KPMG
cutting through complexity

Compliance im Finanzsektor

2. Auflage

Herausforderungen und Lösungswege für Versicherungen

Inhalt

Regulatorische Entwicklungen im Versicherungsumfeld	4
Compliance Management System	6
Geldwäscheprävention	8
Finanzsanktionen und Embargos	10
Fraud Risk Management	14
Antikorruption	16
Effiziente Performance der Compliance IT-Anwendungen für Ihr Unternehmen	18
Vertriebs-Compliance-System	20
Automatischer Austausch von Steuerdaten – Automatic Exchange of Information (AEOI)	22
Compliance Due Diligence	25

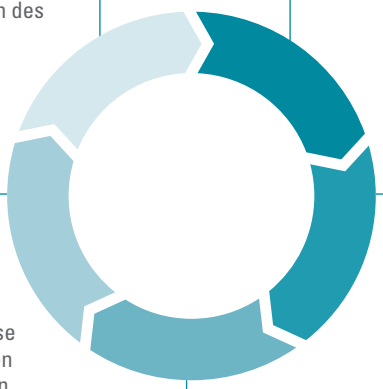
Regulatorische Entwicklungen im Versicherungsumfeld

Versicherer sehen sich gegenwärtig mit an Zahl und Komplexität stetig zunehmenden externen Regelwerken und neuen Marktstandards konfrontiert.

Das ab dem 1. Januar 2016 vollständig anzuwendende Solvency-II-Regelwerk sieht erstmalig die Etablierung einer Compliance-Funktion als integralen Bestandteil des Internen Kontrollsystems und damit des Governance-Systems von Versicherungen vor.

Diese abstrakten Anforderungen werden anhand einer Durchführungsverordnung sowie durch Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkretisiert.

Regelkreis der wesentlichen Anforderungen an die Compliance-Funktion von Versicherungen



Beobachtung des Rechtsumfelds
Implementierung einer laufenden Beobachtung von Änderungen des Rechtsumfelds

Risikoidentifizierung und -beurteilung
Einschätzung von rechtlichen Anforderungen zur Bestimmung des Compliance-Risikos (auch als Wesentlichkeitsanalyse bezeichnet) zur Ausgestaltung der Tätigkeiten der Compliance-Funktion (Compliance-Plan)

Festlegung von Verantwortlichkeiten in Abstimmung mit den Fachbereichen
Ausgestaltung des Hinwirkens auf die Implementierung angemessener und wirksamer interner Verfahren; Beratungsaufgabe und Festlegung von Verantwortlichkeiten

Beurteilung der Angemessenheit und Wirksamkeit/ Überwachungshandlungen
Beurteilung der Angemessenheit und Wirksamkeit der eingeführten Verfahren auf Basis des identifizierten Compliance-Risikos; Durchführung von Überwachungshandlungen; Ableitung von Maßnahmen

Berichterstattung
Regelmäßige Berichte über Compliance-Themen, Compliance-Risiken, Angemessenheit und Wirksamkeit der Verfahren und Erkenntnisse aus Überwachungshandlungen sowie Rechtsänderungsrisiken

Insbesondere die BaFin-Verlautbarung vom 3. Dezember 2014 stellt neben der Analyse von Compliance-Risiken folgende Themenfelder in den Mittelpunkt:

- Aufbauorganisation
- unabhängige Aufgabenerfüllung
- uneingeschränkter Informationszugriff und aktive Informationspflicht
- Überwachung der Einhaltung aller externen Anforderungen und internen Vorgaben
- Compliance-Leitlinien
- Beurteilung der Angemessenheit und Wirksamkeit eingeführter Verfahren und Hinwirken auf Einführung wirksamer Verfahren
- Beratungsaufgabe
- Trendbeobachtung des Rechtsumfelds und Beurteilung möglicher Auswirkungen von Änderungen
- Compliance-Planung
- Berichterstattung

Inhaltlich rückt der Vertrieb von Versicherungsprodukten immer stärker in den Fokus von Compliance. Insbesondere der vom Gesamtverband der deutschen Versicherungswirtschaft im Sinne einer Selbstverpflichtung überarbeitete Kodex für den Vertrieb von Versicherungsprodukten postuliert in Leitsatz 3 deutliche Anforderungen an die Compliance von Versicherungsunternehmen. Dabei ist es nicht ausreichend, Leitlinien zum Umgang mit Geschenken und Zuwendungen oder zur Handhabung von Interessenkonflikten zu verabschieden. Maßgeblich sind vielmehr die prozessuale Umsetzung im Unternehmen und die Überwachung der Einhaltung solcher Vorgaben.

Aber auch auf internationaler Ebene zeichnet sich mit Verabschiedung des Abkommens zum Automatic Exchange of Information (AEOI) im Juli 2014 ein weiterer Standard ab, der hohe Anforderungen an das steuerliche Meldewesen für Versicherer festlegt.

Zur umfassenden Herangehensweise von KPMG bei der Beratung zu Compliance-Fragen zählen folgende Maßnahmen:

- Entwicklung eines Zielbilds für die Compliance-Funktion nach Solvency II
- Konzeption und Durchführung einer Analyse zur Identifizierung der maßgeblichen rechtlichen Anforderungen und ihrer Compliance-Risiken
- Definition und Umsetzung eines Prozesses für ein regulatorisches Monitoring
- Ausgestaltung der sogenannten Hinwirkungspflicht
- Konzeption eines Prozesses zur regelmäßigen Feststellung der Angemessenheit und Wirksamkeit implementierter Maßnahmen
- Entwicklung und Implementierung einer ganzheitlichen Compliance-Berichterstattung
- Unterstützung bei der gruppenweiten Umsetzung der Anforderungen
- Ausgestaltung der Compliance-Leitlinie und des Compliance-Plans

Compliance Management System

Die Regulierungsintensität der Versicherungsbranche nimmt stetig zu – mit der Folge, dass Compliance immer bedeutsamer wird. Die Compliance Management System (CMS)-Methodik von KPMG zeigt auf, wie Sie den vielfältigen Compliance-Anforderungen effizient und umfassend begegnen können.

Die Vorgaben aus Solvency II, VAG, IDW PS 980, ISO 19600 und aus den Branchenstandards des GDV formen ein komplexes Gebilde aus unter anderem rechtlichen Anforderungen, die an die Compliance-Funktion – als Schlüsselfunktion im Governance-System einer Versicherung – gerichtet werden.

