SAP PRESS

Handbuch SAP-Revision

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

Bearbeitet von
Maxim Chuprunov

erweitert 2012. Buch. 743 S. Hardcover
ISBN 978 3 8362 1928 0
Format (B x L): 16 x 24 cm

Maxim Chuprunov

Handbuch SAP®-Revision

Internes Kontrollsystem und GRC

Galileo Press

Bonn • Boston

Auf einen Blick

Inhalt

Vorwort

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

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

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

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

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

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

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

Annett Nowatzki
Vorstand der DSJ Revision und Treuhand AG, Berlin

Vertrauen ist gut, Kontrolle ist billiger: Einleitung

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

Warum Compliance?

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

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

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

Warum ist Compliance eine Herausforderung?

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

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

ner Jahresabschlussprüfung und branchenspezifische Kontrollanforderungen effizient erfüllt werden?

Wie macht man es richtig?

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

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

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

Thema, Aufbau und Inhalt des Buches

Immer mehr Anforderungen

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

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

IKS im IT-Umfeld

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

Compliance auf Knopfdruck

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

Konzept dieses Buches

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

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

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

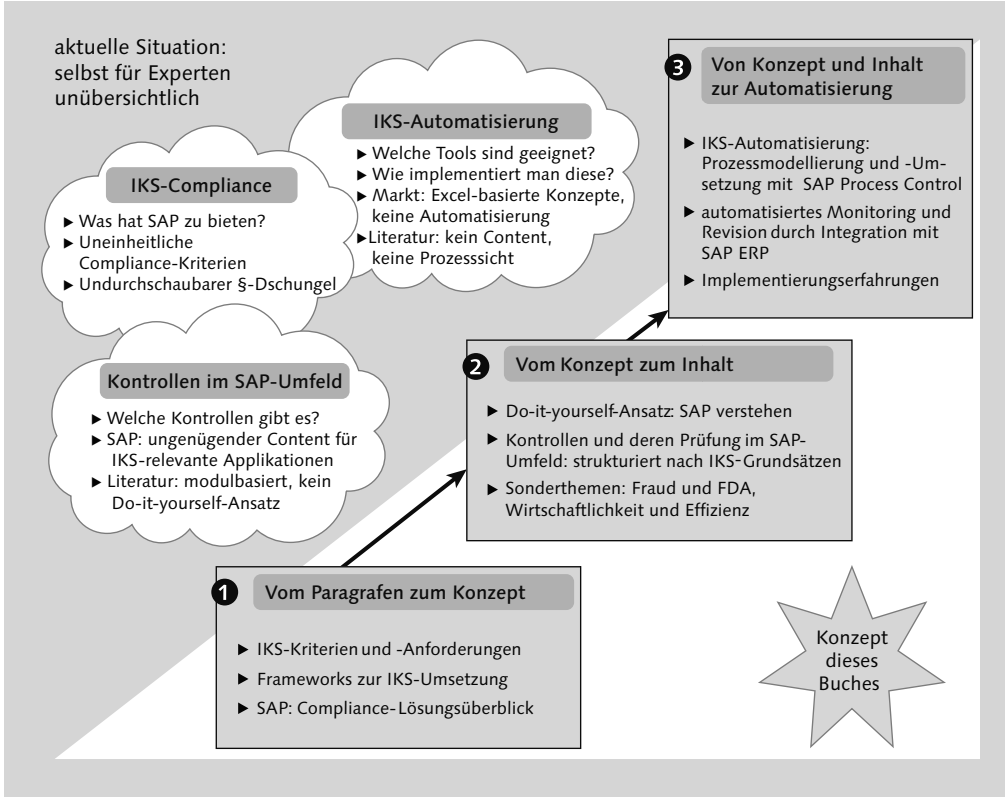

Abbildung 1 Konzept dieses Buches

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

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

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

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

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

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

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

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

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

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

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

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

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

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

An wen richtet sich dieses Buch?

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

An wen richtet sich dieses Buch?

