SAP PRESS

Handbuch SAP®-Revision

Internes Kontrollsystem und GRC

3., aktualisierte und erweiterte Auflage

- Prüfung aller relevanten SAP-Komponenten und Prozesse
- Implementierung und Automatisierung eines tragfähigen IKS
- Inkl. SAP S/4HANA, der neuen GRC-Tools für SAP HANA und der Neuerungen von GRC 12.0

Maxim Chuprunov

Rheinwerk Publishing

Kapitel 8
Kontrollen in der Finanzbuchhaltung

IKS, Prüfung und Revision assoziiert man in erster Linie mit der Finanzberichterstattung. Aus diesem Grund eröffnen wir in diesem Buch das vielfältige Thema der SAP-Prozesskontrollen mit der Finanzbuchhaltung.

Eine der Hauptursachen und der Auslöser der IKS-Compliance-Anforderungen (IKS = Internes Kontrollsystem) ist die externe Finanzberichterstattung, auf die sich bestimmte Zielgruppen außerhalb des Unternehmens verlassen. Einige Elemente dieser Finanzberichterstattung, zum Beispiel Bilanz sowie Gewinn- und Verlustrechnung (GuV), kommen gewissermaßen »per Knopfdruck« zustande. Dabei sind im Wesentlichen folgende FI-Komponenten von SAP ERP relevant:

- Hauptbuchhaltung (FI-GL und gegebenenfalls das neue Hauptbuch, New General Ledger, GL)
- Kreditorenbuchhaltung (FI-AP)
- Debitorenbuchhaltung (FI-AR)
- Bankbuchhaltung (FI-BL)
- Anlagenbuchhaltung (FI-AA)

Neuerungen in SAP S/4HANA

Wir stützen uns in diesem Kapitel auf Release SAP ERP 6.0. In Kapitel 15, »Risk und Compliance in SAP S/4HANA«, finden Sie die zusammenfassende Übersicht der relevanten Neuerungen in SAP S/4HANA.

Um sich auf diese Berichterstattung verlassen zu können und damit ein SAP-System den in Abschnitt 3.1.1, »IKS-Grundsätze im SAP-ERP-Umfeld: Von GoB zu GoBS und GoBD«, beschriebenen Grundsätzen gewachsen sein kann, müssen bestehende Risiken erkannt und mit effektiven Kontrollen adressiert werden. Ohne Anspruch auf eine vollständige Aufzählung aller relevanten Sachverhalte zu erheben, gehen wir in diesem Kapitel auf die wichtigsten Risiken und Kontrollmechanismen ein und beschreiben Prüfungshandlungen, die in der Praxis ein »Muss« in jedem SAP-System sind.

Bei der Beschreibung der Prüfungshandlungen gehen wir verstärkt auf relevante Datenmodelle ein (Datenbanktabellen). Diese Informationen helfen Ihnen, in Teil III, »Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsystems«, eine Verbindung zu möglichen automatisierten Test- und Monitoring-Szenarien im SAP-System herzustellen – da bei der Einrichtung der meisten dieser Szenarien Daten direkt aus Datenbanktabellen gelesen werden müssen und das Verständnis der zugrundeliegenden Datenmodelle dabei sehr wichtig ist.

8.1 Grundlegende Kontrollmechanismen im Hauptbuch

Das Hauptbuch ist aus IKS-Sicht das »Herz« der SAP-ERP-Anwendung, in dem alle für die externe Finanzberichterstattung relevanten Informationen zusammenkommen. In diesem Abschnitt vermitteln wir Ihnen das Grundverständnis der Vorgänge im Hauptbuch (Komponente FI-GL von SAP) und sprechen einige ausgewählte Kontrollbereiche an.

8.1.1 Grundsatz: Zeitnähe der Buchungen

Periodengenau buchen

Der Grundsatz eines zeitgerechten bzw. zeitnahen Ausweises der Geschäftsvorfälle in der Berichterstattung wird in SAP ERP dadurch realisiert, dass das Geschäftsjahr in sogenannte Buchungsperioden aufgeteilt ist. Dabei kann das Geschäftsjahr einem Kalenderjahr entsprechen oder als Rumpfgeschäftsjahr bzw. als vom Kalenderjahr abweichendes Geschäftsjahr abgebildet sein. Systemtechnisch müssen dabei die sogenannte *Geschäftsjahresvariante* und die *Variante für Buchungsperioden* konfiguriert und einem Buchungskreis – einer eigenständig bilanzierenden Einheit im SAP-System – zugewiesen sein. Die einzelnen Buchungsperioden entsprechen in der Regel einem Kalendermonat und generell gilt, dass zu einem Zeitpunkt nur eine Buchungsperiode offen sein darf (bzw. maximal zwei Buchungsperioden, da zum Beispiel am Anfang eines Monats noch Buchungen vorgenommen werden können, die den Vormonat betreffen). Die Minimalanforderung wäre folgende: Wenn der Jahresabschluss erstellt/festgestellt ist, müssen alle Buchungsperioden des abgelaufenen Geschäftsjahres geschlossen sein.

Sonderperioden

Eine Ausnahme können die sogenannten *Sonderperioden* darstellen: Über die »normalen« Buchungsperioden (in der Regel zwölf) hinaus werden üblicherweise weitere Hilfsperioden eingerichtet – in der Regel bis zu vier zusätzliche Perioden zu den normalen Buchungsperioden. Diese zusätzlichen

Buchungsperioden stehen am Jahresende während der Erstellung des Jahresabschlusses für allerlei Korrekturen und manuelle Buchungen zur Verfügung. Die Buchungsperiode 12 wird bei der Bebuchung der Sonderperioden geschlossen.

In Tabelle T001 können Sie die einem Buchungskreis zugeordnete Variante für Buchungsperioden finden, deren aktuelle Einstellungen Tabelle T001B zu entnehmen sind. Die für Variante 1000 in Tabelle T001B ausgewerteten Einträge zeigen, dass für die meisten Kontengruppen alle Hauptbuchungsperioden offen sind (siehe Abbildung 8.1). Dies gilt für alle Buchungskreise, die die Variante 1000 verwenden. Dieses Negativbeispiel stammt aus einem Entwicklungssystem; in einem produktiven SAP-System würde es zu einer wesentlichen Beanstandung führen.

Data Browser: Tabelle T001B 154 Treffer

Prüftabelle...

Tabelle: T001B
Angezeigte Felder: 19 von 19 Feststehende Führungsspalten: 5 Listbreite 0250

Mandant	Satzart	Var. BuchPer.	Kontoart	Bis Konto	Von Konto	Geschäftsjahr	Von Periode	Geschäftsjahr	Bis Periode	Geschäftsjahr
100	0	0001	+			2000	001	2007	016	2000
100	0	0001	A	zzzzzzzzzz		2000	001	2007	016	2000
100	0	0001	D	zzzzzzzzzz		2000	001	2007	016	2000
100	0	0001	G			1992	001	2098	012	1991
100	0	0001	K	zzzzzzzzzz		2000	001	2007	016	2000
100	0	0001	S	zzzzzzzzzz		2000	001	2007	016	2000
100	0	0002	G			1995	001	1995	012	1995
100	0	1000	+			2017	001	2017	012	2017
100	0	1100	+			2017	001	2017	012	2017
100	0	1100	D	zzzzzzzzzz		2017	001	2017	012	2017
100	0	1100	G			1992	001	2098	012	1991
100	0	1100	K	zzzzzzzzzz		2017	001	2017	012	2017

Abbildung 8.1 Varianten für Buchungsperioden – Einstellungen

Die Differenzierung zwischen den einzelnen Sachkonten wird hier anhand der Kontengruppen vorgenommen:

- A – Anlagen
- D – Debitoren
- G – Special Ledger
- K – Kreditoren
- M – Material
- S – Sachkonten

Prüfung: Grundsatz der zeitnahen Buchungen

Prüfen Sie die Einhaltung des Grundsatzes der Zeitnähe der Erfassung von Geschäftsvorfällen folgendermaßen:

1. Sorgen Sie für einen Überblick über die eingerichteten Geschäftsjahresvarianten (Transaktion OB29, Geschäftsjahresvarianten, oder Tabelle T009) sowie über deren Zuordnung zu den relevanten Buchungskreisen (Tabelle T001).

2. Prüfen Sie, ob gleichzeitig mehr als eine Buchungsperiode offen sind (Tabelle T001B) oder ob die Ein-Monats-Regel (bzw. maximal zwei Monate) in der Vergangenheit eingehalten wurde (Auswertung der Änderungen in Tabelle T001B mithilfe des Reports RSTBHIST).