KPMG begegnet diesen Anforderungen mit einem integrierten Lösungsansatz, der das Ziel der präventiven Sicherstellung der Compliance-Konformität verfolgt. Diese von KPMG entwickelte CMS-Methodik gestaltet die Grundelemente des CMS im Sinne des IDW PS 980 in Wechselwirkungen mit den weiteren externen (Solvency II, VAG et cetera) und internen Anforderungen (unter anderem Unternehmensstandards und Selbstverpflichtungen) aus.

Kultur und Ziele

Im Mittelpunkt steht die Etablierung einer Compliance-Kultur, die durch ein Bewusstsein für die Thematik bei Mitarbeitern und Management geschaffen wird. Die Kultur des Unternehmens und das Verhalten des Managements sind wesentliche Eckpfeiler des CMS. Hierzu sind zum einen die Ziele der Compliance-Funktion zu definieren, um die Ausrichtung des CMS zu gestalten. Dabei werden neben der Bestimmung der relevanten Teilrechtsgebiete auch die von dem System erfassten Organisationsbereiche und Regeln definiert. Zum anderen bilden die Ziele die Grundlage der Compliance-Risiken und grenzen gleichzeitig die Kompetenzen und Funktionsweisen gegenüber anderen Governance-Funktionen ab.

Organisation

Aufbauend auf den Zielen erfolgen die Definition von Rollen und Verantwortlichkeiten der Compliance-Funktion, die Etablierung der Compliance-Strukturen und die Gestaltung der Prozesse der Ablauforganisation.

Risiken

Ein CMS verlangt die kontinuierliche und systematische Identifizierung und Analyse von Compliance-Risiken. Die unternehmensweite Compliance-Risikoanalyse ermöglicht eine regelmäßige Identifizierung und Analyse der relevanten Risiken sowie der damit einhergehenden Präventions- und Handlungsmaßnahmen.

Programm

Das Compliance-Programm umfasst die an den vorhandenen Risiken orientierten Maßnahmen zur Vermeidung von Compliance-Verstößen und demzufolge zur Minimierung von Compliance-Risiken. Darunter fallen Richtlinien (einschließlich Verhaltenskodizes), Kontrollmechanismen und Schulungen. Zudem werden in einem solchen Programm Maßnahmen festgelegt, die bei gegebenenfalls festgestellten Verstößen zu ergreifen sind. In diesem Zusammenhang sind zum Beispiel Reporting-Konzepte, Kommunikationsmethoden und Sanktionssysteme zu nennen.

Kommunikation

Ferner sind die Durchführung von Compliance-Schulungsprogrammen und die Anwendung effizienter Kommunikationsmethoden erforderlich. Ein risikobasiertes Compliance-Berichtswesen rundet die Kommunikation ab.

Überwachung und Verbesserung

Ein übergreifendes Compliance Monitoring bewertet die Wirksamkeit und Angemessenheit des CMS. Zudem ist die Compliance-Funktion aufgefordert, neue Trends sowie regulatorische Anforderungen zu identifizieren und die Auswirkungen auf das CMS zu bewerten.

Aufgrund der zahlreichen – miteinander in Wechselwirkung stehenden – Anforderungen ist die Etablierung eines wirkungsvollen und verlässlichen CMS ein komplexes Unterfangen.

KPMG unterstützt Sie diesbezüglich gern bei der auf Ihr Versicherungsunternehmen zugeschnittenen Implementierung eines solchen Systems, wobei vorhandene Organisationsstrukturen und Prozesse Berücksichtigung finden.

Die Anforderungen an die Bekämpfung von Geldwäsche und Terrorismusfinanzierung nehmen stetig zu. KPMG unterstützt Sie dabei, die in diesem Bereich geltenden Normen und Regelwerke einzuhalten.

Geldwäscheprävention

Die Umsetzung der gesetzlichen und aufsichtsrechtlichen Vorgaben zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung bringt für Versicherungsunternehmen angesichts der Komplexität der Anforderungen besondere Herausforderungen mit sich. Gefordert sind insbesondere:

- Erstellung und Aktualisierung der jährlich durchzuführenden Gefährdungsanalyse
- Überwachung der Geschäftsbeziehungen und Zahlungen – gegebenenfalls durch den Einsatz angemessener Datenverarbeitungssysteme
- Erstellung individueller Risikoprofile der Vertragspartner und eine darauf basierende Datenaktualisierung
- Feststellung und Überprüfung der wirtschaftlich Berechtigten und Bezugsberechtigten
- Untersuchung jeder einzelnen Geschäftsbeziehung oder Zahlung, die als zweifelhaft oder ungewöhnlich anzusehen ist
- gruppenweite Einhaltung von Sorgfaltspflichten

Wesentliche Voraussetzung für eine wirksame Prävention ist ein unternehmensübergreifender iterativer Prozess. Die Informationsgewinnung bildet hierbei die Grundlage für die Erstellung eines entsprechenden Risikoprofils eines Vertragspartners. Besonders wichtig ist in diesem Zusammenhang, dass die verschiedenen Unternehmenseinheiten und die jeweils eingesetzten Datenverarbeitungssysteme optimal aufeinander abgestimmt sind. Auf dieser Basis müssen anschließend entsprechende Maßnahmen, zum Beispiel Genehmigungsprozesse und die risikobasierte Überwachung, durchgeführt werden.

Die Gefährdungsanalyse erfasst die Gesamtheit der Geldwäscherisiken eines Unternehmens und bewertet dessen Geschäftsbeziehungen. Insbesondere daraus leiten sich die Prozesse ab, die von den betroffenen Unternehmenseinheiten umzusetzen sind. Im Rahmen des Risikomanagements ist für die gesamte Gruppe ein einheitliches Zielbild zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu etablieren, dessen Umsetzung in der Folge zu koordinieren und gruppenweit zu überwachen ist.

KPMG unterstützt Sie bei der Umsetzung der gesetzlichen und aufsichtsrechtlichen Vorgaben in Ihrem Unternehmen. Neben Gesetzeskonformität fokussieren wir dabei vor allem eine praktikable Umsetzung, die Ihre spezifischen Anforderungen berücksichtigt.

