

Dipl.-Kfm. Lars Hartke
Dipl.-Ök. Georg Hohnhorst
Dipl.-Ök. Gernot Sattler

SAP[®] Handbuch

Sicherheit und Prüfung

Praxisorientierter Revisionsleitfaden für SAP[®]-Systeme

4., völlig überarbeitete und aktualisierte Auflage



Düsseldorf 2010

Inhaltsverzeichnis

1	SAP-Systeme im Überblick	1
1.1	SAP-Systeme und -Produkte	1
1.1.1	SAP AG – Das Unternehmen.....	1
1.1.2	Einordnung des SAP-Systems als Produkt.....	1
1.1.3	Übersicht der Funktionsbereiche eines SAP-Systems.....	2
1.1.3.1	Rechnungswesen.....	2
1.1.3.2	Logistik.....	3
1.1.3.3	Personalwirtschaft.....	3
1.1.3.4	Werkzeuge.....	4
1.2	Aufbau der SAP-Systeme	4
1.2.1	Grundlagen SAP-Systemarchitektur.....	4
1.2.2	Schnittstellen des SAP-Systems	6
1.2.2.1	Datenein- und -ausgabe im Überblick	6
1.2.2.2	Dialogverarbeitung.....	6
1.2.2.3	Batch-Input-Mappenverarbeitung.....	6
1.2.2.4	Direct-Input.....	7
1.2.2.5	Remote Function Call (RFC).....	8
1.2.2.6	Intermediate Document (IDoc).....	8
1.2.2.7	Application Link Enabling (ALE)	9
1.2.2.8	Business Application Programming Interface (BAPI).....	9
1.2.2.9	Legacy System Migration Workbench (LSMW)	10
1.2.3	Organisation der Daten in einem SAP-System.....	10
1.2.3.1	Mandant	11
1.2.3.2	Buchungskreis.....	11
1.2.3.3	Kontenplan.....	11
1.2.3.4	Kostenrechnungskreis	12
1.2.3.5	Geschäftsbereich.....	12
1.2.3.6	Werk.....	12
1.2.3.7	Einkaufsorganisation.....	13
1.2.3.8	Verkaufsorganisation.....	13

2 Einführung in grundlegende SAP-Prüfungstechniken	15
2.1 Regulatorische Anforderungen an den Einsatz von SAP-Systemen	15
2.2 Vorgehen des Abschlussprüfers	16
2.3 Prüfung anhand von Tabellen.....	17
2.3.1 Aufbau und Inhalt von Tabellen.....	17
2.3.2 Tabellenanzeige	18
2.3.3 Speichern von Tabelleninhalten	22
2.3.4 Auffinden relevanter Tabellen.....	24
2.3.5 Tabellendokumentation.....	26
2.4 Prüfung anhand von Programmen	27
2.4.1 Grundlagen der Programme.....	27
2.4.2 Zusammenhang von Programmen und Transaktionen.....	28
2.4.3 Aufruf eines Programms.....	30
2.4.4 Speichern von Programmresultaten.....	31
2.4.5 Auffinden relevanter Programme.....	31
2.4.6 Programmdokumentation	32
2.4.7 Programmquelltexte.....	32
2.5 Prüfung mit Transaktionen.....	34
2.6 Prüfung des Customizings	35
2.6.1 Grundlagen des Customizings	35
2.6.2 Einsichtnahme in das Customizing.....	35
2.6.3 Dokumentation des Customizings	37
2.7 Auswertung von Tabellenänderungsprotokollen.....	37
2.8 Auswertung von Programmänderungen.....	40
2.9 Auswertung von Customizingänderungen.....	40
2.10 Auswertung von Änderungsbelegen.....	40
3 Generelle prozessübergreifende SAP-Kontrollen	43
3.1 Zugriffskontrollen.....	43
3.1.1 Typische Risiken und Kontrollziele	43
3.1.2 Quick Wins	45
3.1.3 Zugriff auf das System	47
3.1.3.1 Systemimmanente Schutzfunktionen.....	47
3.1.3.2 Parameter zur Kennwortqualität	48
3.1.3.3 Unzulässige Kennwörter.....	54
3.1.3.4 Parameter zum Authentifizierungsverfahren	55
3.1.3.5 Parameter zum Security Audit Log	62