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

- **Leiter von SAP Competence Centern, Projektleiter, Data Governance Experts, Business-Analysten und Berater für die SAP ERP-Implementierungen**
  Die Compliance-Anforderungen bei der Implementierung von SAP ERP zu berücksichtigen ist nicht einfach. Daher werden insbesondere Teil I und Teil II wichtige Hinweise für eine revisions- und IKS-konforme Gestaltung Ihrer Implementierungsprojekte und auch für den täglichen Betrieb der SAP ERP-Anwendungen geben.
- **SAP-Berater für die SAP-Lösungen für GRC**
  Teil III sollte Ihre obligatorische Lektüre werden. In Ihren Implementierungsprojekten, bei denen die Prozesssicht auf das IKS im Fokus steht, sollten Sie den Bezug zum IKS-Inhalt niemals verlieren: Aus diesem Grund ist auch Teil II wichtig für Sie. Und nicht zuletzt: Das Verständnis der komplexen Zusammenhänge zwischen gesetzlichen Anforderungen und deren Umsetzung im IT-Umfeld muss ebenfalls zu Ihrem Rüstzeug gehören, um mit Kunden eine gemeinsame Compliance-Sprache zu finden. Aus diesem Grund wäre für Sie auch Teil I relevant.
- **MBA-, BWL- und Wirtschaftsinformatik-Studenten**
  Für Sie sind vor allem Teil I und Teil II dieses Buches interessant: In Teil I gehe ich recht detailliert auf die gesetzlichen Anforderungen im internationalen Vergleich sowie auf die betriebswirtschaftliche Konzeption des IKS im IT-Umfeld ein. Die Übersicht über international anerkannte GRC-Referenzmodelle könnte für Sie ebenfalls interessant sein. Teil III können Sie entnehmen, was die Automatisierung von IKS konzeptionell bedeutet.
- **Senior Management**
  Ob Sie ein CFO, CEO oder CIO in einem Unternehmen sind oder Ihren Pflichten in Vorstand oder Prüfungsausschuss nachgehen – die Compliance-Fragestellungen haben Sie sicherlich nicht umgangen. Selbst wenn Prozesse in Ihrem Unternehmen nicht SAP-gestützt ablaufen und eine richtige Definition des SAP-spezifischen Inhalts Ihres IKS für Sie irrelevant ist, haben Sie sich sicherlich Gedanken über dessen effiziente Gestaltung gemacht: Erfahrungen anderer Unternehmen im Umgang mit den IKS- und Compliance-Themen in Teil III werden gute Anhaltspunkte für Sie liefern. Darüber hinaus werden die gesetzlichen und sonstigen Compliance-Anforderungen, Empfehlungen zum Umgang mit der