Keine monatlichen Abschlüsse

Nicht alle Unternehmen führen monatliche Abschlüsse durch. In diesem Fall wäre es ausreichend, dass die Buchungsperioden geschlossen sind, für die bereits Abschlüsse erstellt worden sind (zum Beispiel Quartalsabschlüsse; bei kleineren Unternehmen Jahresabschlüsse). Wichtig ist in diesem Zusammenhang noch, dass Abschlüsse, die bereits veröffentlicht oder geprüft worden sind, nicht mehr geändert werden dürfen.

In Abbildung 8.2 und Abbildung 8.3 sehen Sie, wie die Prüfung der in der Vergangenheit vorgenommenen Änderungen der offenen Buchungsperioden mithilfe des Standardreports RSTBHIST durchgeführt werden kann.

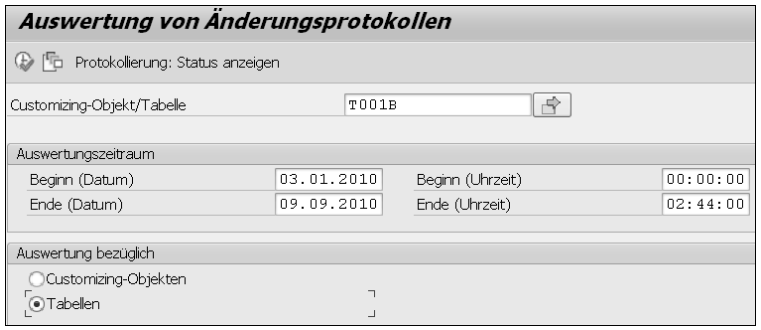

Abbildung 8.2 Prüfung der Änderung der Buchungsperioden in der Vergangenheit

Starten Sie den Report RSTBHIST (siehe Abbildung 8.2). Geben Sie den Namen der Tabelle im Feld **Customizing-Objekt/Tabelle** ein, und klicken Sie auf (**Ausführen**).

In Abbildung 8.3 sehen Sie, dass am 11. September 2017 für einige Kontoarten innerhalb der Variante 3300 die Periode 4 wieder geöffnet wurde.

Berechtigungsobjekt F_BKPF_BUP

Buchungsperioden können zusätzlich berechtigungstechnisch geschützt werden – mithilfe des Berechtigungsobjektes F_BKPF_BUP. Mit diesem optionalen Berechtigungsobjekt kann festgelegt werden, in welchen offenen Buchungsperioden Buchungen erlaubt sein sollen.

Erlaubte Buchungsperioden
Technische Bezeichnung: T001B
Mandant: 100

Datum: 11.09.2017 Benutzer: 22TDITTES

	Schlüsselfelder				Funktionsfelder, geändert		
Uhrzeit	Satzart	Variante	Kontoart	Bis Kto.	Feldname	alt	neu
04:35:03	0	3300	+		Von Per. 1	005	004
04:35:03	0	3300	D	9999999999	Von Per. 1	005	004

Abbildung 8.3 Änderungsprotokoll für Tabelle T001B

8.1.2 Bilanz

Entstehung der Bilanz

Wie entsteht eine Bilanz? Während der Erfassung einer manuellen Buchung müssen den einzelnen Positionen in einem Beleg Sachkonten zugewiesen werden. *Sachkonten* sind Hauptkontierungsmerkmale in einem SAP-ERP-System: Bei der Erfassung einer Buchung müssen mindestens zwei Positionen vorhanden sein, mit jeweils einem Soll- und einem Haben-Betrag. Die Summe dieser Beträge muss pro Beleg null ergeben (diese »Null-Kontrolle« ist systemimmanent, das heißt in der Programmlogik codiert, und kann nicht einfach geändert werden).

Gesamtheit aller rechnungslegungsrelevanten Vorgänge

Die Gesamtheit aller rechnungslegungsrelevanten Vorgänge, die die Bewegungsdaten (siehe Abschnitt 5.1.1, »Daten im SAP-System«) in einem SAP-System ausmachen, muss am Jahresende, gegliedert nach Sachkonten, als Bilanz und GuV präsentiert werden. Die korrekte und vollständige Zuordnung der einzelnen Sachkonten zur Struktur dieser Berichte ist eine wichtige Voraussetzung für die Richtigkeit der externen Finanzberichterstattung.

In Abbildung 8.4 sehen Sie das Beispiel einer Bilanzhierarchie, die über Transaktion OB58 (Pflege der Tabellen T011/T011T) gepflegt wird.

Prüfung: Bilanzstruktur

Die Bilanz muss auf die Richtigkeit der Struktur und auf die Vollständigkeit der Kontenzuordnung hin geprüft werden:

1. Rufen Sie die Bilanzstruktur über Transaktion OB58 oder im Einführungsleitfaden (Implementation Guide, IMG) über **Finanzwesen • Hauptbuchhaltung • Geschäftsvorfälle • Abschluss • Dokumentieren • Bilanz-/GuV-Strukturen definieren** (Transaktion SPRO) auf.
2. Klappen Sie die Hierarchie innerhalb eines relevanten Knotens auf. Die fachliche Beurteilung der Richtigkeit der Zuordnung der Sachkonten ist Aufgabe des Wirtschaftsprüfers.

3. Die nicht zugeordneten Sachkonten sind als solche außerhalb der Bilanz/GuV-Hierarchie aufgelistet. Die nicht zugeordneten Sachkonten können auf eine unvollständige Bilanzstruktur hinweisen. Es ist zu empfehlen, solche Konten zum Beispiel der Position »Verrechnungskonten« zuzuweisen und dann zu prüfen, ob die Position den Saldo null aufweist.

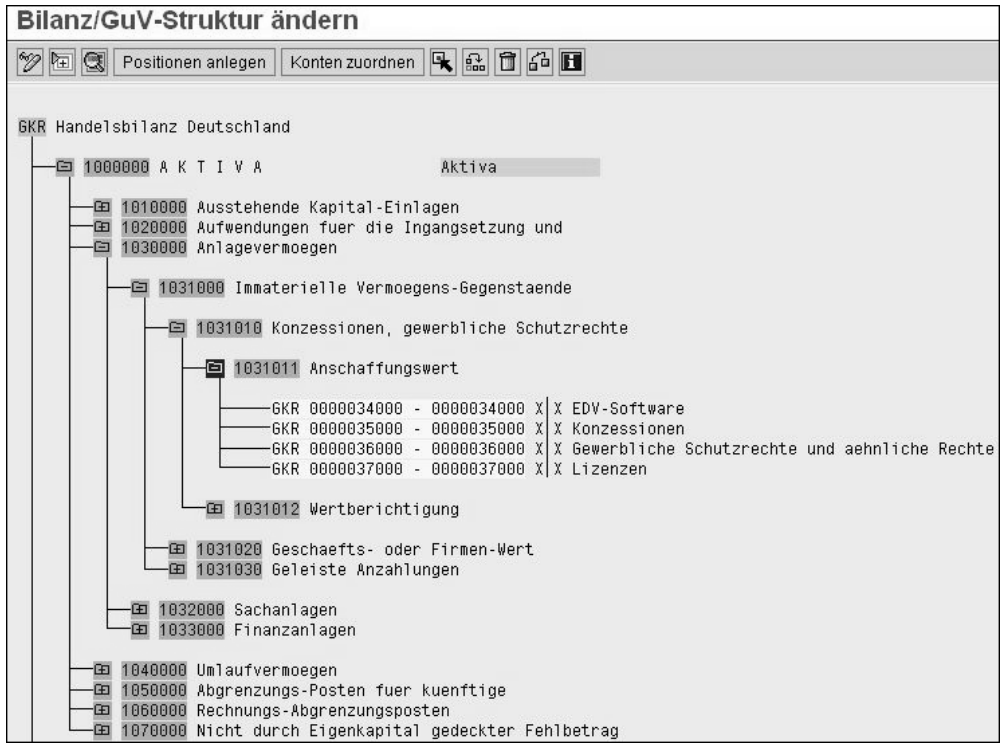

Abbildung 8.4 Bilanzstruktur

Parallele Rechnungslegung

Bei der Zuordnung der Sachkonten der Bilanzhierarchie kann es Ausnahmen geben: Bei der Abbildung der parallelen Rechnungslegung, zum Beispiel um gleichzeitig länderspezifische (HGB) und international anerkannte (US-GAAP oder IFRS) Bilanzierungsrichtlinien umzusetzen, basierend auf der sogenannten Sachkontenlösung, ist die Verwendung von Hilfskonten üblich, die als »Dummys« verwendet und nicht in der Bilanz gebraucht werden. Solche Sachkontenlösungen haben sich allerdings mit der Etablierung des neuen Hauptbuches (New GL) erübrigt.

8.1.3 Sachkontenstammdaten

Auf der Datenbankebene findet man Sachkonten in SAP ERP in den Tabellen SKA1 (Zentrale Sachkontendaten) und SKB1 (Buchungskreisspezifische

Daten, siehe Abbildung 8.5 sowie Abschnitt 5.1, »Am Anfang war die Tabelle: SAP-System als tabellengesteuerte Applikation«).