3.1.3.6	Zusammenfassung der Authentifizierungs-Parameter und Soll-Werte	62
3.1.3.7	Prozesse der Benutzerverwaltung	64
3.1.3.8	Standardbenutzer	76
3.1.3.9	Notfallbenutzer und privilegierte Benutzer	78
3.1.3.10	Security Audit Log	80
3.1.4	Autorisierung innerhalb des Systems	82
3.1.4.1	Ablauf der Berechtigungsprüfung	82
3.1.4.2	Elemente zur Steuerung der Zugriffsrechte	87
3.1.4.3	Parameter zur Autorisierung	92
3.1.4.4	Zusammenfassung der Autorisierungs-Parameter und Soll-Werte	95
3.1.4.5	Prozesse der Rollenverwaltung	96
3.1.5	Ausgewählte Fragestellungen zum Berechtigungskonzept	105
3.1.5.1	Vergabe kritischer Profile	105
3.1.5.2	Vergabe kritischer Basis-bezogener Berechtigungen	108
3.1.5.3	Vergabe kritischer Geschäftsprozess-bezogener Berechtigungen	113
3.1.5.4	Schutz der Zugriffe auf SAP-Programme	116
3.1.5.5	Schutz der Zugriffe auf SAP-Tabellen	118
3.1.6	Abbildung von Funktionstrennungen	120
3.1.6.1	Möglichkeiten der Umsetzung von Funktionstrennungen	120
3.1.6.2	Funktionstrennungen bei der Benutzerverwaltung	124
3.1.6.3	Funktionstrennungen bei der Berechtigungsverwaltung	126
3.1.6.4	Funktionstrennung bei IT-bezogenen Aktivitäten	127
3.1.6.5	Funktionstrennung innerhalb der fachlichen Prozesse	127
3.1.7	Checkliste	129
3.1.8	Transaktionen, Tabellen, Programme	130

3.2	Kontrollen im Bereich Verfahrensänderungen.....	133
3.2.1	Typische Risiken und Kontrollziele	133
3.2.2	Quick Wins	136
3.2.3	Change Management bei Einsatz eines SAP-Systems	136
3.2.3.1	Systemlandschaft	136
3.2.3.2	Softwarekomponenten und Namensräume	139
3.2.4	Änderbarkeit des Produktivsystems	142
3.2.4.1	Kontrolle der Systemänderbarkeit	142
3.2.4.2	Kontrolle der Mandantenänderbarkeit	144
3.2.5	Transporte von Änderungen	148
3.2.5.1	Management von Transportaufträgen	148
3.2.5.2	Genehmigungsverfahren für Transporte	150
3.2.5.3	Releasewechsel	154
3.2.6	Entwicklung im Produktivsystem.....	155
3.2.6.1	Entwicklungsrechte.....	155
3.2.6.2	Debugging von Programmen	157
3.2.7	Protokollierung von Änderungen	159
3.2.7.1	Protokolle der Tabellenänderungen	159
3.2.7.2	Tabellenänderungen mittels der Transaktion SE16N.....	162
3.2.7.3	Protokolle der Objektänderungen	163
3.2.7.4	Protokolle der Reparaturen	165
3.2.8	Checkliste	168
3.2.9	Transaktionen, Tabellen, Programme	169
3.3	Verarbeitungskontrollen	171
3.3.1	Typische Risiken und Kontrollziele	171
3.3.2	Quick Wins	172
3.3.3	Vorerfasste Belege	173
3.3.3.1	Organisation.....	173
3.3.3.2	Prüfung der vorerfassten Belege.....	173
3.3.3.3	Betragsabhängige Belegvorerfassung.....	175
3.3.4	Buchungsabbrüche.....	175
3.3.4.1	Organisation.....	176
3.3.4.2	Systemparameter zur Steuerung abgebrochener Buchungen	176
3.3.4.3	Auswertung abgebrochener Buchungen	177
3.3.4.4	Berechtigungen	179