Finanzsanktionen und Embargos

Finanzsanktionen und Embargos sind ein oftmals genutztes politisches Druckmittel, Regierungen eines Staates zu einem gewissen Handeln zu bewegen. Von der Umsetzung der einschlägigen Vorschriften sind auch Versicherungs- und Rückversicherungsunternehmen betroffen, die wirksame Sicherungsmaßnahmen implementieren müssen. Bei Verstößen drohen den Unternehmen und handelnden Personen empfindliche Strafen.

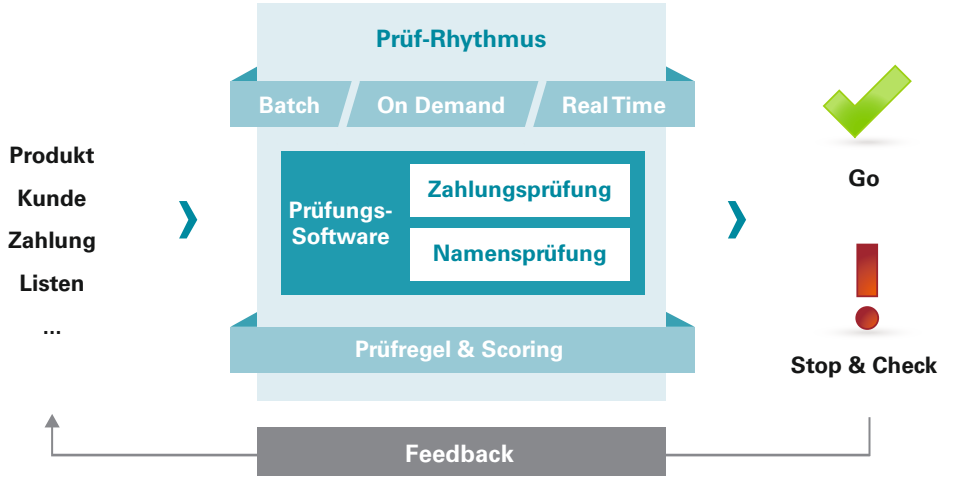
Das Aussprechen von Finanzsanktionen und Embargos erfolgt zumeist aus politischen Gründen, wenn gegen Diktaturen, deren Repressionen gegen Bevölkerungsgruppen und Länder oder auch gegen Akteure des internationalen Terrorismus vorgegangen werden soll. Ein solches Vorgehen verfolgt zumeist das Ziel, dass derartige Personen, Gruppen oder Organisationen weder direkt noch indirekt auf finanzielle und andere wirtschaftliche Ressourcen Zugriff erhalten.

In den vergangenen Jahren sind Versicherungs- und Rückversicherungsunternehmen in den einschlägigen Verordnungen explizit zur Einhaltung der Vorgaben angehalten worden. Somit rücken Versicherungs- und Rückversicherungsunternehmen immer mehr in den Fokus der Aufsichtsbehörden und sind verpflichtet, die Versicherung von Waren und Dienstleistungen sowie Geldtransfers auf vorliegende Verbote zu prüfen, Verträge einzufrieren und Meldungen an die zuständigen Behörden zu versenden.

Für Versicherungs- und Rückversicherungsinstitute im europäischen Raum sind die Sanktionsbestimmungen der EU maßgeblich. Institute mit wirtschaftlichen Beziehungen in die USA müssen neben den EU-Vorgaben zudem die Vorschriften des US-amerikanischen Office of Foreign Assets Control (OFAC) berücksichtigen.

Verstöße gegen die Sanktionsbestimmungen werden von den Aufsichtsbehörden mit teilweise erheblichen Geldstrafen belegt. Zusätzlich drohen betroffenen Unternehmen politische Folgen, hohe Aufwände zur Wiederherstellung der Reputation, Geschäftseinbußen und das Abwandern von Kunden zu Konkurrenzunternehmen.

Prüfung von Datenmengen durch spezielle Screening Software



KPMG unterstützt Sie bei der Umsetzung der Anforderungen, die sich aus Vorgaben der EU, der Vereinten Nationen und gegebenenfalls des OFAC ergeben, anhand von prüfungssicheren und dennoch effizienten Prozessen, die einen bestmöglichen Schutz gegen Verstöße bieten, ohne dabei eine Störung des Kerngeschäfts zu verursachen.

Die Implementierung effizienter und risikoorientierter Maßnahmen zur Einhaltung der Vorschriften erfordert zunächst die Identifizierung der relevanten Anforderungen und ihrer Auswirkungen. Im Fokus steht dabei, ein höchstmögliches Maß an Rechtssicherheit der handelnden Personen sowie die Organisationssicherheit im Unternehmen sicherzustellen. Folgende Geschäftsvorgänge sollten vor allem berücksichtigt werden:

- neubegründete und laufende Geschäftsbeziehungen
- Versicherung und Rückversicherung kritischer Grundgeschäfte und Vertragsgegenstände
- Auszahlung bei Schadensfällen
- nationale und internationale Abwicklung des Abrechnungsverkehrs
- Kapitalanlage und Handel mit Finanzinstrumenten

Damit die Prüfung dieser Geschäftsvorgänge auf Finanzsanktions- und Embargovorgaben durch effiziente und risikoadäquate Prozesse abgebildet werden kann, ist eine lückenlose Aufnahme der relevanten Informationen über den jeweiligen Vertragspartner und die betreffenden Vertragsgegenstände im Rahmen der Kundenannahme unerlässlich.

Im weiteren Verlauf empfiehlt sich der Einsatz einer speziellen Prüfsoftware. Auf diese Weise ist es möglich, größere Datenmengen zügig hinsichtlich der relevanten Sanktionslisten zu prüfen und gegebenenfalls Anknüpfungspunkte im Hinblick auf vorliegende Embargos zu erkennen. Die Anwendung präzise formulierter Arbeitsanweisungen und Leitlinien sowie die Durchführung regelmäßiger Schulungen der betroffenen Mitarbeiter sorgen für weitere Sicherheit in Prozessen, die nicht durch eine technische Prüfung abgedeckt werden können.

Darüber hinaus sollten die Institute und Unternehmen über eine effektive Organisation, insbesondere eine eindeutige Zuständigkeit und Verantwortung der Ansprechpartner und Entscheidungsträger, aber idealerweise auch über entsprechend eingestellte IT-Systeme verfügen, sodass sie bei Auffälligkeiten und Verdachtsmomenten sicher agieren können.