Die einzelnen Felder im Sachkontenstamm haben eine wichtige Steuerungsfunktion. Manche dieser Funktionen sind mit Risiken verbunden und müssen somit aus IKS-Gesichtspunkten kontrolliert werden.

Tabelle: SKA1
Angezeigte Felder: 9 von 9 Feststehende Führungsspalten: 3 Listbreite 0250

Kontenplan	Sachkonto	Bestandskonto	ErfolgsktoTyp	Kontengruppe	Buchungssperre	Kurztext
1000	0001000000	X		10		Hauptkasse
1000	0001000001	X		10		Hauptkasse USD
1000	0001000002	X		10		Petty Cash EUR
1000	0001000003	X		10		Hauptkasse CAD
1000	0001000004	X		10		Hauptkasse GBP
1000	0001000005	X		10		Petty Cash CHF
1000	0001000006	X		10		Hauptkasse CAD
1000	0001000007	X		10		VERVE Hauptkasse JOD
1000	0001000008	X		10		AB Hauptkasse JOD
1000	0001000010	X		10		Kasse Bistromax
1000	0001000013	X		10		Hauptkasse JPY

Abbildung 8.5 Steuerungsfelder in zentralen Sachkontendaten

Die Prüfung der Plausibilität und der Richtigkeit der Sachkontenstammdaten ist im Rahmen einer Systemprüfung sehr wichtig.

Prüfung: Felder im Sachkontenstamm

Kontenplan finden

Über Tabelle T001 finden Sie den relevanten Kontenplan, der der untersuchten Organisation bzw. dem Buchungskreis zugeordnet ist. In Tabelle SKA1 sind wichtige Steuerungsinformationen pro Sachkonto definiert.

Eines der Steuerungsfelder ist das Feld **nur Automatisch bebuchbar** in Abbildung 8.6.

Tabelle: SKB1
Angezeigte Felder: 17 von 24 Feststehende Führungsspalten: 3 Listbreite 0250

Buchungskreis	Sachkonto	Berechtigung	Feldstatusgrp	Abstimmkennz.	Steuerkat.	Zins-Kennz.	Autom.bebuchb.	OP-Verwaltung
0001	0000012010		G001	A				
0001	0000012050		G007	A				
0001	0000013000		G007	A	-			
0001	0000013010		G001	A				
0001	0000013050		G007	A				
0001	0000021000		G007	A	-			
0001	0000021010		G001	A				
0001	0000021050		G007	A				
0001	0000022000		G007	A	-			
0001	0000022010		G001	A				
0001	0000022050		G007	A				
0001	0000031000		G039	K	-B			
0001	0000031010		G001		-			
0001	0000031100		G007	A				
0001	0000031200		G001				X	
0001	0000032000		G007	A	-			

Abbildung 8.6 Buchungskreisspezifische Steuerungsfelder in den Sachkontendaten

Es ist wichtig, dass bei Konten, die nicht manuell bebucht werden dürfen, in Tabelle SKB1 in diesem Feld der Wert »X« eingetragen ist (zum Beispiel bei einigen Konten in der Materialwirtschaft oder Umsatzkonten, die nur im Rahmen eines Fakturalaufs bebucht werden dürfen).

Darüber hinaus ist die Richtigkeit der Zuordnung von Feldstatusgruppen wichtig (siehe Abschnitt 8.2.2, »Feldstatusgruppen«). Der Abgleich der zugeordneten Feldstatusgruppen mit den im Blueprint vorgesehenen Einstellungen und die Prüfung der einzelnen Feldstatusgruppen in Stichproben sind zu empfehlen.

Sicherheitstipp: Schutz der Sachkonten

Das SAP-System bietet die Möglichkeit, wichtige Stammdatenobjekte einzeln zu schützen. Tabelle SKB1 (Sachkonten buchungskreisspezifische Daten) enthält das Feld **Berechtigung**. In diesem Feld können den einzelnen Konten Berechtigungsgruppen zugeordnet werden, die bei einer kontengenauen Einschränkung des Zugriffs in Benutzerrollen verwendet werden können.

8.1.4 Konsistenzcheck der Verkehrszahlen mit der großen Umsatzprobe

Im Rahmen eines Monatsabschlusses werden in der SAP-gestützten Buchhaltung periodisch unter anderem Aktivitäten durchgeführt, denen aus IKS-Sicht eine wichtige Rolle zukommt. Hierbei handelt es sich etwa um Aktivitäten, die die Konsistenz der rechnungslegungsrelevanten Transaktionsdaten überprüfen.

Konsistenzcheck: zwei Optionen

Ein solcher Konsistenzcheck kann mithilfe der sogenannten großen Umsatzprobe durchgeführt werden. Dabei gibt es zwei Optionen:

- **Report TFC_COMPARE**
  Sollte das neue Hauptbuch aktiv sein, können Sie den Report TFC_COMPARE_VZ verwenden; die Auswertung wird dabei pro eingerichtetem Ledger durchgeführt.
- **Report SAPF190**
  Ist das neue Hauptbuch nicht aktiv, verwenden Sie für die Abstimmung den Report SAPF190 (große Umsatzprobe).

[+]

Aktivierung des neuen Hauptbuches

Mithilfe von Tabelle FAGL_ACTIVEC können Sie überprüfen, ob das neue Hauptbuch aktiviert ist. Ist dies der Fall, finden Sie im Feld **Active** den Wert »X« vor.

Konsistenzprüfungen

Die erwähnten Reports führen eine erweiterte Abstimmung in der Finanzbuchhaltung durch. Dabei werden folgende Konsistenzprüfungen ausgeführt:

- Soll- und Haben-Verkehrszahlen der Debitorenkonten, Kreditorenkonten und Sachkonten mit den Soll- und Haben-Summen der gebuchten Belege.
- Soll- und Haben-Verkehrszahlen der Debitorenkonten, Kreditorenkonten und Sachkonten mit den Soll- und Haben-Summen der Anwendungsindizes (die Anwendungsindizes werden systemintern für Konten mit OP-Verwaltung oder Einzelpostenanzeige gebraucht).

Die Ergebnisse der Abstimmung werden gespeichert, das heißt, die vergangenen Läufe dieser Berichte können im SAP-System nachvollzogen werden.

SAP-Hinweis 31875

Die Durchführung der Abstimmanalyse kann unter Umständen mehrere Stunden andauern. Deshalb sollte die Datenselektion im Hintergrund (als Batch-Job) ausgeführt werden. Differenzen bei den Anwendungsindizes haben ihre Ursache oft in der Änderung der Einstellung **Einzelpostenanzeige** des Sachkontos. Weitere Informationen hierzu können SAP-Hinweis 31875 entnommen werden.

In der Praxis besteht häufig der Irrglaube, dass die große Umsatzprobe prüft, ob Haupt- und Nebenbuch übereinstimmen. Das ist nicht der Fall und sollte durch zusätzliche (manuelle) Prüfungen im Rahmen des IKS sichergestellt werden (sehen Sie hierzu Abschnitt 8.1.6, »Abstimmarbeiten im Hauptbuch«).

8.1.5 Ausgewählte Kontrollen bei Abschlussarbeiten

Berichte mit Änderungen

Außer der großen Umsatzprobe ist es im Rahmen der Abschlussarbeiten anzuraten, eine Reihe von Reports auszuführen, die Änderungen von wichtigen Stammdaten im Hauptbuch auflisten. In Tabelle 8.1 haben wir die wichtigsten Berichte zusammengetragen.

Beschreibung	Report	Kommentar
große Umsatzprobe/Vergleich Belege/Verkehrszahlen	SAPF190 TFC_ COMPARE_VZ	Fehlermeldungen mit Basis besprechen
Änderungen der Sachkontenstammdaten	RFSABL00	»Templates« für andere Konten ebenfalls prüfen

Tabelle 8.1 Übersicht über die bei Abschlussarbeiten auszuführenden Kontrollberichte im Hauptbuch

Beschreibung	Report	Kommentar
Änderungen der Buchhaltungsbelege	RFBABL00	besondere Vorsicht bei Dauerbuchungen
Auswertung von abgebrochenen Buchungssätzen	RFVBER00	Belege zu den Unterlagen nehmen
Auswertung von vorerfassten Belegen	RFPUEB00	buchen oder stornieren
Auswertung von gemerkten Belegen	RFTMPBEL	buchen oder stornieren
Kontrolle von Dauerbuchungsurbelegen	RFDAUB00	Beginn, Ende und Plausibilität
Kontrolle von Kreditorenstammdatenänderungen	RFKABL00	Plausibilität von Änderungen und Erfasser prüfen
Kontrolle von Debitorenstammdatenänderungen	RFDABL00	Plausibilität von Änderungen und Erfasser prüfen
Kontrolle von Bankstammdatenänderungen	RFBKABL0	Plausibilität von Änderungen und Erfasser prüfen
Kontrolle von Buchhaltungsbelegänderungen	RFBABL00	Plausibilität von Änderungen und Erfasser prüfen
Auswertung von FI-Buchungen	RFBELJ00	Plausibilität von Erfasser prüfen
Änderungsanzeige Kreditmanagement	RFDKLIAB	Änderungen der Limits und Sperren prüfen

Tabelle 8.1 Übersicht über die bei Abschlussarbeiten auszuführenden Kontrollberichte im Hauptbuch (Forts.)

