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.

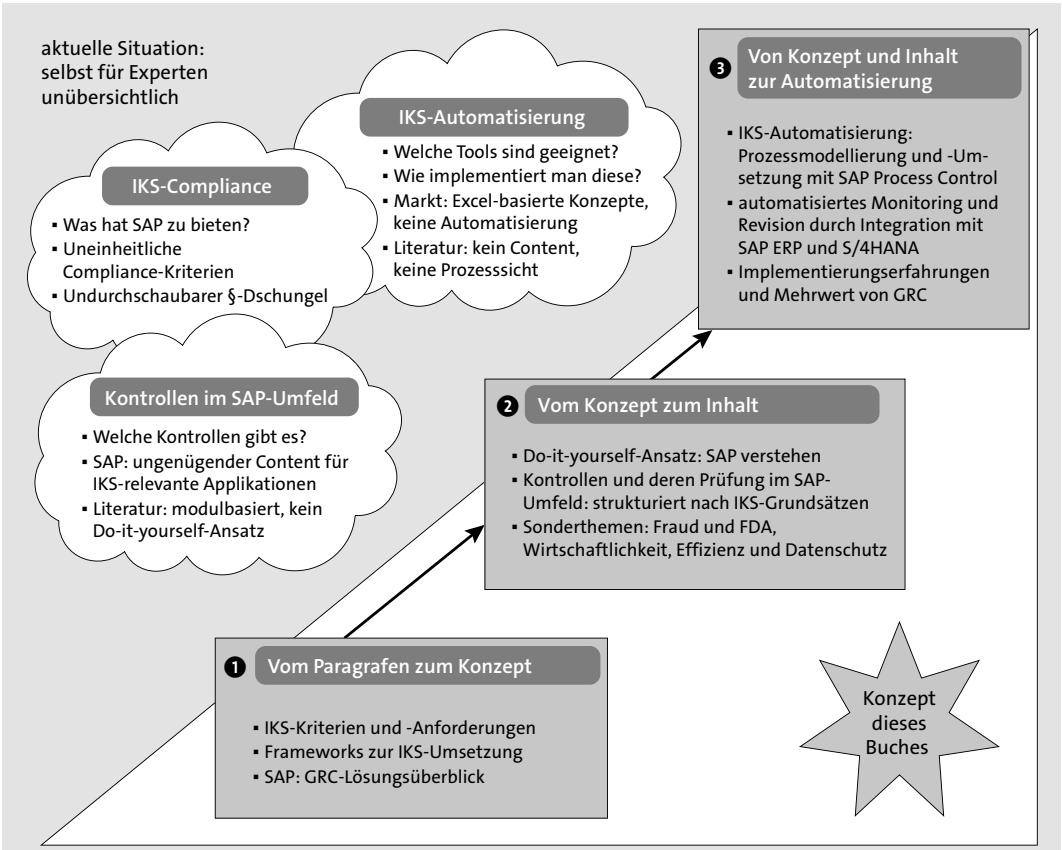


Abbildung 1 Konzept dieses Buches

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.

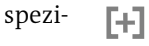
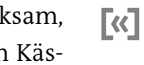
Hinweise zur Lektüre

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. 

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