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

Hinweise zur Lektüre

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

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

Marginalien

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

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

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

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

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

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

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

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

Maxim Chuprunov

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

9.4 Kontrollen rund um das Thema Bestände

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

9.4.1 Pflege von Materialstammdaten

Wichtige Rolle der Materialstammdaten

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

Kontrollen rund um den Materialstamm

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

SAP Business Workflow

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

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

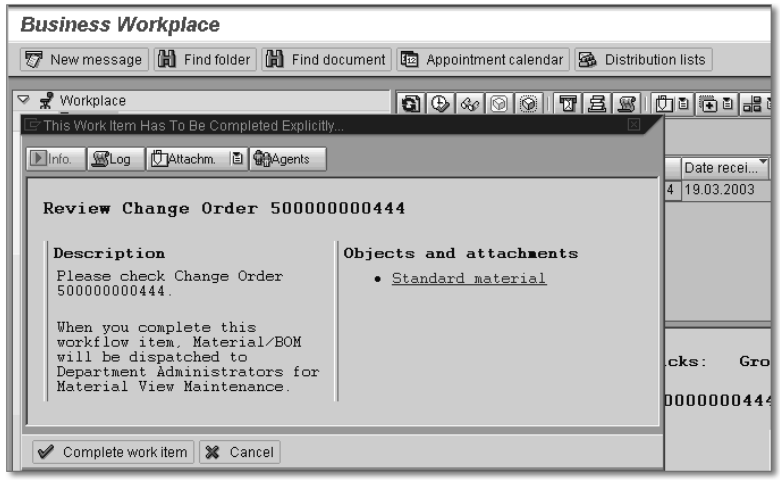

Abbildung 9.8 Änderungsauftrag für den Materialstamm

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

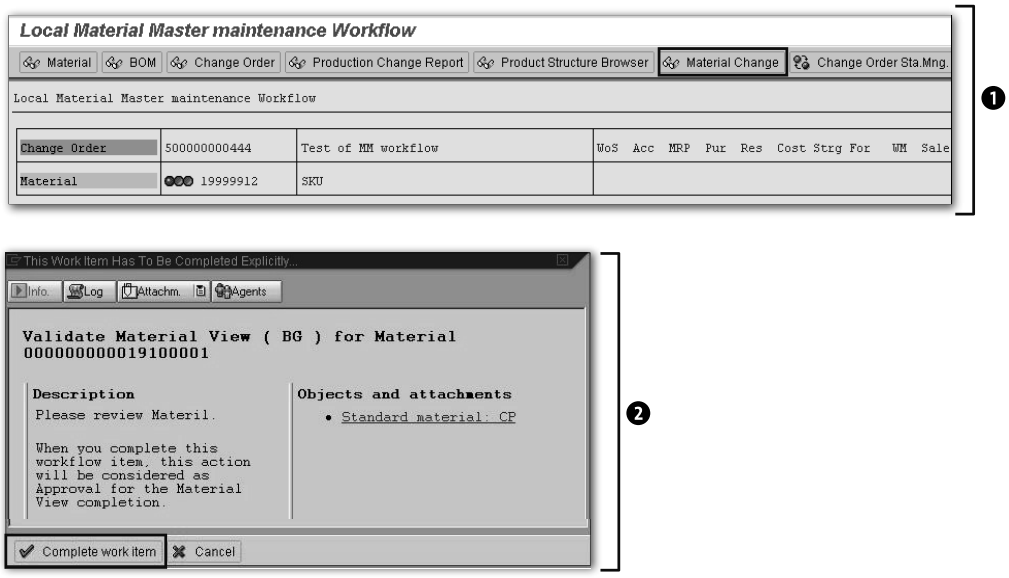

Abbildung 9.9 Workflowbasierte Bearbeitung von Materialstammdaten

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

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

Prüfung: Pflege Materialstammdaten

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

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

9.4.2 Unbewertetes Vorratsvermögen und getrennte Bewertung

Bewerteter vs. unbewerteter Bestand

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

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

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

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

Konfiguration zur Umklassifizierung des Bestandes

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

Handhabung der getrennten Bewertung

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

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

Konfiguration der getrennten Bewertung

Die Einstellung der getrennten Bewertung erfolgt im Customizing unter MATERIALWIRTSCHAFT • BEWERTUNG UND KONTIERUNG • GETRENNTE BEWERTUNG • GETRENNTE BEWERTUNG AKTIVIEREN/EINSTELLEN oder mithilfe der Transaktion OMW0/OMWC. Mithilfe dieser Konfigurationseinstellungen werden beispielsweise Bewertungstypen konfiguriert (ob ein Eigen- oder Fremdbezug vorliegt etc.).

Prüfung: Bewertung des Vorratsvermögens

Folgende Prüfungshandlungen sind im Zusammenhang mit der Materialbewertung zu empfehlen:

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

2. Die Aktivierung der Prüfung auf das Mindesthaltbarkeitsdatum im Rahmen der Chargenverwaltung kann in den Tabellen T159L und T156 überprüft werden.
3. Prüfen Sie die Einstellungen zur getrennten Bewertung von Vorratsvermögen im Customizing mit den Transaktionen OMW0 (MM-IV Steuerung Bewertung) und OMWC (MM-IV Getrennte Materialbewertung).

9.4.3 Kontenfindung bei Materialbewegungen

Materialbewegungen in SAP

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

Bewegungsarten und Kontenfindung

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

Konfiguration der Kontenfindung

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

- Bewertungssteuerung
- Bewertungskreis
- Bewertungsklasse
- Kontomodifikation

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

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

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

Prüfung: Kontenfindung bei Materialbewegungen

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

1. Verschaffen Sie sich einen Überblick über die Systemeinstellungen zur Kontenfindung, insbesondere der Kontomodifikation für Bewegungsarten, sowie über die Anbindung der Kontenpläne (Transaktion OMWD oder mithilfe der Fixkontentabelle T030).
2. Kontrollieren Sie in Stichproben die Kontierung der Bewegungsarten für wichtige Materialarten. Wählen Sie dazu die Transaktion OMWB (Simulation der Kontenfindung), und klicken Sie anschließend auf den Button Simulation oder Sachkonten.
3. Hinweis: Das Programm `RM07MMFI` führt einen Saldenabgleich zwischen der SAP-Materialwirtschaft und -Finanzbuchhaltung durch. Zusätzlich gleicht das Programm `RM07MBST` summarisch den Lagerbestand mit dem Bestandskonto in der Finanzbuchhaltung ab. Eine Konsistenzprüfung der Bestände sollte regelmäßig mithilfe des Programms `RM07KO01` durchgeführt werden.

9.4.4 Berichtigung des Vorratsvermögens: Inventur und Materialabwertungen

Werte anpassen – wann und warum?

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

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

Inventur

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

Inventurkontrolle: Sperre der Lagerorte

Um eine Abweichung durch Materialbewegungen während der Inventur zu verhindern, sollten während der Inventur die Bestände durch eine Sperre der Lagerorte fixiert werden. Diese Sperre kann im Customizing aktiviert werden (Materialwirtschaft • Bestandsführung und Inventur • Inventur • Buchbestand fixieren im Lagerort erlauben im Einführungsleitfaden).