Je nach Compliance-Umfeld kann es notwendig sein, die Ergebnisse der Berichte aus Tabelle 8.1 als Nachweis der durchgeführten Kontrollhandlungen aufzubewahren bzw. zu archivieren (zum Beispiel in Form von Spool-Listen).

8.1.6 Abstimmarbeiten im Hauptbuch

Im Rahmen des Monats- und Jahresabschlusses werden unter anderem Abstimmarbeiten durchgeführt, die die Kontrolle der Richtigkeit der Bilanz- und GuV-Positionen als Hauptziel haben.

Saldenbestätigungen

Diese wichtige Prüfungshandlung wird sowohl von Unternehmen (gegebenenfalls in Abstimmung mit Wirtschaftsprüfern) oder unter Aufsicht der Wirtschaftsprüfer durchgeführt und ist primär dazu gedacht, die Risiken der Überbewertung von Forderungen und Umsatzerlösen sowie der Unterbewertung von Verbindlichkeiten zu adressieren.

Zusammenarbeit von Unternehmen und Wirtschaftsprüfern

Zum Beispiel druckt und verschickt das Unternehmen Anschreiben zur Saldenbestätigungen an Lieferanten und Kunden, die ihrerseits die Antworten an die Wirtschaftsprüfungsgesellschaft senden.

Um Bestätigungsbriefe zu generieren, werden die SAP-Transaktionen F.17 (für Debitoren bzw. Kunden) und F.18 (für Kreditoren bzw. Lieferanten) verwendet.

Abgleich der Haupt- und Nebenbücher

Geringe Risiken

Weitere Kontrollhandlungen beziehen sich auf die Abstimmung der Zahlen mit dem Hauptbuch, beispielsweise aus der Anlagen-, Kreditoren- und Debitorenbuchhaltung. Unserer Auffassung nach sind in diesem Bereich in SAP ERP 6.0 systemseitig wenig Risiken vorhanden: Der Integrationsgrad der einzelnen FI-Komponenten stellt inzwischen die Einheit des Buchungsstoffes sicher: Zum Beispiel werden in der Anlagenbuchhaltung die Abschreibungsergebnisse nicht mehr per Batch-Input-Technik weitergereicht, sondern direkt in das Hauptbuch gebucht. Des Weiteren sind kreditorische und debitorische Vorgänge im SAP-System nur möglich, wenn in Kreditoren- und Debitorenstammdaten sogenannte Abstimmkonten hinterlegt sind – das heißt, Buchungen erfolgen automatisch direkt im Hauptbuch.

Hilfreiche Abstimmarbeiten

Trotzdem können folgende Abstimmarbeiten hilfreich sein:

- **Abstimmung der Summe der Belege mit Kontensalden**
  Ergebnisse des Reports RFSSLD00 (Sachkontensalden) mit den Ergebnissen des Reports RFHABU00 (Hauptbuch aus der Belegdatei)

- **Abstimmung der Nebenbücher**
  Abstimmung der Ergebnisse des Reports RFKKBU00 (Kontokorrentkontenschreibung aus der Belegdatei) mit den Reports RFKSLD00 (Kreditorensalden in Hauswährung) und RFDSLD00 (Debitorensalden in Hauswährung)

Etwas komplizierter wird es hingegen bei der Abstimmung des Hauptbuches bzw. bei der Erfassung von Zahlen, die außerhalb der FI-Komponente zustande kommen: bei der Materialbewertung in der Komponente MM (Materialwirtschaft), bei der WIP-Ermittlung (WIP = Work in Progress) in der Kostenträgerrechnung oder bei der Auftragsabrechnung in der Komponente PS (Projektabwicklung). Auf weitere Abstimmarbeiten mit Zahlen außerhalb von FI (Finanzwesen) gehen wir in Kapitel 9, »Kontrollmechanismen im SAP-ERP-gestützten Procure-to-Pay-Prozess«, und in Kapitel 10, »Kontrollmechanismen im SAP-ERP-gestützten Order-to-Cash-Prozess«, ein. In Kapitel 15, »Risk und Compliance in SAP S/4HANA«, sehen Sie außerdem, dass der noch höhere Integrationsgrad in SAP S/4HANA einige Abstimmungen überflüssig macht.

8.2 Kontrollen zur Richtigkeit und Qualität der Daten im Hauptbuch

Buchungsvorgänge im SAP-System

In Abschnitt 5.2, »Berechtigungen«, haben Sie Grundlegendes über die Buchungsbelege bzw. Transaktionsdaten im SAP-System erfahren – dies wird Ihnen helfen, sich mit den Informationen in diesem Abschnitt auseinanderzusetzen. Etwas verallgemeinert, kann man Buchungsvorgänge im SAP-System einer dieser beiden Gruppen zuordnen:

- **Non-Routine Transactions**
  Diese werden im SAP-System von einem Buchhalter, größtenteils basierend auf dem eigenen Urteil oder auf der Expertenmeinung, erfasst (zum Beispiel Bilanzpositionen im Bereich Rückstellungen).
- **Routine Transactions**
  Diese werden im SAP-System massenhaft und zum größten Teil automatisiert generiert.

In beiden Gruppen sind Risiken enthalten, die die Richtigkeit und Vollständigkeit des Buchungsstoffes im SAP-System gefährden. Während Risiken bei Non-Routine Transactions im Prüfungswesen durch substantive Prüfungshandlungen (Einzelprüfung der Vorgänge) adressiert werden, stehen bei der zweiten Gruppe (Routine Transactions) die Applikationskontrollen

im Vordergrund (diese werden primär im Rahmen einer Systemprüfung bewertet). Die Applikationskontrollen können verhindern, dass sich Ungenauigkeiten häufen, zum Beispiel aufgrund der schlechten Datenqualität durch die Massendatenverarbeitung. Solchen Risiken kann man mit Kontrollen entgegenwirken, auf die wir im Folgenden eingehen (siehe Abschnitt 8.2.2, »Feldstatusgruppen«, und Abschnitt 8.2.4, »Validierungen im SAP-System«).

8.2.1 Richtigkeit der Kontenfindung

Automatische Zuordnung der Sachkonten

Eine manuelle Belegerfassung, bei der die Zuordnung *aller* Sachkonten im Ermessen eines Buchhalters liegt, macht nur einen Bruchteil aller Transaktionsdaten in einem SAP-ERP-System aus. Die meisten Vorfälle, die aus Buchhaltungssicht inhaltlich den Nebenbüchern angehören, werden in SAP ERP automatisch auf vordefinierte Konten gebucht. Aus IKS-Gesichtspunkten muss die Vollständigkeit und Richtigkeit der Pflege der *Kontenfindung* für relevante Vorgänge geprüft werden. In Abstimmung mit zuständigen Ansprechpartnern können relevante risikobehaftete Vorgänge ausgewählt und geprüft werden, wobei die Prüfung der inhaltlichen Richtigkeit der Kontenfindung ein gutes Buchhaltungsgrundverständnis und Kenntnisse des relevanten Kontenplans voraussetzt. Eine gute Möglichkeit zur Überprüfung der Kontenfindung bietet Transaktion FBKP (Konfiguration Buchhaltung pflegen), siehe Abbildung 8.7.

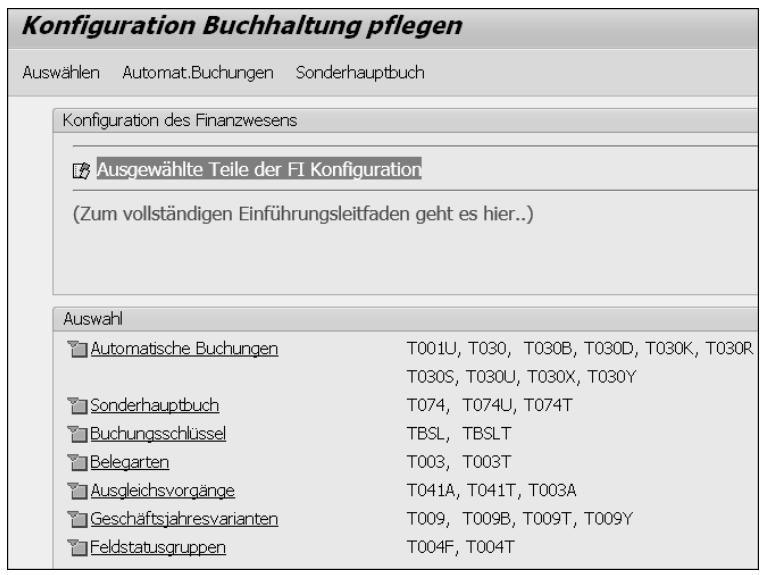

Abbildung 8.7 Prüfung der Kontenfindung mit Transaktion FBKP

Klicken Sie in Transaktion FBKP im Bereich **Auswahl** auf **Automatische Buchungen**. Dadurch erhalten Sie eine Übersicht über die einzelnen Kontenfindungsgruppen (siehe Abbildung 8.8).