3.3.5	Gelöschte Buchungsaufträge	179
3.3.5.1	Prüfung des Verbuchers	180
3.3.5.2	Prüfung des SysLogs.....	180
3.3.6	Dauerbuchungen	181
3.3.6.1	Organisation.....	182
3.3.6.2	Prüfung der Dauerbuchungsurbelege.....	183
3.3.7	Belegnummern.....	183
3.3.7.1	Interne und externe Belegnummernvergabe	183
3.3.7.2	Belegnummernlücken	184
3.3.7.3	Pufferung von Belegnummern	185
3.3.8	Buchungsperioden	187
3.3.8.1	Organisation.....	189
3.3.8.2	Prüfung der Buchungsperioden	189
3.3.8.3	Buchungszeiträume während des Geschäftsjahresverlaufs	190
3.3.9	Kontenabstimmung.....	190
3.3.9.1	Große Umsatzprobe	191
3.3.9.2	Abgleich Kontensalden mit den Summen der Einzelbelege.....	194
3.3.9.3	Abgleich Salden Hauptbuch mit den Belegen aus Nebenbüchern.....	195
3.3.10	Belegabstimmung	196
3.3.10.1	Organisation.....	197
3.3.10.2	Mindestanforderungen zur Erfüllung der Belegfunktion.....	198
3.3.11	Jobverarbeitung.....	200
3.3.11.1	Organisation.....	200
3.3.11.2	Kontrollen zur Verarbeitung von Batch-Jobs	200
3.3.11.3	Berechtigungen zur Batch-Job-Administration	202
3.3.12	Batch-Input-Mappen.....	203
3.3.12.1	Organisation.....	205
3.3.12.2	Analyse des Batch-Input-Mappen-Monitors.....	205
3.3.12.3	Berechtigungen im Bereich der Batch-Input- Mappen	206
3.3.13	Direct-Input.....	206
3.3.13.1	Organisation.....	207
3.3.13.2	Analyse Direct-Input.....	207
3.3.13.3	Berechtigungen	207

3.3.14	ALE und IDocs	208
3.3.14.1	Systemarchitektur ALE und Aufbauprüfung	209
3.3.14.2	Schnittstellenkontrollen	209
3.3.15	Maschinelle Buchungen aus der CO-FI-Integration.....	212
3.3.15.1	Organisation.....	213
3.3.15.2	Aktivierung Neues Hauptbuch.....	213
3.3.15.3	Vollständigkeit der Verarbeitungen aus dem Abstimmledger.....	213
3.3.15.4	Prüfung der Protokolle.....	214
3.3.15.5	Prüfung des Customizings	214
3.3.16	Checkliste	216
3.3.17	Transaktionen, Tabellen, Programme	217
4	SAP-Prüfung orientiert an Posten der Bilanz sowie Gewinn- und Verlustrechnung.....	219
4.1	Anlagevermögen und Abschreibungen.....	219
4.1.1	Typische Risiken und Kontrollziele	219
4.1.2	Quick Wins	220
4.1.3	Überblick über den Anlagenbuchhaltungsprozess	220
4.1.4	Kontrollen der Anlagenbuchhaltung.....	221
4.1.4.1	Organisationsstrukturen	221
4.1.4.2	Ländereinstellungen.....	222
4.1.4.3	Mitzubuchende Bewertungsbereiche	224
4.1.4.4	Festlegung der Hauptbuchkontierung	226
4.1.4.5	Abschreibungsschlüssel.....	229
4.1.4.6	Abschreibungsbuchungen und Abschreibungs- läufe	229
4.1.4.7	Anlagengitter	232
4.1.4.8	Anlagenstamm und Anlagenklassen	233
4.1.4.9	Vorgänge	237
4.1.4.10	Geringwertige Wirtschaftsgüter (GWG).....	240
4.1.5	Checkliste	242
4.1.6	Transaktionen, Tabellen, Programme	243
4.2	Vorräte und Materialaufwand.....	245
4.2.1	Typische Risiken und Kontrollziele	246
4.2.2	Quick Wins	247
4.2.3	Bestandsführung und Warenbewegungen: SAP-Fakten...	248
4.2.3.1	Warenbewegungen	248
4.2.3.2	Bewegungsarten	250