Inventurkontrolle: Funktionstrennung

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

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

AHK-bezogene Wertberichtigung

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

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

Abwertung des Vorratsvermögens

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

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

- **Prüfungshandlungen zur Abwertung**
  Wichtige Parameter zur Berechnung der Niederstwertermittlung müssen zum Zeitpunkt des Programmstarts im Customizing richtig gesetzt sein:
  - Reichweitenabschläge bei der Niederstwertermittlung im Customizing (Transaktionen OMW5 und OMW5W)
  - Selektion der Beleg- und Bewegungsarten, die bei der Niederstwertermittlung nach Marktpreisen für die Berechnung der Zugangspreise berücksichtigt werden (Transaktion OMWI für Bewegungsarten/Transaktion OMWJ für Belegarten)
  - Abschlagswerte für die Niederstwertermittlung nach Gängigkeit (Transaktionen OMW5 und OMW5W)
  - Bewertungsebene für LIFO/FIFO (Transaktion OMWL) sowie die Definition der LIFO/FIFO-relevanten Bewegungsarten
- **Kontrollen zur Funktionstrennung**
  Zusätzlich sollte eine angemessene Funktionstrennung sichergestellt sein. SAP ermöglicht die Erstellung einer Batch-Input-Mappe sowie die direkte Aktualisierung der Bewertungspreise im Materialstamm. Eine angemessene Funktionstrennung kann auf zwei unterschiedliche Arten erreicht werden.
  - *Präventive Kontrolle*
    Die Wertberichtigung wird ausschließlich mithilfe der Batch-Input-Mappe durchgeführt. Der Benutzer, der die Bewertung

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

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

Wichtig für die Transaktion CKMPCD **[!]**

Wählen Sie die Option Belegpositionen pro Material aus, anderenfalls werden die Wertänderungen nicht ausgegeben.

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

Prüfung: Berichtigung des Vorratsvermögens

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

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

9.4.5 Freigabe von Verschrottungen

IKS-konform Bestände ausbuchen

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

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

Kontrolle: Kritische Bewegungsarten

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

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

Prüfung: Freigabe von Verschrottungen

Bezüglich der Behandlung der Verschrottungen prüfen Sie Folgendes:

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

9.4.6 Produktkostenrechnung

Wertefluss für Eigenerzeugnisse in SAP

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

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

Eigenschaften von Auflagen

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

Begriffe »Auflage« und »Compliance-Initiative«

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

Technische Details und Konfiguration

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

Neue Auflage anlegen

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

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

16.4 Implementierung des IKS-Prozesses

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

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

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

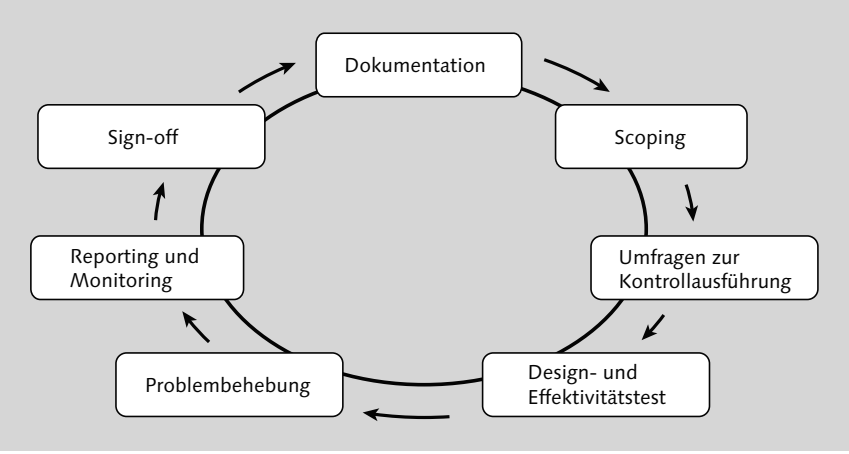

Abbildung 16.14 IKS-Zyklus – vereinfachte Darstellung

16.4.1 IKS-Dokumentationsprozess

Betriebswirtschaftliche Sicht

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

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

Pflege im zentralen Katalog

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

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

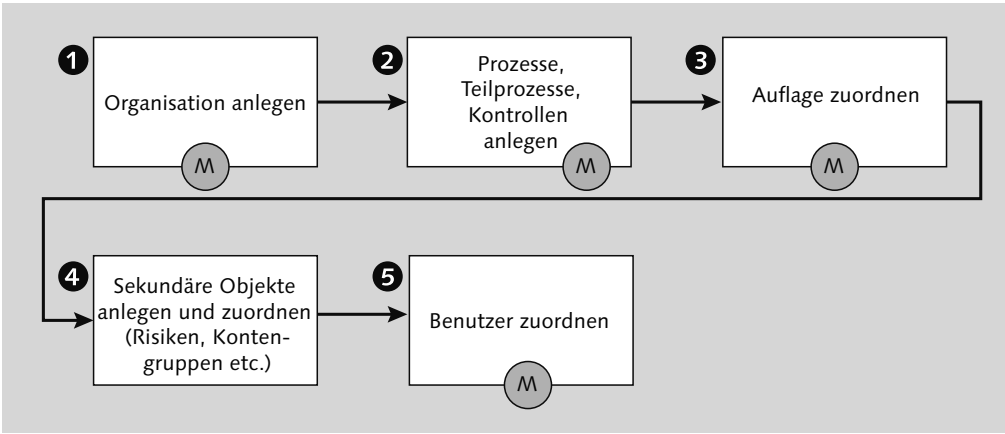

Abbildung 16.15 Ablauf der IKS-Stammdatenpflege

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

Technische Details und Konfiguration

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

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

Betriebswirtschaftliche Sicht

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

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

Vier-Augen-Prinzip bei der Kontrolldokumentation [zB]