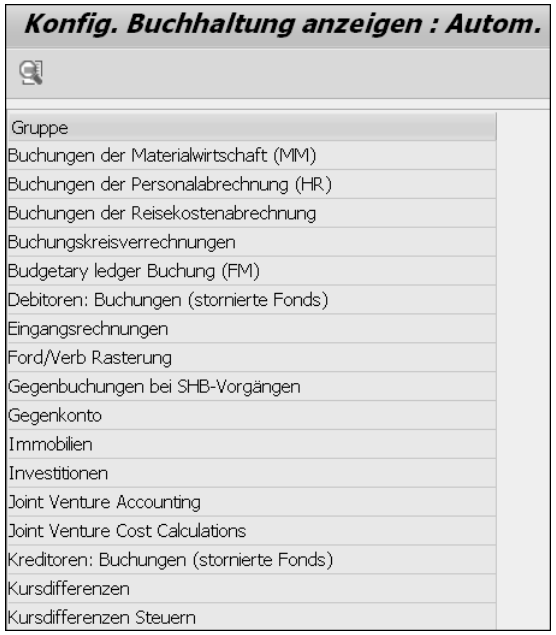

Abbildung 8.8 Übersicht über Kontenfindungsgruppen

Führen Sie einen Doppelklick auf eine der Gruppen im Bereich **Gruppe** aus, in unserem Beispiel auf **Buchungen der Materialwirtschaft (MM)**. Daraufhin gelangen Sie zu einer Übersicht über die einzelnen Vorgänge innerhalb der Gruppe (siehe Abbildung 8.9).

Abbildung 8.9 Übersicht über Vorgänge in einer Gruppe

Ein Doppelklick auf einen Vorgang im Bereich **Vorgänge** führt Sie zu der Übersicht über die hinterlegten Konten. In unserem Beispiel klicken Sie auf **Rückstellungen nachträgliche Abrechnung** und gelangen in die Sicht aus Abbildung 8.10.

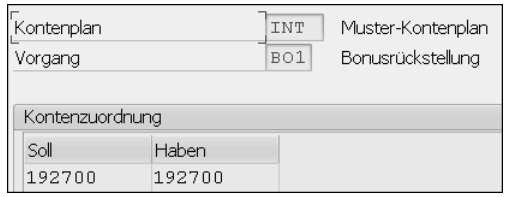

Abbildung 8.10 Übersicht über hinterlegte Konten

Prüfung: Buchungslogik und Kontenfindung

Prüfen Sie für ausgewählte Vorgänge in der automatischen Kontenfindung die Richtigkeit und Vollständigkeit der hinterlegten Sachkonten mithilfe von Transaktion FBKP.

8.2.2 Feldstatusgruppen

Die Pflege von Stammdaten oder die Erfassung von Buchungen erfordert im SAP-System die Eingabe bestimmter Informationen. Der Umfang der erforderlichen Informationen reicht bei Default-Konfigurationseinstellungen nicht immer aus, um eine vollständige und/oder richtige Verarbeitung zu gewährleisten, besonders wenn Standardprozesse im Rahmen der SAP-Implementierung wesentlich angepasst wurden. Um die erforderliche Qualität und Vollständigkeit der Daten zu gewährleisten, bietet das SAP-System die Möglichkeit, vorgangs- und datenspezifische *Feldstatusgruppen* einzurichten.

Kostenstelle: Muss-Eingabe systemseitig erzwingen

In Abbildung 8.11 sehen Sie, dass für die Erfassung der Buchungen, bei denen Aufwandskonten verwendet werden (Kostenkonten), eine eigenständige Feldstatusgruppe ZCA2 eingerichtet wurde. Diese Feldstatusgruppe stellt sicher, dass bei einer Buchung die Kostenstelle als zusätzliches Kontierungsmerkmal eingegeben werden muss (Muss-Eingabe). Nur so kann dieser Vorgang auch im Controlling bzw. Management Accounting berücksichtigt werden (zum Beispiel im Rahmen der Kostenstellenrechnung). Feldstatusgruppen werden den Sachkonten in deren Stammdaten zugeordnet und systemseitig verwendet, falls ein entsprechendes Sachkonto bei der Belegerfassung ausgewählt wurde.

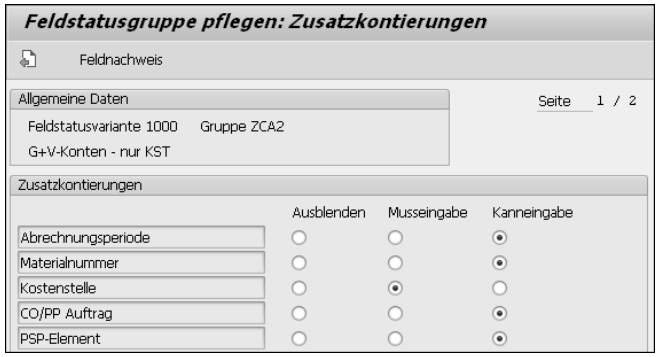

Abbildung 8.11 Pflege der Feldstatusgruppen

Prüfung: Feldstatusgruppen

Eine Analyse und Prüfung der Definition von Feldstatusgruppen sind im Rahmen einer SAP-Systemprüfung zu empfehlen. Dabei prüfen Sie zweierlei:

Mithilfe von Transaktion OBC4 (Pflege Tabelle T004V) können Sie zum einen prüfen, ob bei den eingerichteten Feldstatusgruppen für die relevanten Vorgänge Daten als Muss-Felder definiert sind, die für eine vollständige und richtige Verarbeitung benötigt werden.

Zum anderen bietet das SAP-System Konsistenzcheck-Reports, die bei komponentenübergreifenden Vorgängen die durch Feldstatusgruppen gesteuerte Qualität der Daten überprüfen können. So können Sie zum Beispiel den Report RM07CUFA (Feldauswahlabgleich Bewegungsart – Sachkonto) verwenden, um die Konsistenzprüfung der Feldstatusgruppen für Konten aus MM- und FI-Sichten durchzuführen.

8.2.3 Berechnung von Steuern bei manuellen Buchungen

Reports

Aus IKS-Gesichtspunkten sind die korrekte Bewertung und der korrekte Ausweis der Steuerverbindlichkeiten wesentlich, für die primär der Staat bzw. das Finanzamt als Gläubiger fungiert. In SAP ERP verlässt man sich dabei auf die Richtigkeit des Reports **Umsatzsteuervoranmeldung** (Report RFUMSV00), der die kumulierten Steuerbeträge am Ende einer Periode präsentiert.

Diese kumulierten Beträge setzen sich aus Einzelbelegen zusammen, die bei der Erfassung diverser Vorgänge entstehen. Die wichtigsten Vorgänge sind folgende:

- **Rechnungseingang**
  In der Regel findet die Steuerfindung hier über die manuelle Eingabe des Vorsteuerkennzeichens statt.

- **Fakturierung**
  Die Umsatzsteuerfindung wird im Zusammenhang mit der Fakturierung separat definiert. Diese legt fest, welcher Steuersatz für die Ausgangssteuer zur Anwendung kommt.

Der Report RFUMSV00 zieht Daten über die einzelnen Vorgänge aus Tabelle BSET (Belegsegment Steuerdaten). Auch der Report RFUMSV10 (Zusatzliste zur Umsatzsteuervoranmeldung) nimmt Daten aus den SAP-Tabellen mit Sachkonteneinzelposten, die durch einzelne Buchungen fortgeschrieben werden.

Die Höhe eines Steuerbetrags wird in SAP ERP bei der manuellen Erfassung (der Fakturierungsvorgang ist an dieser Stelle nicht relevant) von einzelnen Buchungen für umsatzsteuerrelevante Vorgänge (Ausgangssteuer und Umsatzsteuer) automatisch berechnet, kann aber manuell geändert werden: Entscheidend ist dabei, wie das ausgewählte Steuerkennzeichen konfiguriert ist.