4.2.3.3	Integration Bestandsführung und Bewertung ...	251
4.2.3.4	Vorgangsarten	251
4.2.3.5	Kontenfindung.....	252
4.2.4	Bestandsführung und Warenbewegungen: Prüfungs- handlungen.....	252
4.2.4.1	Organisation.....	252
4.2.4.2	Massendatenanalysen/belegorientierte Prüfungshandlungen	253
4.2.4.3	Konsistenz zwischen Lager-Materialbestand und Bestand in der Finanzbuchhaltung.....	254
4.2.4.4	Konsistenzprüfung der Bestände	255
4.2.4.5	Toleranzeinstellungen	256
4.2.4.6	Umlagerungen zwischen Werken aus unterschiedlichen Bewertungskreisen.....	257
4.2.4.7	Kontenfindung und Vorgangsschlüssel	258
4.2.4.8	Kritische Warenbewegungen und Berechtigungen	263
4.2.4.9	Nachbuchungen in Vorperioden.....	265
4.2.4.10	Negative Bestände.....	265
4.2.5	Inventur: SAP-Fakten.....	266
4.2.5.1	Inventurdurchführung mit dem SAP-System....	266
4.2.5.2	Inventurverfahren: Körperliche Aufnahme und Buchinventur.....	271
4.2.5.3	Inventurverfahren: Stichtagsinventur und Permanente Inventur	272
4.2.5.4	Inventurverfahren: Stichprobeninventur	272
4.2.5.5	Inventurverfahren: Einlagerungsinventur	273
4.2.5.6	Inventurverfahren: Systemgestützte Werkstatt- inventur	273
4.2.5.7	Inventurverfahren: Cycle-Counting	273
4.2.6	Inventur: Prüfungshandlungen.....	274
4.2.6.1	Organisation.....	274
4.2.6.2	Berechtigungen und Funktionstrennungs- aspekte	275
4.2.6.3	Fixieren des Buchbestands im Inventurbeleg während der Inventur	276
4.2.6.4	Automatische Anpassung des Buchbestands im Inventurbeleg	277

4.2.6.5	Umlagerungen in zeitlicher Nähe zu Inventuren	278
4.2.6.6	Nachbuchungen in Vorperioden und negative Bestände.....	279
4.2.6.7	Verwendung von Änderungsbelegen	279
4.2.6.8	Pflegen von Toleranzgrenzen für Inventurdifferenzen	279
4.2.6.9	Stichprobeninventur	280
4.2.7	Bilanzbewertung: SAP-Fakten.....	282
4.2.7.1	Gesetzliche Vorschriften	282
4.2.7.2	Standardpreis	282
4.2.7.3	Gleitender Durchschnittspreis.....	283
4.2.7.4	Periodisch gleitender Durchschnittspreis.....	283
4.2.7.5	Mittlerer Zugangspreis.....	283
4.2.7.6	Niederstwertprinzip.....	283
4.2.7.7	Verbrauchsfolgeverfahren	284
4.2.7.8	Niederstwertermittlung	284
4.2.7.9	Niederstwertermittlung nach Marktpreisen	285
4.2.7.10	Niederstwertermittlung nach Reichweite.....	285
4.2.7.11	Niederstwertermittlung nach Gängigkeit.....	286
4.2.7.12	Verlustfreie Bewertung	287
4.2.7.13	LIFO und FIFO	287
4.2.8	Bilanzbewertung: Kontrollen und Prüfungshandlungen..	287
4.2.8.1	Organisation.....	287
4.2.8.2	Bewertungskreis- und Buchungskreisebene	288
4.2.8.3	Pflege der prozentualen Abschläge und Abwertungskennziffern für die Niederstwertermittlung.....	288
4.2.8.4	Preissteuerung im Materialstammdatensatz	289
4.2.9	Checkliste	290
4.2.10	Transaktionen, Tabellen, Programme	291
4.3	Forderungen und Umsatzerlöse.....	295
4.3.1	Typische Risiken und Kontrollziele	295
4.3.2	Quick Wins	296
4.3.3	Überblick über den Vertriebsprozess	296
4.3.4	Kontrollen des Vertriebs und des Forderungsmanagements	299
4.3.4.1	Organisationsstrukturen	299
4.3.4.2	Sichten des Kundenstamms	302