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

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

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

Technische Details und Konfiguration

Um die beschriebenen Optionen zu ermöglichen, müssen Workflows für Stammdatenänderungen aktiviert sein. Dies nehmen Sie im Einführungsleitfaden über den Pfad GRC • Gemeinsame Stammdateneinstellungen • Workflow für Stammdatenänderungen aktivieren vor.

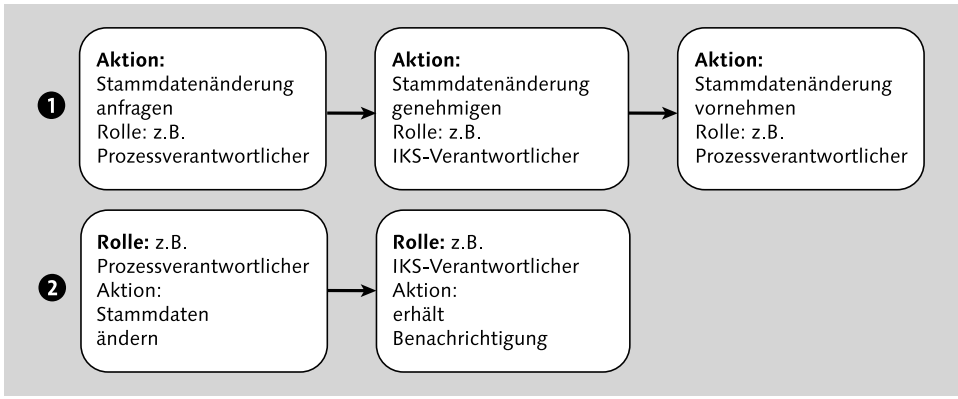

Abbildung 16.16 Zwei Optionen zur Abbildung des Vier-Augen-Prinzips

Zentralisierte vs. dezentralisierte Dokumentation des IKS

Betriebswirtschaftliche Sicht

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

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

[+] **FEI-Survey-Ergebnisse**

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

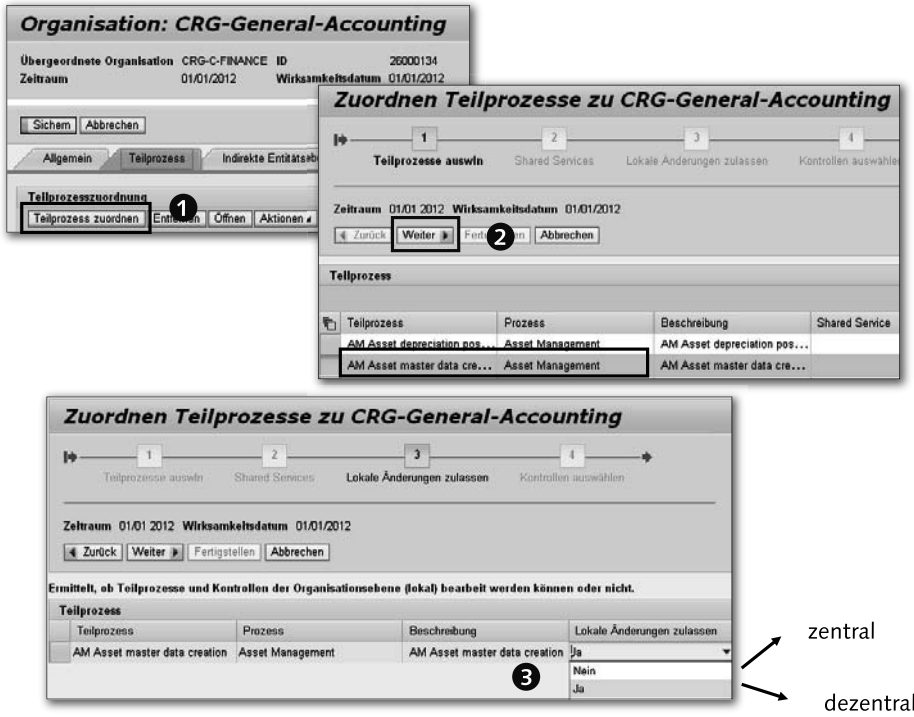

Abbildung 16.17 Voraussetzungen für die Realisierung eines zentralisierten vs. dezentralisierten Ansatzes bei der Stammdatenverwaltung