Die Einhaltung nationaler und internationaler regulatorischer Vorschriften dient dem Schutz des weltweiten Finanzsystems und trägt dazu bei, strafrechtliche Konsequenzen, Sanktionen und Reputationsschäden für alle Beteiligten zu vermeiden.

Fraud Risk Management

Eine frühzeitige Identifizierung von Fraud-Risiken wie auch die aktive und effiziente Gestaltung adäquater Gegenmaßnahmen sind wichtige Bausteine einer risikobewussten Unternehmensführung und können gravierende Reputationsschäden, finanzielle Einbußen und auch die persönliche Haftung von Organen verhindern.

Das Thema Fraud Risk Management gerät aufgrund aktueller Vorfälle und Skandale in der Branche immer mehr in den Fokus. Ein angemessenes und wirksames Fraud Risk Management dient der Reduzierung des Risikos, Opfer von betrügerischen Handlungen zu werden.

Ein effektives Fraud Risk Management System besteht aus den drei Kernelementen Prävention, Aufdeckung und Reaktion.

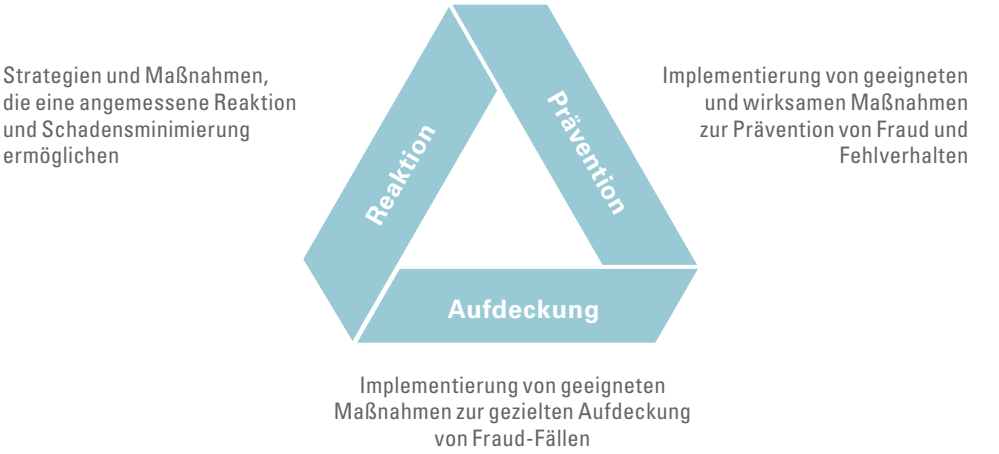
Zur Prävention gehören Maßnahmen wie der Aufbau einer effizienten Anti-Fraud-Organisation, Risiko- beziehungsweise Gefährdungsanalysen, Arbeitsanweisungen und Richtlinien sowie Compliance-Abteilungs-interne wie auch unternehmensweite Schulungen.

Die Aufdeckung umfasst Maßnahmen wie Hinweisgebersysteme, Monitoring, Überwachungshandlungen durch die Compliance-Funktion sowie regelmäßige Prüfungen durch die Interne Revision.

Im Rahmen der Reaktion werden Grundsätze zu Fallaufarbeitung sowie Krisenmanagement, Notfallpläne und Sanktionsprogramme verstanden.

Idealerweise besteht bereits eine aufbau- und ablauforganisatorische Abbildung der verschiedenen Elemente dieses Themenkomplexes im Unternehmen. Gegebenenfalls werden einige Aspekte, die dem Fraud Risk Management zuzuordnen sind, durch andere Organisationseinheiten wahrgenommen. In diesem Fall sollte eine lückenlose Abstimmung und Zusammenarbeit unter Nutzung von Synergien sichergestellt werden, um eine effiziente Ausgestaltung des Fraud Risk Management Systems realisieren zu können.

Kernelemente eines effektiven Fraud Risk Management Systems



Wir beraten und unterstützen Sie bei der Konzeption und Umsetzung sämtlicher Elemente eines Fraud Risk Management Systems – punktuell als auch gesamthaft – individuell gemäß den spezifischen Gegebenheiten Ihres Unternehmens. Unsere Beratungs- und Unterstützungsleistungen erstrecken sich dabei von der Definition des unternehmensindividuellen Zielbilds, der Analyse des Status Quo über die Identifizierung von Lücken und der risikoorientierten Ableitung und Priorisierung von Maßnahmen zur Schließung der Lücken bis hin zur Umsetzung. Im Rahmen der Umsetzung achten wir insbesondere auf eine individuelle Ausgestaltung der zu implementierenden Maßnahmen unter Berücksichtigung von Risiko- und Wirtschaftlichkeitsgesichtspunkten.

Das Wissen um die spezifischen Fraud-Risiken Ihres Unternehmens ist von zentraler Bedeutung für die effektive sowie effiziente Ausgestaltung des Fraud Risk Managements eines Unternehmens. Grundlage einer erfolgreichen Prävention ist demzufolge eine unternehmensindividuelle Analyse der potenziellen Fraud-Risiken.

Dank der Verwendung standardisierter Methoden im Rahmen der Risikobewertung ermöglichen wir eine Messbarkeit von Schadenspotenzialen und können geeignete Gegenmaßnahmen im Rahmen einer Wirtschaftlichkeitsbetrachtung ableiten beziehungsweise überprüfen. Diese Methodik ermöglicht zugleich Synergien für Ihre Risikoinventur.

Antikorruption

In den vergangenen Jahren haben mehrere Unternehmen aufgrund von Korruptionsskandalen erhebliche Finanz- und Reputationsschäden erlitten. Eine Vielzahl von Parametern wirkt sich auf die Korruptionsrisikosituation von Unternehmen aus. Unternehmen können in diesem Zusammenhang sowohl Täter als auch Geschädigte sein.

Aufgrund der Globalisierung und damit der Expansion auf neue Märkte, insbesondere Märkte in Hochrisikoländern, haben sich die Anforderungen an eine effektive Korruptionsprävention deutlich erhöht. Weitere Faktoren sind die Einbeziehung externer Dritter – auch im Rahmen von Outsourcing –, hoher Wettbewerbs- und Zeitdruck, die Reduzierung von Personal und Kontrolltätigkeiten sowie die Bildung von Joint Ventures und der Kauf von Unternehmen.