SAP-Prüfung der Richtigkeit des Steuerbetrags

Wie Sie in Abbildung 8.12 sehen, kann pro Steuerkennzeichen definiert werden, ob eine Fehlermeldung ausgegeben werden soll, wenn der Steuerbetrag nicht korrekt ist. Die Prüfung erfolgt systemseitig:

Pro Steuerkennzeichen wird die korrekte Steuer anhand des Basisbetrags und des Prozentsatzes errechnet. Bei einer Abweichung von mehr als einer Währungseinheit (zum Beispiel Cents oder Centimes) pro Belegposition wird eine Fehlermeldung ausgegeben. Enthält das Steuerkennzeichen keinen Eintrag im Feld **Fehler bei Abweichung**, erscheint anstelle der Fehlermeldung eine Warnung, und die Erfassung der Buchung ist weiterhin möglich.

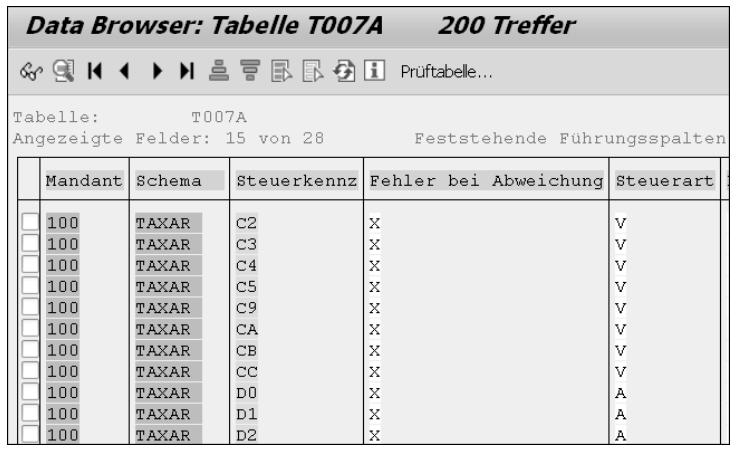

Abbildung 8.12 Steuerung der Fehlermeldung bei abweichendem Steuerbetrag

Prüfung: Einstellungen bei der Steuerberechnung

Mithilfe von Tabelle T007A oder über Transaktion FTXP (Steuerkennzeichen pflegen) können Sie in Bezug auf Steuerkennzeichen auswerten, ob Einstellungen im Feld **Fehler bei Abweichung** angemessen sind: »Leere« Einträge bedeuten, dass die manuelle Eingabe eines Betrags zugelassen ist, der von dem systemseitig errechneten Betrag abweicht.

8.2.4 Validierungen im SAP-System

Kundeneigene logische Regeln

Das SAP-System bietet die Möglichkeit, für verschiedene Vorgänge und zusätzlich zu den bereits vorhandenen Standardkonsistenzchecks kundeneigene logische Regeln einzurichten, die die Richtigkeit der beispielsweise manuell eingegebenen Daten überprüfen. Diese Möglichkeit heißt *Validierung*, und die entsprechende Funktionalität erlaubt es, Validierungs- und Substitutionsregeln einzurichten, die die Kontrollen in der Finanzbuchhaltung stärken können.

In der Praxis werden zum Beispiel folgende Regeln eingerichtet:

- Regeln, die eine unzulässige Kombination von Sachkonten ausschließen
- Regeln, die die Verwendung von nicht zulässigen Geschäftsbereichen unterbinden
- Regeln, die sinnvolle Einträge in Kommentarfeldern (zum Beispiel durch die Minimallänge) begünstigen
- Regeln, die automatische Einträge bestimmter Informationen korrigieren (Substitution)
- Regeln, die einen Maximalbetrag bei einer Buchung einschränken (alternativ dazu können Toleranzgruppen eingerichtet werden, siehe Abschnitt 8.4.2, »Toleranzgruppen«)

Validierungen

Validierungen können aber auch alternativ zu den SAP-Berechtigungsrollen verwendet werden, um den Zugriff auf bestimmte Vorgänge benutzerspezifisch einzuschränken. In Abbildung 8.13 sehen Sie ein Beispiel für eine Validierung. Diese Validierung stellt sicher, dass bei der Erfassung einer Buchung für den Buchungskreis 1510 und der Verwendung der Belegarten DR oder DZ ein Kreditkontrollbereich mitgegeben werden muss.

Abbildung 8.14 zeigt die Voraussetzungen für die Validierung. Sie werden mit der Nachricht **Please enter a credit control area** um die Angabe eines Kontrollbereichs gebeten.

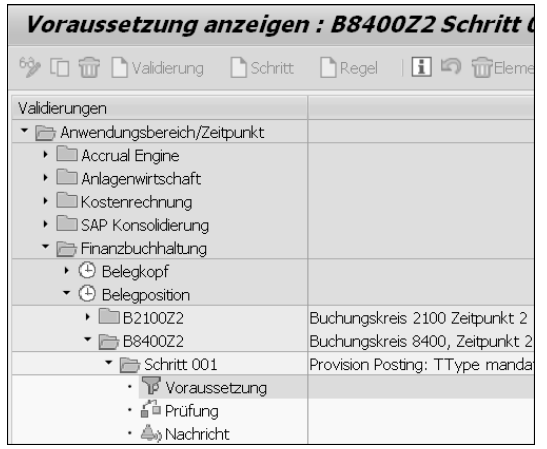

Abbildung 8.13 Beispiel für die Einrichtung einer Validierung

```
( Buchungskreis = '1510' ) AND ( Belegart = 'DR' OR
Belegart = 'DZ' )
```

Abbildung 8.14 Validierung: Voraussetzung

Prüfung: Validierungen und Substitutionen

Bei der Einrichtung von Validierungen sind drei Ebenen zur Überprüfung der Regeln möglich: bei der Eingabe von Daten im Belegkopf, in Einzelpositionen oder erst beim Speichern des Belegs. Dabei gibt es zwei Optionen hinsichtlich des Ausgangs einer Prüfung: eine Warnung oder eine Fehlermeldung. Eine Warnung hat eher informativen Charakter und stellt aus IKS-Sicht keine effektive Kontrolle dar.

1. Validierungen und Substitutionen spielen aus IKS-Sicht eine wichtige Rolle. Versuchen Sie, im Interview und über Transaktion GGBO (Validierungsbearbeitung) einen Überblick über den Zweck und den Inhalt der eingerichteten Validierungsregeln zu erhalten.
2. Beachten Sie bei Substitutionen, dass selbst »gut gemeinte« Regeln mit Risiken verbunden sind: Falls keine Meldungen eingerichtet sind, merkt der Benutzer eventuell nicht, dass die eingegebenen Daten vom SAP-System automatisch geändert bzw. ersetzt werden.

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

- Nicht-Compliance ist einfach zu teuer. Wem nutzt eine strategische Entscheidung, zum Beispiel Daten von Kunden aus dem EU-Raum zu bearbeiten, wenn im Unternehmen keine hinreichenden technischen und organisatorischen Maßnahmen für deren Schutz etabliert sind? Strafen in Höhe von 4 % des weltweiten Jahresumsatzes eines Unternehmens können dessen Position spürbar schwächen.
- Oft wird übersehen, dass das Thema IKS aufgrund seiner traditionellen Fokussierung auf Compliance auch die Überwachung der Geschäftsprozesse hinsichtlich Effizienz, Wirtschaftlichkeit und Performance umfassen kann. Außerdem setzt das im Vorwort angesprochene und das IKS mitumfassende intelligente GRC voraus, dass neben der Gesetzeskonformität auch operative und strategische Zielsetzungen im Fokus von Governance, Risk und Compliance stehen. Es geht daher nicht nur um Paragrafen.
- 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. Darüber hinaus wirkt sich ein IKS positiv auf den Unternehmenswert aus.

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:

- IKS-Management in einem integrierten Ansatz als Teil von intelligentem GRC zu betrachten, ist für viele Unternehmen Neuland. Die Frage nach einem praktikablen Zusammenspiel von IKS und Risikomanagement stellt Unternehmen nicht nur vor konzeptionelle und GRC-lösungsspezifische Herausforderungen, sondern fordert organisatorisch eine engere Zusammenarbeit zwischen den drei Verteidigungslinien im Unternehmen.
- Ohne hinreichende Aufmerksamkeit auf Governance-, Risk- und Compliance-Themen und ohne überzeugende Vorbildrolle der Führungsetagen geht nichts. Liegen diese Voraussetzungen nicht vor, ist es sehr schwierig, eine positive Risikokultur im Unternehmen zu fördern, bei der man einen Risikomanager als Freund, Helfer und Budgetbeschaffer für Problembereiche betrachtet.
- Das komplexe SAP-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 Falle 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 sind, sondern vielmehr die Kontrollen, die ausgeführt werden. Dabei sorgt die in der Praxis oft noch fehlende Automatisierung für viel administrativen Aufwand. Microsoft Excel Sheets, E-Mails und manuelle Systemauswertungen dominieren noch erschreckend oft die IKS- und Revisionswelt, auch in großen Unternehmen.