Optionen bei der Zuordnung von Subprozessen

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

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

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

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

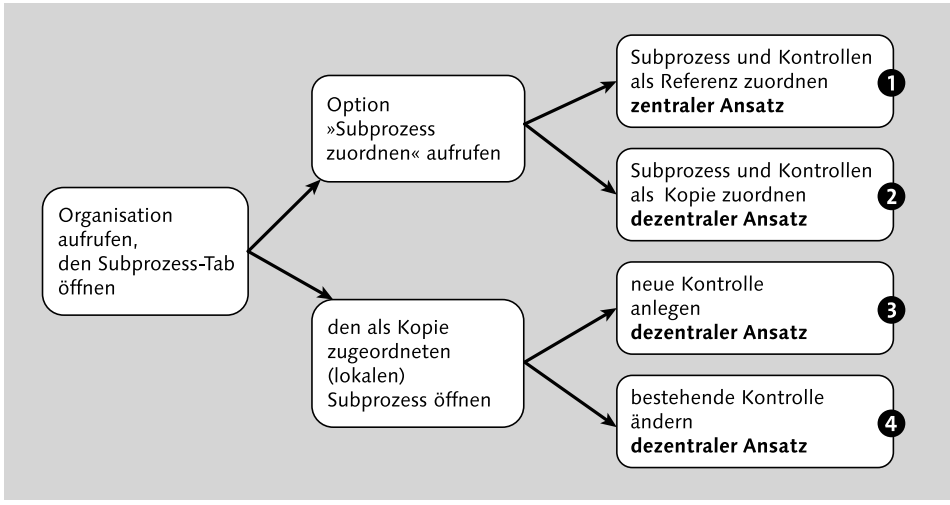

Abbildung 16.18 Zentralisierter vs. dezentralisierter IKS-Dokumentationsansatz in Aktion

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

Shared-Services-Konzept im IKS

Betriebswirtschaftliche Sicht

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

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

[zB] **Outsourcing oder zentralisierte Dienstleistungen**

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

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

[zB] **IT-General-Controls-Szenario**

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

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

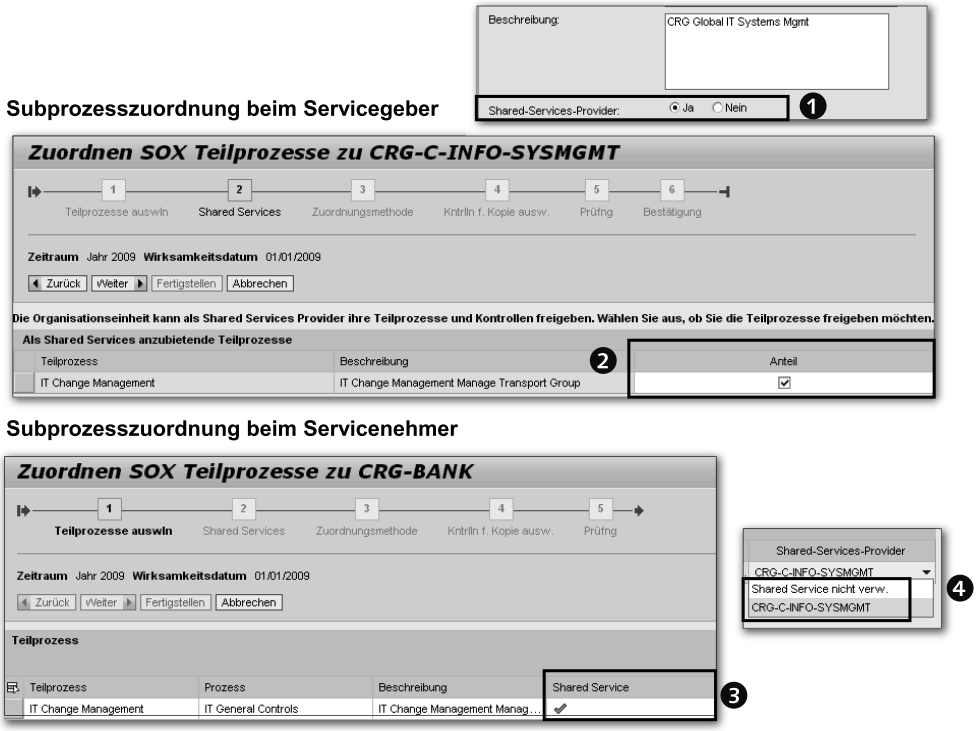

Abbildung 16.19 Abbildung des Shared-Services-Szenarios

Voraussetzungen

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

- Die Auswahl der entsprechenden Option muss in einer Servicegeber-Organisation ❶ getroffen werden.
- Des Weiteren müssen die in der Servicegeber-Organisation verwendeten Subprozesse für die Wiederverwendung von den Servicenehmer-Organisationen freigegeben sein ❷.
- Bei der Zuordnung von Subprozessen zu einer Servicenehmer-Organisation werden die freigegebenen Subprozesse als solche gekennzeichnet ❸.
- Im weiteren Schritt ❹ ist die Servicegeber-Organisation in einer Drop-down-Liste auszuwählen.