Neben den verschärften nationalen Gesetzen sind insbesondere zwei internationale Vorgaben von Bedeutung, die vor allem das Sanktions- und Reputationsrisiko für Unternehmen erheblich steigen lassen:

Foreign Corrupt Practices Act (FCPA): Diese Regelung, verabschiedet 1977 in den USA, verbietet die (versuchte) Bestechung ausländischer Amtsträger zur Durchführung oder Verlängerung eines Geschäfts. Verstöße gegen den FCPA können mit Geldstrafen von bis zu zwei Millionen US-Dollar pro Einzelfall geahndet werden. Die Definition des Einzelfalls ist sehr eng ausgelegt und das Strafmaß kann sich daher um ein Vielfaches erhöhen. Darüber hinaus können bei natürlichen Personen Geldstrafen von bis zu hunderttausend Euro sowie Freiheitsstrafen verhängt werden. Zudem ist eine mögliche Straferhöhung durch ergänzende Anwendung des Alternative Fines Act zu beachten.

Der FCPA gilt im Wesentlichen für Unternehmen, die an einer US-amerikanischen Börse gelistet sind, sowie für ausländische Tochtergesellschaften von US-amerikanischen Muttergesellschaften. Darüber hinaus werden vom FCPA ebenfalls Unternehmen erfasst, die nach US-Recht gegründet wurden oder deren Geschäftssitz in den USA liegt. Auch natürliche Personen fallen in den Anwen-

dungsbereich des FCPA, sofern sie die US-Staatsbürgerschaft besitzen oder ihren Wohnsitz in den USA haben. Unabhängig von den zuvor genannten Kriterien finden die Vorgaben des FCPA grundsätzlich auf jede (auch ausländische) natürliche und juristische Person Anwendung, die Korruptionshandlungen auf dem Hoheitsgebiet der USA vornimmt.

UK Bribery Act: Diese im Juli 2011 erlassene Regelung verpflichtet Unternehmen zum Nachweis der Implementierung diverser Maßnahmen, die auf die Verhinderung und Bekämpfung von Korruption abzielen. Betroffen sind weltweit Unternehmen einschließlich der für diese handelnden Personen, die eine geschäftliche Verbindung nach Großbritannien pflegen. Das Strafmaß bei Verstößen gegen den UK Bribery Act kann bis zu zehn Jahre Haft für natürliche Personen und Geldstrafen in unbegrenzter Höhe für juristische Personen betragen. Zudem drohen Nachteile bei oder gar der Ausschluss von der Vergabe öffentlicher Aufträge.

KPMG unterstützt Sie gern bei der Umsetzung gezielter Maßnahmen zur Korruptionsbekämpfung.

Folgende Maßnahmen zeigen exemplarisch auf, wie das Korruptionsrisiko gezielt reduziert werden kann:

- Management Commitment – klare Unterstützung einer Antikorruptionskultur seitens der Geschäftsführung
- Verhaltensvorgaben – Erstellung von Verhaltens-, Ethik- und Antikorruptionsrichtlinien und ähnlichen Regeln, wie beispielsweise eine Zuwendungs- und Interessenkonfliktrichtlinie
- Kenntnis der Geschäfte und Mitarbeiter – Due Diligence, Integrity Checks et cetera
- Risikofrüherkennungssysteme – Erfassung der individuellen Risikosituation eines Unternehmens (unter anderem Risk Assessments und Risiko- beziehungsweise Gefährdungsanalysen)
- Monitoring – Aufsetzen von Prozessen zur Überwachung und Verbesserung der Einhaltung von Compliance-Regeln
- Sanktionen – Etablierung stringenter Prozesse zur Ahndung von Verstößen

Effiziente Performance der Compliance IT-Anwendungen für Ihr Unternehmen

Eine präzise und effektive Performance sowie die Einhaltung fachlicher, gesetzlicher, organisatorischer und technischer Anforderungen von Compliance IT-Systemen sind ein unabdingbarer Beitrag zu einer erfolgreichen Unternehmenssteuerung.

Die Befolgung gesetzlicher Regelungen und Auflagen beispielsweise zu den Themen Geldwäsche, Finanzsanktionen und Embargos wie auch Fraud sowie das stets anspruchsvollere regulatorische Umfeld stellen Unternehmen vor immer neue fachliche und technische Herausforderungen.

Insbesondere die Komplexität der Thematik erfordert eine präzise und effektive Performance IT-gestützter Tools und weiterer Anwendungen. Solche technischen Hilfsmittel ermöglichen es, die Einhaltung der regulatorischen Anforderungen zu überwachen und das Unternehmen risikobewusst und effizient zu steuern.

Der integrative und modulare Gesamtlösungsansatz von KPMG vereinfacht die Umsetzung der Anforderungen an die Informationstechnologie und minimiert Restrisiken. Die individuelle Gestaltung einzelner Applikationen hat das Ziel, einen wichtigen Beitrag der Compliance IT zur erfolgreichen Unternehmenssteuerung zu leisten.

Die methodische Vorgehensweise führt erfahrungsgemäß zu Verbesserungen in den Prozessen und auch in der Effizienz im Umgang mit den Compliance IT-Anwendungen.

Ziel ist es, die Compliance IT-Anwendungen in die täglichen Abläufe zu integrieren, ohne einen spürbaren Mehraufwand in der Organisation selbst zu verursachen. Vielmehr soll sich dadurch ein Mehrwert in Form von Effizienzsteigerung ergeben. Die dabei notwendigen Prozesse erfordern eine wirksame Integration in bestehende Systeme und eine individuelle Ausrichtung zu implementierender Applikationen an der Unternehmensumgebung in fachlicher und technischer Hinsicht.

Die Aufnahme und Analyse der gesetzlichen, technischen und fachlichen Rahmenbedingungen sowie der bestehenden Compliance IT ist die Basis für die Auswahl der Applikationen und für deren Implementierung. Hinzu kommen deren individuelle Gestaltung und die Integration in bestehende Systeme. Dabei werden wesentliche Informationsbeziehungen anhand der Quell- und Zieldaten untersucht, Risiken erkannt und individuelle (Mindest-)Anforderungen an die bestehende Compliance IT definiert.