4.3.4.3	Integrität des Kundenstamms	304
4.3.4.4	Vier-Augen-Prinzip bei der Stammdatenpflege	306
4.3.4.5	Dubletten im Kundenstamm	307
4.3.4.6	Sperren im Kundenstamm	308
4.3.4.7	Angebote	311
4.3.4.8	Aufträge	313
4.3.4.9	Fakturen	316
4.3.4.10	Kredit- und Forderungsmanagement	320
4.3.4.11	Mahnwesen	327
4.3.4.12	CpD-Kunden	331
4.3.5	Checkliste	333
4.3.6	Transaktionen, Tabellen, Programme	334
4.4	Verbindlichkeiten aus Lieferungen und Leistungen.....	337
4.4.1	Typische Risiken und Kontrollziele	338
4.4.2	Quick Wins	339
4.4.3	Stammdaten: SAP-Fakten	340
4.4.3.1	Materialstammdaten.....	340
4.4.3.2	Lieferantenstammdaten.....	344
4.4.3.3	Weitere Stammdaten	348
4.4.3.4	Risiken	349
4.4.4	Stammdaten: Kontrollen und Prüfungshandlungen.....	349
4.4.4.1	Richtlinien und Standards zur Stammdatenpflege	349
4.4.4.2	Berechtigungsvergabe im Bereich der Materialstammdaten.....	349
4.4.4.3	Mengen- und Wertfortschreibung.....	350
4.4.4.4	Funktionstrennung und Berechtigungsvergabe bzgl. Lieferanten- und Kreditorenstammdaten	350
4.4.4.5	Erweiterter Berechtigungsschutz für bestimmte Felder im Lieferantenstammsatz.....	351
4.4.4.6	Definition sensibler Felder für das Vier-Augen-Prinzip im Lieferantenstammsatz	353
4.4.4.7	Berechtigung zur Massenpflege von Materialstammdaten	353
4.4.4.8	Sperren von Lieferanten.....	354
4.4.4.9	Konsistenzcheck: Abgleich Lieferantenstammdaten bzgl. Einkaufs- und Buchhaltungssicht...	354
4.4.4.10	Auswerten des Änderungsprotokolls	354

4.4.4.11	CpD-Kreditoren	355
4.4.4.12	Doppelte Rechnungen / Doppelte Zahlungen...	356
4.4.5	Bestellanforderung: SAP-Fakten	357
4.4.5.1	Überblick.....	357
4.4.5.2	Risiken	359
4.4.6	Bestellanforderung: Kontrollen und Prüfungshandlungen	359
4.4.6.1	Kritische Berechtigungen	359
4.4.6.2	Freigabestrategien und Unterschriften- regelungen	360
4.4.7	Bestellung und Bestellverfolgung: SAP-Fakten	361
4.4.7.1	Überblick.....	361
4.4.7.2	Risiken	362
4.4.8	Bestellung und Bestellverfolgung: Kontrollen und Prüfungshandlungen	363
4.4.8.1	Organisation der Einkaufsabteilung.....	363
4.4.8.2	Funktionstrennungsaspekte und kritische Berechtigungen	364
4.4.8.3	Nutzung der Freigabestrategie (Unterschriftenregelung).....	365
4.4.8.4	Nachträgliche Änderungen von Bestellungen ..	367
4.4.8.5	Nutzung des InfoUpdate-Kennzeichens	367
4.4.8.6	Unbegrenzte Überlieferungen.....	368
4.4.8.7	Toleranzgrenzen in Bestellungen.....	368
4.4.9	WE/RE-Verrechnungskonto: SAP-Fakten	368
4.4.9.1	Funktionsweise des WE/RE-Kontos	369
4.4.9.2	Risiken	371
4.4.10	WE/RE-Verrechnungskonto: Kontrollen und Prüfungs- handlungen.....	371
4.4.10.1	Organisation und automatische Bebuchung des WE/RE-Kontos	371
4.4.10.2	Regelmäßige manuelle Pflege des WE/RE- Kontos	372
4.4.10.3	Direkte Bebuchbarkeit des WE/RE-Kontos.....	374
4.4.10.4	Berechtigung zur WE/RE-Kontenpflege.....	374
4.4.10.5	Analyse des WE/RE-Kontos über Massen- datenanalyse	375