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

16.4.2 Scoping-Prozess

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

Wesentlichkeitsbasierter Scoping-Prozess

Betriebswirtschaftliche Sicht

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

Kontengruppen in SAP Process Control

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

Zwei Optionen

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

- Konsolidierte Salden (Consolidated Balances and Significance)
- Organisationsbilanzen (Organization-Level Balances and Significance)

Durchführung

Bei beiden Scoping-Optionen müssen folgende Schritte durchgeführt werden:

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

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

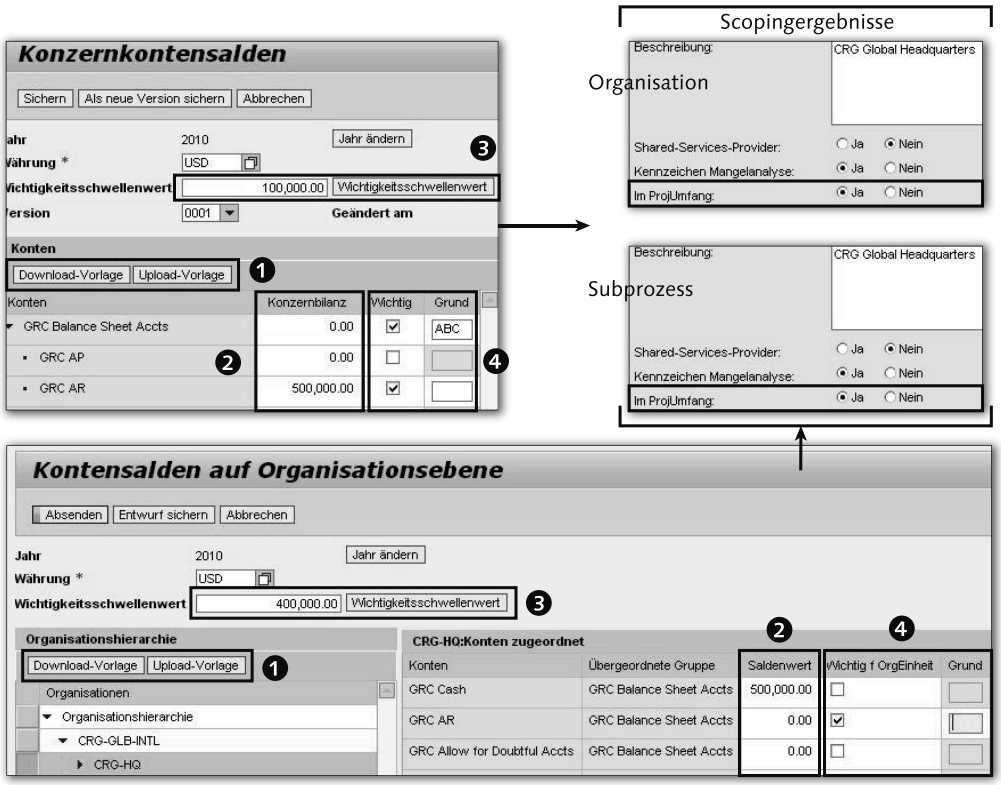

Abbildung 16.20 Wesentlichkeitsbasierter Scoping-Prozess

Unterschied der Optionen

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

Risikobasierter Scoping-Prozess

Workflowbasierte Risikobeurteilung

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

- qualitative Bewertung der Risiken
- Risikoeinstufung von Kontrollen

Szenarien