In diesem Zusammenhang bietet KPMG Ihnen beispielsweise folgende maßgeschneiderte Lösungen:

- Überblick über den aktuellen Stand der vorhandenen Compliance IT mithilfe einer ausführlichen Analyse und der Definition individueller Anforderungen
- Auswahl präziser und effizienter Applikationen nach einem individuell auf den Unternehmensbedarf ausgerichteten risikobasierten Ansatz
- Herstellung von Informationsbeziehungen anhand von Quell- und Zieldaten sowie Strukturierung unterschiedlicher Datenquellen zur Erstellung einer einheitlichen Zieldatenbank; Datenvalidierung während des Implementierungsprozesses zur frühzeitigen Identifizierung eventueller Fehlerquellen und Umsetzung entsprechender Anpassungen
- Parametrisierung und Feinjustierung zur effizienten Eingliederung in die Unternehmensumgebung
- Go-live im Unternehmen erfolgreich getesteter und spezifischer Applikationen und eventuelle Übertragung auf weitere Unternehmensbereiche
- Postimplementation und weitere Feinjustierungen aufgrund geänderter Rahmenbedingungen oder Anbindungen an weitere Produkte Ihres Unternehmens

Vertriebs-Compliance-System

Ein wirksames Vertriebs-Compliance-System gibt Versicherungsunternehmen Gelegenheit, das Vertrauen der Kunden zu stärken, sie durch Ausweitung der Transparenz zu schützen, Vertriebsrisiken zu minimieren und einen Wettbewerbsvorteil herzustellen.

Damit die einheitliche Umsetzung von Präventivmaßnahmen zur Einhaltung der Vorgaben, beispielsweise aus dem Verhaltenskodex des Gesamtverbands der Deutschen Versicherungswirtschaft für den Vertrieb, gewährleistet ist, empfiehlt KPMG wie eingangs dargestellt, die Implementierung eines CMS auf Basis der Grundelemente des IDW PS 980 und die Berücksichtigung des GDV-Verhaltenskodexes.

Darüber hinaus hat die EU bereits den Rahmen für die Zukunft des Versicherungsvertriebs abgesteckt. Zukünftig werden in unterschiedlichen Regelwerken die Anforderungen an die Vermittlung von Versicherungsprodukten weiter erhöht. Damit die vorhandenen und zukünftigen Anforderungen erfüllt werden, sind folgende Kernthemen Inhalt der umzusetzenden Maßnahmen:

Aufbau einer Vertriebs-Compliance-Einheit

Wesentliche Bestandteile des KPMG-Lösungsansatzes sind der Aufbau eines für die Vertriebs-Compliance zuständigen Bereichs innerhalb der Compliance-Funktion und die Integration der Vertriebs-Compliance-Maßnahmen in das CMS. Zur Schaffung von Transparenz und zur Gewährleistung von Risikobewusstsein im Handeln ist es unverzichtbar, Standards festzulegen, Kontroll-, Überwachungs-, Reporting-, Kommunikations- und Schulungsmaßnahmen durchzuführen und ein Anreiz- und Sanktionssystem einzuführen.

„Know your Agent"-Maßnahmen

Wesentliche Inhalte sind die Integration von Mindestqualifikationsanforderungen und transparenten Auswahlprozessen zur Prüfung von Qualifikation, Ausbildung und Zuverlässigkeit der Vertriebsmitarbeiter. Dabei ist auch zu prüfen, ob und welche Anpassungen am Weiterbildungsprogramm erforderlich sind oder wie die Qualifizierungsmaßnahmen zum Beispiel bei Maklern gesteuert und überwacht werden können.

Information und Beratung im Vertrieb

Die Pflicht zur Aufklärung und Beratung stellt die Schaffung von Transparenz für den Kunden in den Mittelpunkt. Dieser Umstand verlangt insbesondere konzernweit einheitliche Vorgaben und Prozesse hinsichtlich der Beratung, des Verhaltens gegenüber Kunden, der Dokumentation von Beratungsgesprächen und der Vorgabe, dass Beratungen bedarfsgerecht erfolgen müssen. Beispielsweise kann es erforderlich sein, die Prozesse und die IT-Systeme anzupassen, die die Beratung der Kunden unterstützen. Zudem können sich Auswirkungen auf das Online-Angebot der Versicherungsunternehmen ergeben.

Compliance-Vorschriften

Die Sicherstellung eines rechtschaffenen Vertriebs durch Ächtung von Korruption, Bestechung und Bestechlichkeit sowie durch die Verhinderung der Unterstützung von Terroristen und von organisierter Kriminalität spielt eine wesentliche Rolle. Zudem muss gewährleistet werden, dass auch der Datenschutz dezentral bei den Versicherungsagenturen sichergestellt wird.

Vergütung, Provisionen und Incentives

Zur Vermeidung von Fehlanreizen und Interessenkonflikten müssen einheitliche Grundsätze zur Vergütung von Vertriebsmitarbeitern und -partnern sowie Vorgaben zur Ausgestaltung von Incentives eingeführt werden. Darüber hinaus ist beispielsweise zu klären, welche Auswirkungen eine Offenlegung einzelner Komponenten der Vergütung oder der Gesamtkostenquote auf das Vergütungssystem und den Vertrieb insgesamt hätte und wie die Versicherungsunternehmen darauf strategisch reagieren sollten.

Produktentwicklung und -genehmigung

Auch bei der Gestaltung der Produkte muss die allgemeine Pflicht beachtet werden, dass Konsumenteninteressen zu berücksichtigen sind. Die geforderte Transparenz und Angemessenheit der Produkte setzt deren Bewertung und Steuerung nach Risiken und die Integration von Compliance-Aspekten in den Neuproduktprozess voraus.

Beschwerdemanagement

Das Ziel der Vermeidung von Reputationsschäden verlangt eine effiziente und kundenorientierte Beschwerdebearbeitung. Die Compliance-Abteilung muss anhand von Reportings regelmäßig Stellung beziehen und gegebenenfalls müssen Verbesserungsmaßnahmen ergriffen werden.

Der KPMG-Lösungsansatz wirkt aktiv auf die Einhaltung der Compliance-Vorgaben in den vertriebsrelevanten Themenfeldern hin. Darüber hinaus unterstützt KPMG Sie dabei, im Rahmen des Vertriebsmanagements aus einer Pflicht eine Chance zu machen. So helfen zum Beispiel standardisierte Beratungsprozesse, die regulatorischen Anforderungen zu erfüllen und gleichzeitig die Produktivität des Vertriebs zu steigern.