4.4.11	Rechnungsprüfung: SAP-Fakten	376
4.4.11.1	Überblick.....	376
4.4.11.2	Risiken	378
4.4.12	Rechnungsprüfung: Kontrollen und Prüfungshandlungen.....	378
4.4.12.1	Organisatorische Vorgaben	378
4.4.12.2	Funktionstrennung und kritische Berechtigungen	378
4.4.12.3	Gesperrte Rechnungen.....	380
4.4.12.4	Toleranzgrenzen.....	381
4.4.12.5	Verwendung von Schätzpreisen	383
4.4.12.6	CpD-Konten.....	384
4.4.12.7	Verbundene Unternehmen	384
4.4.13	Zahlung: SAP-Fakten.....	384
4.4.13.1	Zahlungsprogramm.....	384
4.4.13.2	Abweichender Zahlungsempfänger	385
4.4.13.3	Verrechnung zwischen Kreditor und Debitor ...	386
4.4.13.4	Risiken	386
4.4.14	Zahlung: Kontrollen und Prüfungshandlungen.....	386
4.4.14.1	Organisation des Zahlwesens.....	386
4.4.14.2	Prüfung der Zahlungsvorschlags- und der Zahlungsliste sowie der Verwendung der Zahlungssperre.....	387
4.4.14.3	Zahlungssperre.....	387
4.4.14.4	Abweichender Zahlungsempfänger	387
4.4.14.5	Funktionstrennung zwischen Kreditorenbuchhaltung und Zahlungsverkehr.....	388
4.4.14.6	Weitere Kontrollen und Prüfungshandlungen...	389
4.4.15	Checkliste	389
4.4.16	Transaktionen, Programme, Tabellen	390
4.5	Personalaufwand.....	393
4.5.1	Typische Risiken und Kontrollziele	393
4.5.2	Quick Wins	396
4.5.3	Überblick zu personalwirtschaftlichen Funktionen	396
4.5.4	Personalstammdatenpflege.....	399
4.5.4.1	Organisationsstrukturen	399
4.5.4.2	Konzept der Infotypen	402
4.5.4.3	Ausgewählte Infotypen	405
4.5.4.4	Zugriffsschutz über klassische Berechtigungen..	406

4.5.4.5	Zugriffsschutz über strukturelle Berechtigungen	412
4.5.4.6	Zugriffsschutz über kontextabhängige Berechtigungen	413
4.5.4.7	Protokollierung von Infotypen.....	416
4.5.5	Personalabrechnungslauf	418
4.5.5.1	Steuerung der Abrechnung durch den Verwaltungssatz	418
4.5.5.2	Programme zur Personalabrechnung	420
4.5.5.3	Prozessmanager für die Personalabrechnung....	422
4.5.5.4	Protokollierung von Programmstarts und HR-Tabellenänderungen	423
4.5.5.5	Protokollierung der Ausführung von Queries ..	426
4.5.6	Buchung und Ausweis des Personalaufwands	428
4.5.6.1	Schnittstellenverarbeitung der Personaldaten ...	428
4.5.6.2	Verarbeitung mittels Lohnarten	431
4.5.6.3	Ausweis in der Erfolgsrechnung	437
4.5.7	Integration der Zeitwirtschaft	441
4.5.8	Integration des Reisemanagements.....	448
4.5.9	Checkliste	456
4.5.10	Transaktionen, Tabellen, Programme	457
	Literaturverzeichnis	459
	Stichwortverzeichnis	461