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

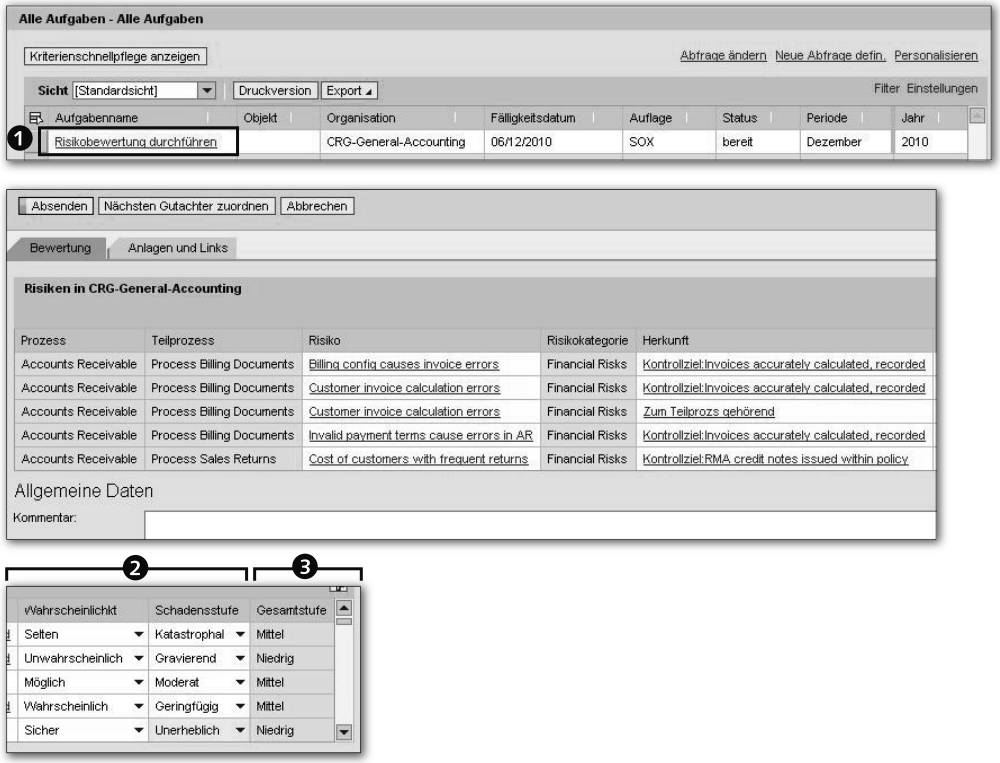

Abbildung 16.21 Risikobewertung als Teil des Scoping-Prozesses

Qualitative Bewertung der Risiken

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

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

Gültigkeit der Bewertungsergebnisse **[+]**

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

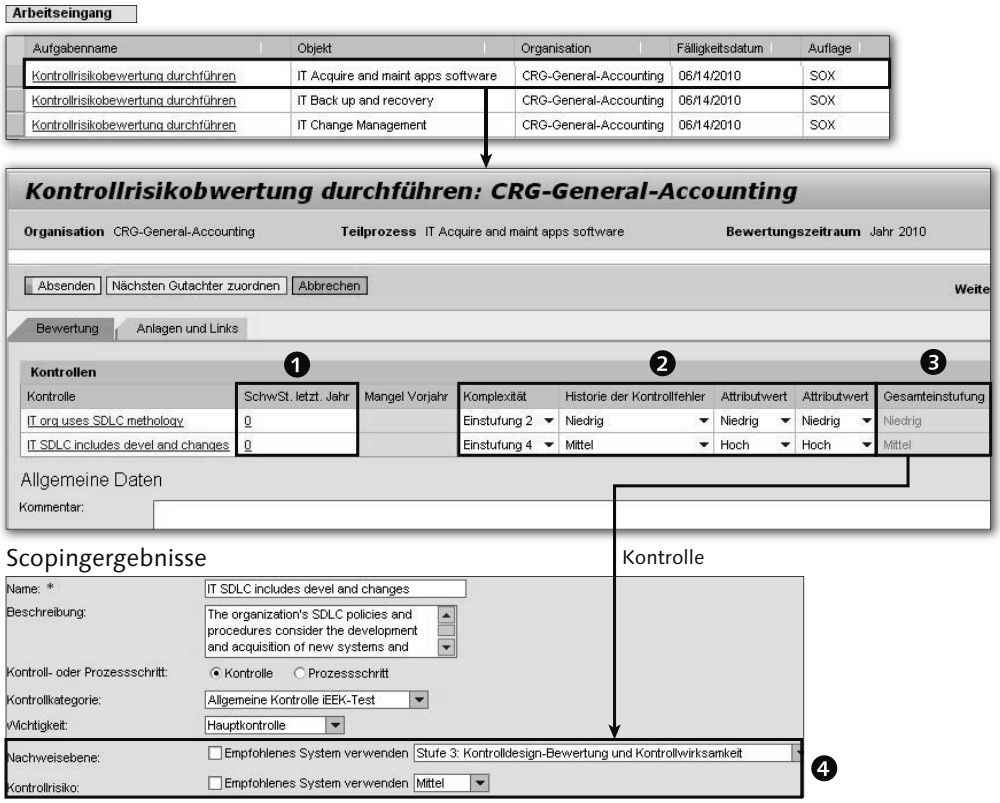

Abbildung 16.22 Kontrollrisikobewertung als Teil des Scoping-Prozesses

Risikoeinstufung von Kontrollen

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

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

Vergleich

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

Ableitung der kombinierten Risikobewertungsergebnisse

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

16.4.3 Planungsprozess, Tests und Bewertungen

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

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

Harmonisierter Planer in Release 10.0

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

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z