Durch die im Dezember 2014 erweiterte EU-Amtshilferichtlinie werden bestimmte Versicherungsunternehmen und andere Finanzinstitute (FI) in der EU verpflichtet, Finanzkonten, deren Kontoinhaber eine steuerliche ausländische Ansässigkeit aufweist, zu identifizieren und an ihre nationale Steuerbehörde zu melden. Trotz der strukturellen Ähnlichkeit der Anforderungen zu den FATCA IGAs bedeuten Detailunterschiede sowie die größere Zahl der meldepflichtigen Konten eine durchgehende Automatisierung der entsprechenden Prozesse.

Automatischer Austausch von Steuerdaten – Automatic Exchange of Information (AEOI)

Nachdem im Juli 2014 der Foreign Account Tax Compliance Act (FATCA) in Kraft getreten ist und Finanzinstitute und bestimmte Versicherungsunternehmen weltweit zur Meldung von Kundendaten an die US-amerikanische Steuerbehörde verpflichtet wurden, richtet sich der Fokus nun auf weitere Rahmenwerke der EU und der OECD, die den automatischen Austausch von Informationen über Kontendaten betreffen.

Vier Jahre nach Verabschiedung des US-Gesetzes Foreign Account Tax Compliance Act (FATCA) sind seit dem 1. Juli 2014 neben Finanzinstituten auch Versicherungsunternehmen mit Kapitalwerten, beispielsweise Lebens- und Rückversicherer, weltweit zur Meldung der Daten von US-steuerpflichtigen Kunden an die US-Steuerbehörde IRS (Internal Revenue Service) verpflichtet.

Nachdem die USA ein Konzept zum Austausch von Steuerinformationen durchsetzen konnten, haben die G20-Staaten die Verhinderung von Steuerhinterziehung explizit als politisches Ziel formuliert. Die OECD hat daraufhin am 21. Juli 2014 den finalen Standard für den automatischen Informationsaustausch über Finanzkonten (Automatic Exchange of Information, kurz AEOI) veröffentlicht. Konzeptuell basiert dieser auf dem „Model 1 Intergovernmental Agreement“ (US-IGA), das eine Vielzahl von Staaten mit den USA abgeschlossen hat. Vorrangiges Ziel der Teilnehmerstaaten ist es, ab 2016 die Besteuerung von Kapitalerträgen ihrer Steuerpflichtigen mit Versicherungspolicen im Ausland anhand eines Steuerdatenaustauschs sicherzustellen. In der EU wird diese Verpflichtung durch die beschlossene Erweiterung der EU-Amtshilferichtlinie konkretisiert, die einen Steuerdatenaustausch bereits ab 2017 für das Meldejahr 2016 vorschreibt.

Aus FATCA haben sich für Versicherungsunternehmen bereits zahlreiche Pflichten zur Identifizierung, zur Dokumentation und letztlich zur Meldung von Kunden- beziehungsweise Policendaten ergeben. Waren bisher jedoch nur US-Steuerpflichtige zu identifizieren und der entsprechenden Behörde zu melden, müssen die Verpflichteten nun alle Kunden erkennen, die in einem oder mehreren am AEOI teilnehmenden Staat ansässig sind, und sie anschließend melden. Damit sind Versicherungen auch nach dem Inkrafttreten von FATCA mit sehr komplexen Herausforderungen konfrontiert. In erster Linie ergibt sich für sie eine funktionale Komplexität, da sich auf der einen Seite die Anwendungsbereiche der verschiedenen Konzepte in Details in dem Maße unterscheiden, dass sich teils gravierende Unterschiede ergeben können. Andererseits überschneiden sich die Anforderungen der Melderegime teilweise, wodurch eventuelle Synergieeffekte genutzt werden können. Eine Herausforderung wird zudem sein, dass die Zeitpläne zur Umsetzung, wenn auch noch nicht final vorliegend, sehr eng gesteckt sein werden.

Der AEOI ist, anders als die US-IGA und FATCA, tatsächlich als internationaler Standard angelegt und daher nicht ausschließlich auf die Vorgaben nur eines Empfängerlandes bezogen. Auch Versicherungsunternehmen, die von den IGA-Regelungen nur gering oder gar nicht betroffen sind, werden einem solch global angelegten Austausch in der Regel kaum ausweichen können. Die Unternehmen sollten daher frühzeitig entsprechende Auswirkungen für ihre Geschäftsfelder, Prozesse und IT-Systeme prüfen, denn die Verpflichtungen werden bereits ab dem Jahreswechsel 2015/2016 gelten.

KPMG hat ein Spezialistenteam aufgebaut, das bei der Einleitung der notwendigen Schritte zur Umsetzung der gesetzlichen Anforderungen sowie bei allen Fragen rund um den automatischen Informationsaustausch entlang der gesamten Wertschöpfungskette (rechtliche, steuerliche, prozessuale und IT-bezogene Aspekte) berät und unterstützt. Hierdurch sorgen wir dafür, dass für jede Fragestellung der Ansprechpartner mit dem spezifischen Detailwissen bereitsteht.

Compliance Due Diligence

Zielbildentwicklung und Bestandsanalyse

KPMG hat ein Vier-Phasen-Modell zur Bewertung Ihrer aktuellen Compliance-Konformität entwickelt: Unter Beachtung individueller Compliance-Ziele sowie gesetzlicher und unternehmensspezifischer Vorschriften werden anhand dieses Modells mögliche Compliance-Risiken aufgezeigt.

Eine effiziente Umsetzung der Compliance-Anforderungen mit dem Ziel, Compliance-Konformität zu erreichen, erfordert eine systematische Vorgehensweise. KPMG hat dafür ein Vier-Phasen-Modell entwickelt.

Ein wesentliches Ergebnis der Anwendung dieses Modells ist eine Risikomatrix, die in übersichtlicher und entscheidungsrelevanter Form Abweichungen und die damit verbundenen Risiken auf einen Blick darstellt.