Die Automatisierung eines IKS könnte Antworten auf viele Fragen geben, die heutzutage die Welt der Compliance beschäftigen:

- Wie lässt sich die Transformation von einem statischen IKS in Richtung eines integrierten und risikoorientierten GRC-Ansatzes bewerkstelligen?
- Können alle drei Verteidigungslinien integriert zusammenarbeiten?
- Lässt sich eine positive Risikokultur durch Tools fördern?
- Wie bringt man die operativen und revisionsspezifischen Sichten auf Kontrollmechanismen zusammen?
- Ist ein Realtime-Reporting über den Compliance-Stand auf Knopfdruck möglich?
- Wie kann man das IKS so abbilden, dass unterschiedliche Anforderungen von Risikomanagement, interner Revision, externer Jahresabschlussprüfung und branchenspezifischen Kontrollanforderungen effizient erfüllt werden?

Wie macht man es richtig?

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

- Integration zwischen Risiko-, IKS-, Richtlinien- und Revisionsmanagement
- gesetzliche Anforderungen und deren Auswirkung auf die heutige Welt der ERP-gestützten Prozesse
- Konzipierung und Aufbau eines IKS-Modells im IT-Umfeld
- Automatisierung eines IKS-Compliance-Prozesses
- Automatisierung der Test- und Überwachungsszenarien durch Integration
- unternehmensinterne IKS- und Compliance-Ziele bezüglich Effizienz, Wirtschaftlichkeit und Performance
- Umgang mit interner und externer Revision

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

Thema, Aufbau und Inhalt des Buches

Wachsende Anforderungen an Unternehmen

Die große Welle von gesetzlich getriebenen IKS-Projekten wurde Anfang der 2000er Jahre durch den Sarbanes-Oxley Act ausgelöst. Diese Welle hat auch in Europa alle in den USA börsennotierten Unternehmen erfasst. Auch in Europa wurde der Ruf nach mehr Transparenz und einer Risiko-

minimierung lauter. Das schlug sich in EU-Richtlinien und weiteren lokalen gesetzlichen Initiativen nieder. Der weltweite Trend zeigt insgesamt, dass ein funktionierendes IKS als eine staatlich geforderte Compliance-Anforderung rasch durchsetzt. Aktuell erleben wir, dass die voranschreitende Digitalisierung und »Cloudisierung« der Geschäftswelt verschärfte Datenschutzauflagen mit sich bringt.

Compliance als Teil von GRC

Das Thema Governance, Risk, and Compliance als einheitliches Konzept (man spricht von einem integrierten GRC-Ansatz) ist auf dem Markt längst angekommen, und das Berücksichtigen von allen drei Verteidigungslinien im Unternehmen spiegelt sich sowohl in den einschlägigen Softwarelösungen als auch in anerkannten Referenzmodellen und Standards wider. Das Thema Compliance kann somit nicht mehr isoliert betrachtet werden.

IKS im IT-Umfeld

In diesem Buch wird Compliance als ein im Rahmen eines IKS abgebildeter 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 den softwarespezifischen Applikationskontrollen im Rahmen der externen Revision, haben sich als Pflicht durchgesetzt. Die Antwort auf die Frage, was all dies für Unternehmen bedeutet, deren Prozesse SAP-ERP-gestützt ablaufen, muss klar strukturiert und beschrieben werden.

Konzept dieses Buches

Wie Sie es gesehen haben, gibt es zahlreiche Puzzleteile rund um die hochaktuellen Themen IKS und Compliance, die es zusammenzufügen gilt, um einen guten Überblick zu erhalten. Dieses Buch berücksichtigt die Verbindung von Compliance mit den weiteren Bestandteilen von GRC, soweit die Integrationssicht 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-Umfeldes betrachtet und konzeptionell in drei Schritten aufgearbeitet:

❶ vom Paragrafen zum Konzept

❷ vom Konzept zum Inhalt

❸ von Konzept und Inhalt zur Automatisierung

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

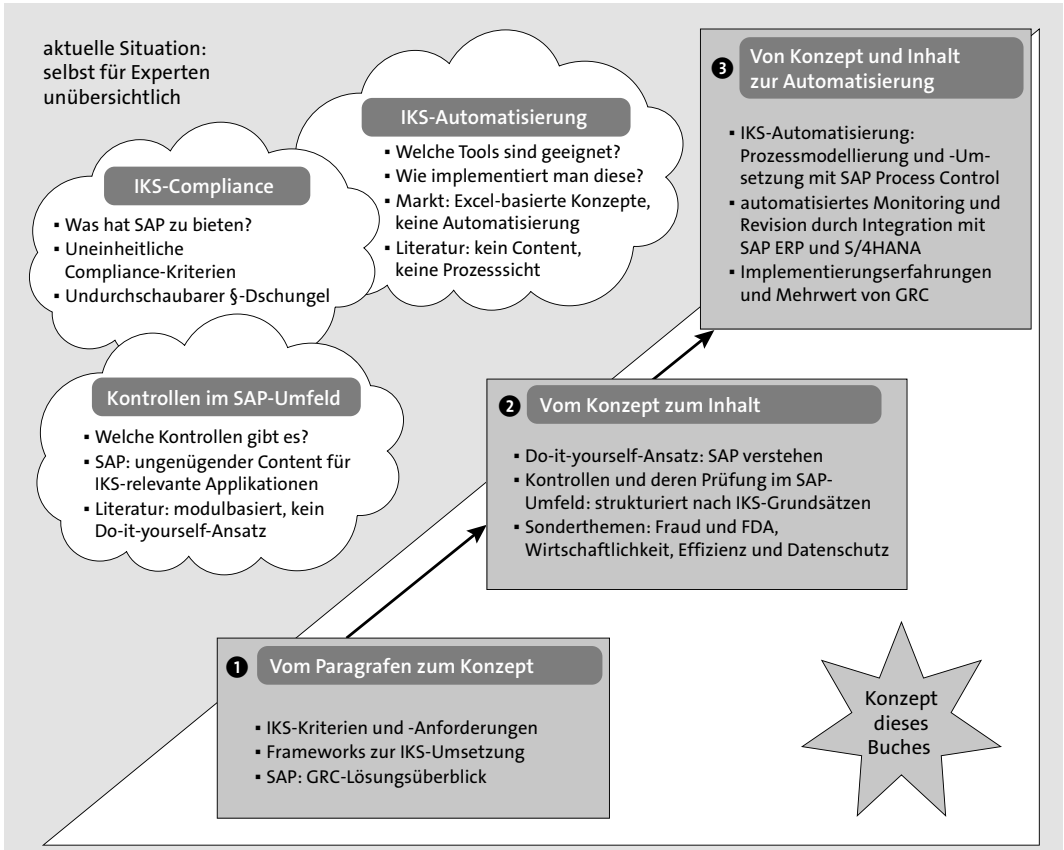

Abbildung 1 Konzept dieses Buches

Bei der vorliegenden dritten Auflage des Buches wurden folgende wesentlichen Anpassungen vorgenommen:

- Sie erhalten eine Delta-Übersicht zu Risk und Compliance in SAP S/4HANA sowie einen Einblick in die erweiterten Sicherheitsanforderungen rund um SAP Fiori und SAP HANA.
- Neu wird Unified Connectivity (UCON) samt Implementierungsschritten vorgestellt.
- Der Mehrwert von GRC, Hilfsmitteln und Erfolgsfaktoren bei der Implementierung von SAP GRC wurde neu aufgearbeitet.
- Alle Kapitel des Buches wurden überdies an die aktuellen gesetzlichen Anforderungen, ISO-Normen und Cloud-Spezifika angepasst sowie auf Release 12.0 der SAP-Lösungen für GRC aktualisiert.

TEIL I – Vom Paragrafen zum Konzept: Kontrollen in 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 SAP-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, Referenzmodelle und ISO-Standards Ihnen dabei behilflich sein können. Die Wichtigkeit des Continuous-Controls-Monitoring-Ansatzes wird dabei besonders hervorgehoben.
- **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 der Übersicht des SAP-GRC-Lösungsportfolios.

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. Themen wie Outsourcing und Cloud dürfen natürlich auch nicht fehlen.
- 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. Dabei wird die DSGVO vorgestellt und deren grundlegenden Prinzipien und Anforderungen beschrieben.
- **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 die 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.

