SAP GRC</b> .....	766
20.2.1 Continuous Monitoring Framework .....	766
20.2.2 Continuous Monitoring Framework – Potenzial und Erwartungshaltung .....	769
<b>20.3 Einrichtung von CMF-Szenarien in SAP Process Control</b> .....	773
20.3.1 SAP GRC mit Geschäftsanwendungen verbinden .....	773
20.3.2 Datenquellen in SAP Process Control .....	779
20.3.3 Geschäftsregeln anlegen .....	785
20.3.4 Überwachung der Datenänderungen im Continuous Monitoring Framework .....	788
20.3.5 Automatisierung mithilfe vordefinierter Best-Practice-Szenarien .....	791
20.3.6 Verbindung von Kontrollen und Regeln .....	794
20.3.7 Und los geht's! .....	795
20.3.8 Verwendung von SAP BW für das Continuous Monitoring Framework .....	798
<b>20.4 Resümees</b> .....	800

## 21 SAP GRC – Erfolgsfaktoren und Erfahrungswerte 801

---

<b>21.1 Wem nutzt GRC: Die drei Verteidigungslinien im Überblick</b> .....	801
21.1.1 Die erste Verteidigungslinie .....	802
21.1.2 Die zweite Verteidigungslinie .....	803
21.1.3 Die dritte Verteidigungslinie .....	804
<b>21.2 Der Mehrwert von GRC</b> .....	805
21.2.1 Einsparung durch Risikoreduktion .....	805

21.2.2	Marktwert eines Unternehmens .....	806
21.2.3	Effizienzsteigerung .....	808
<b>21.3</b>	<b>Projekterfahrungen bei der Automatisierung von IKS und Risikomanagement</b> .....	<b>810</b>
21.3.1	Hilfsmittel und Skills für das GRC-Projekt .....	810
21.3.2	Best-Practice-Projektaufbau bei der IKS-Umsetzung .....	814
21.3.3	IKS-Content .....	816
21.3.4	Erfolgsfaktoren .....	819
<b>21.4</b>	<b>Resümee</b> .....	<b>822</b>

## **Anhang** 827

---

<b>A</b>	<b>Abkürzungsverzeichnis</b> .....	<b>827</b>
<b>B</b>	<b>Literatur</b> .....	<b>839</b>
<b>C</b>	<b>Der Autor</b> .....	<b>845</b>
	 Index .....	 851