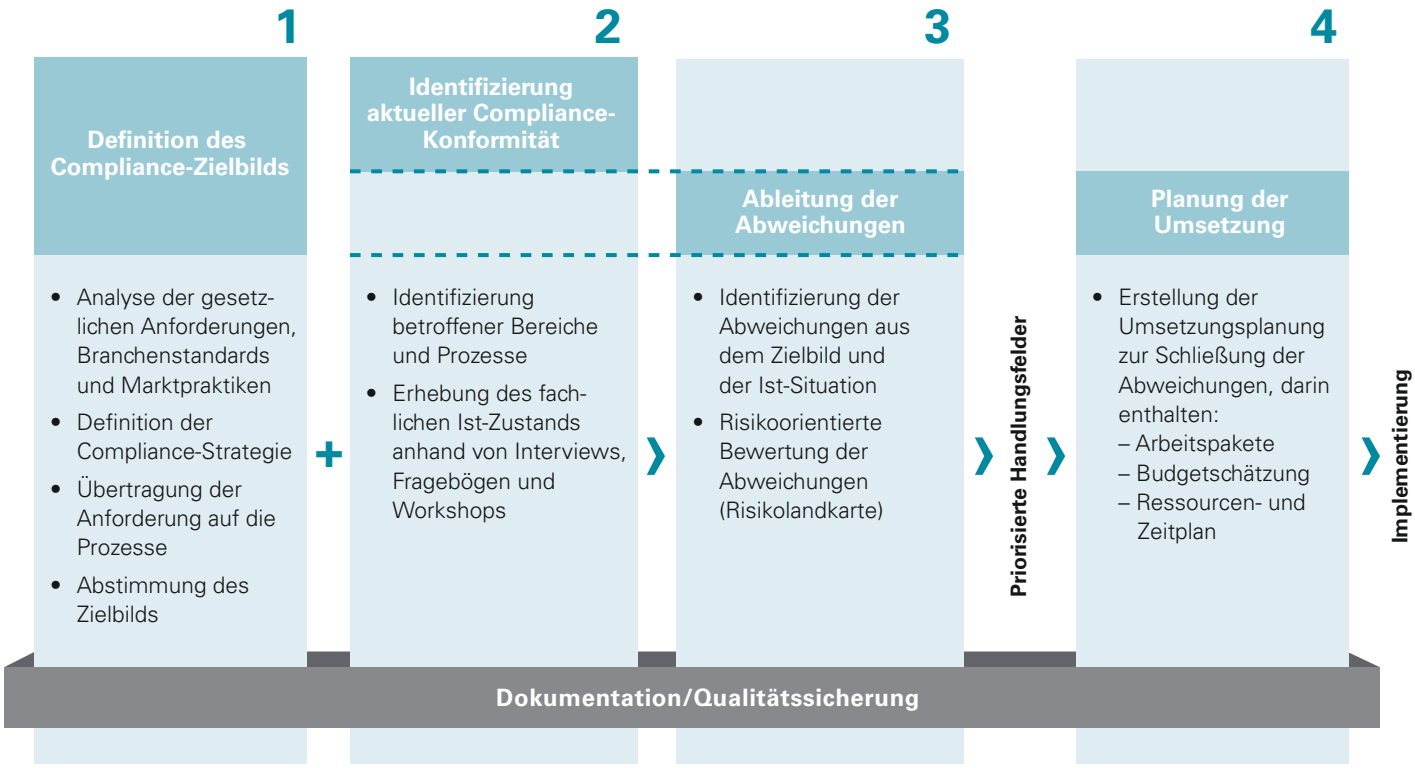
Lösungsansatz zur Umsetzung

In **Phase eins** wird gemeinsam mit Ihnen ein Compliance-Zielbild entwickelt. Dessen Basis sind neben unternehmensspezifischen Vorgaben, gesetzliche und aufsichtsrechtliche Anforderungen sowie Branchenstandards.

In **Phase zwei** wird die Ist-Situation des jeweiligen Unternehmens mithilfe einer fundierten Analyse auf der Grundlage von Dokumenten, Interviews oder Workshops ermittelt. Dabei werden alle unternehmensrelevanten Bereiche, Prozesse und Dienstleistungen hinsichtlich möglicher Risiken überprüft, woraus wiederum fachliche Anforderungen abgeleitet werden.

In **Phase drei** erfolgt eine Identifizierung der Abweichungen, die sich aus dem Abgleich des Compliance-Zielbilds mit der Ist-Situation ergeben. Mit einem von KPMG entwickelten Bewertungsmodell werden die Abweichungen anhand verschiedener Risikoparameter – beispielsweise Eintrittswahrscheinlichkeit, Auswirkung des potenziellen Schadens und Aufwand bei der Schließung der Abweichung – und deren Gewichtung dreidimensional und zugleich risikoorientiert pro Themenfeld und untersuchter Einheit bewertet. Ergebnis dieser Phase ist eine Risikomatrix, die eine Zusammenfassung der Abweichungen einschließlich der damit verbundenen Risiken und deren Priorisierung zeigt.

Compliance Due Diligence als Basis für den Aufbau einer effizienten und effektiven Compliance



Den **Abschluss** des Vier-Phasen-Modells bildet ein konkreter Plan für die Umsetzung – die priorisierten Handlungserfordernisse sind hierbei leitend. In diesem Zusammenhang werden eine Ressourcenplanung, Budgetschätzungen und eine zeitliche Planung vorgenommen.

Ihr Vorteil

Dank der Eindeutigkeit und der hohen Transparenz ermöglicht es die Compliance Due Diligence, die unternehmensweit vorhandenen Compliance-Abweichungen zu bewerten und entsprechende Maßnahmen zu priorisieren. Durch eine frühzeitige Umsetzungsorientierung bringt sie zudem eine Reduzierung der Umsetzungskosten und Effektivitätssteigerungen mit sich. Darüber hinaus können praxisorientierte „Quick Wins" identifiziert werden. Schließlich stellt eine Definition der notwendigen Arbeitsschritte eine detaillierte Grundlage interner Ressourcenplanungen dar.

Wir stehen Ihnen sehr gern für Fragen und Gespräche zur Verfügung. Sprechen Sie uns an!

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Bernd Michael Lindner
Partner
Financial Services
T +49 89 9282-1368
blindner@kpmg.com

Oliver Wolff
Partner
Financial Services
T +49 6131 370-129
owolff@kpmg.com

www.kpmg.de/compliance