- **Kapitel 15**, »Risk und Compliance in SAP S/4HANA«, geht auf die Neuerungen und Besonderheiten im Vergleich zu SAP ERP ein; dabei wird die Risk- und Compliance-Sicht hervorgehoben.
- **Kapitel 16**, »Berechtigungen in SAP S/4HANA«, bietet einen Einblick in die komplexer gewordene Welt der SAP-Sicherheit und geht dabei auf die drei Sichten ein: SAP Fiori, das S/4HANA-Backend sowie die SAP-HANA-Datenbank. Eine kurze Zusammenfassung der Migrationsschritte sowie die Darstellung der Auswirkungen auf die Funktionstrennungs-Anforderungen runden dieses Kapitel ab.
- **Kapitel 17**, »Unified Connectivity: Wirksamer Schutz der SAP-ERP-Umgebungen«, stellt die IKS-Vorteile von UCON vor und liefert eine ausführliche Anleitung zur Implementierung dieser Lösung. Es werden außerdem mehrere Verwendungsszenarien für UCON miteinander verglichen.

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

Compliance auf Knopfdruck ist ein realistisches Szenario. 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 der SAP GRC 12.0).

- In **Kapitel 18**, »IKS-Automatisierung: Wie bringt man den COSO-Cube ins Rollen?«, gehen wir auf die konzeptionelle Bedeutung der risikoorientierten IKS-Automatisierung ein und erläutern die einzelnen Bausteine, die bei der Modellierung der Automatisierung von IKS-Prozessen verwendet werden können.
- **Kapitel 19**, »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 Integrationsszenarien SAP Process Control als Bestandteil eines integrierten GRC-Ansatzes angesehen werden kann.
- In **Kapitel 20**, »Umsetzung von automatisierten Test- und Monitoring-Szenarien«, wird erläutert, welche Optionen – unter anderem die Integration von SAP Process Control mit Ihren SAP-ERP- und SAP-S/4HANA-Systemen – die große Vision eines »Tests auf Knopfdruck« ermöglichen. Sie werden Schritt für Schritt durch die Einrichtung des Continuous-Monitoring-Ansatzes in SAP Process Control 12.0 geleitet.

- In **Kapitel 21**, »SAP GRC – Erfolgsfaktoren und Erfahrungswerte«, wird der Nutzen von SAP GRC aus der Sicht von drei Verteidigungslinien dargestellt. Außerdem erfahren Sie, wie sich der Mehrwert von SAP GRC beurteilen lässt. Es werden Hilfsmittel und Erfolgsfaktoren für SAP-GRC-Implementierungen beschrieben.

An wen richtet sich dieses Buch?

Benötigte Vorkenntnisse

Welche Vorkenntnisse sollten Sie als Leser mitbringen? Während für Teil I, »Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld«, des Buches nur gesunder Menschenverstand und etwas betriebswirtschaftliches Grundwissen benötigt werden, ist 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 also?

- **Risikomanager**, **IKS-Verantwortliche**, **Mitarbeiter der internen Revision**, **externe Wirtschaftsprüfer**, **IT-Auditors**, **Compliance-Beauftragte**
  Das ist Ihr Buch – vom ersten bis zum letzten Kapitel!
- **SAP-Manager**, **Projektleiter**, **Datenschutzbeauftragte**, **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 geben insbesondere Teil I, »Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld«, und Teil II, »Vom Konzept zum Inhalt: Kontrollen in SAP ERP«, wichtige Hinweise für eine revisions- und IKS-konforme Gestaltung Ihrer Implementierungsprojekte und auch für den täglichen Betrieb der SAP ERP-Anwendungen.
- **SAP-Berater für die SAP-Lösungen für GRC**
  Teil III, »Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsystems«, 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, »Vom Konzept zum Inhalt: Kontrollen in SAP ERP«, 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-Spra-

che zu finden. Aus diesem Grund wäre für Sie auch Teil I, »Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld«, relevant.

- **MBA-, BWL- und Wirtschaftsinformatik-Studenten**
  Für Sie sind vor allem Teil I, »Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld«, und Teil II, »Vom Konzept zum Inhalt: Kontrollen in SAP ERP«, dieses Buches interessant: Teil I geht recht detailliert auf die gesetzlichen Anforderungen im internationalen Vergleich sowie auf die betriebswirtschaftliche Konzeption des IKS im IT-Umfeld ein. Die Übersicht über die international anerkannten GRC-Referenzmodelle könnte für Sie ebenfalls interessant sein. Teil III, »Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsystems«, können Sie entnehmen, was die Automatisierung von IKS konzeptionell bedeutet.
- **Senior-Management**
  Ob Sie in Ihrem Unternehmen CFO, CEO oder CIO sind oder Ihren Pflichten in Vorstand oder Prüfungsausschuss nachgehen – die Governance-, Risk- und 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, »Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsystems«, 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, »Vom Paragrafen zum Konzept: IKS und Compliance im ERP-Umfeld«, dieses Buches für Sie interessant sein. Die visionären und konzeptionellen Ausführungen zum Thema »Compliance auf Knopfdruck« in Teil III, »Von Konzept und Inhalt zur Umsetzung: Die Automatisierung eines Internen Kontrollsystems«, sollten Sie sich ebenfalls nicht entgehen lassen.

Hinweise zur Lektüre

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

Infokästen

In grauen Informationskästen sind Inhalte zu finden, die wissenswert 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:

- Die mit diesem Symbol gekennzeichneten **Tipps** und geben Ihnen spezielle Empfehlungen, die Ihnen die Arbeit erleichtern können. [+]
- Das Symbol **Hinweis** macht Sie auf Themen oder Bereiche aufmerksam, bei denen Sie besonders achtsam sein sollten. Sie finden in diesen Kästen auch Informationen zu weiterführenden Themen oder wichtigen Inhalten, die Sie sich merken sollten. [«]
- **Beispiele**, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen. [zB]

Marginalien

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.

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 dieses Buch neben meinen Hauptaufgaben bei der Riscomp GmbH und parallel zu spannenden Projekten verfasst habe, mussten mich meine Familie und Freunde 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 vereinzelten Fragestellungen gegeben: Großer Dank gebührt den SAP-Experten Frau Jan Gardiner, Herrn Marcel Hotz, Herrn Thomas Frenehard, Herrn Dr. Gero Mäder, Herrn Jürgen Möller, Herrn Dominik Yow-Sin-Cheung, Herrn Daniel Welzbacher und Herrn Jochen Thierer.

Hoch geschätzte Kollegen haben selbst Beiträge zu diesem Buch verfasst: Frau Moldir Abdikerim (Riscomp GmbH) hat mit ihrer Masterarbeit an der Queens University Belfast die Basis für die Aussagen bezüglich des Mehrwerts des IKS geliefert. Herr Christian Spiegelburg (Riscomp GmbH) hat bei der Erstellung von Screenshots für SAP GRC geholfen. Herr Vishal Padiyar

(Riscomp GmbH) hat das UCON-Kapitel beigesteuert. Herr Gerhard Wasnick hat mir während seiner Zeit bei der Riscomp GmbH bei der Beschreibung der Kontrollmechanismen in den SAP-ERP-gestützten Procure-to-Pay- und Order-to-Cash-Prozessen geholfen. Frau Maria Spöri, ebenfalls Ex-Riscomp-Kollegin, hat wesentlich zu dem SAP-S/4HANA-Berechtigungskapitel beigetragen. Alle erwähnten und einige weitere Kollegen haben nicht nur zu diesem Buch beigetragen, sondern auch zur Anerkennung der der Riscomp GmbH als SAP-Partner mit Recognized Expertise für GRC-Lösungen.

Herr Günther Emmenegger (SAP Schweiz AG) hat das Kapitel zur Abbildung der FDA-Anforderungen im SAP-Umfeld geschrieben. Herr Volker Lehnert (SAP SE) hat den größten Teil des Kapitels über DSGVO und datenschutzrelevante Kontrollen in SAP ERP HCM verfasst. Herr Marc Michely (PricewaterhouseCoopers) hat den Beitrag über Fraud-Szenarien in SAP beigesteuert. Herr Reto Bachmann (ABB) hat Ideen für den Beitrag über effizienzorientierte Szenarien geliefert. Herr Gerhard Jurasek (SAPPHIR IT & Management Training GmbH) hat mir bei einigen Ausführungen bezüglich SAP S/4HANA geholfen. Frau Jennifer Schmider (Xiting AG) hat mich mit einem fachlichen Review zu SAP-S/4HANA-Security-Themen unterstützt.

Acht Augen sehen mehr als zwei: Eva Tripp, Helene Bandholtz und Monika Klarl haben erste Entwürfe, Vor- und Rohfassungen sowie den fertigen Text gelesen und durch ihre Anmerkungen verbessert. Herzlichen Dank für Ihre kompetenten Hinweise, Ihre Geduld 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 GRC und IKS-Automatisierung mit SAP zu lösen, und wünsche Ihnen viel Erfolg und auch Freude bei der Lektüre.

Maxim Chuprunov

Auf einen Blick

Inhalt

17 Unified Connectivity: Wirksamer Schutz der SAP-ERP-Umgebungen 607

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