FORENSIC, RISK & COMPLIANCE

COMPLIANCE FÜR DEN MITTELSTAND

WAS IST COMPLIANCE?

Der englische Begriff „to comply with“ bedeutet ins Deutsche übersetzt: „mit etwas übereinstimmen“ oder „etwas beachten“. Als Compliance im Bereich der Unternehmensführung wird das Einhalten und Befolgen von Gesetzen und anderen verbindlichen Regelungen, vertraglichen Verpflichtungen und internen Richtlinien in einem Unternehmen, durch seine Organmitglieder, Führungskräfte und Mitarbeiter bezeichnet. Compliance soll erreichen, dass sich alle Unternehmensangehörigen im Rahmen ihrer Tätigkeit für das Unternehmen stets gesetzestreu und rechtskonform verhalten.

Obwohl es sich bei der Einhaltung von Rechtsvorschriften eigentlich um eine Selbstverständlichkeit handelt, zeigen die in den letzten Jahren bekannt gewordenen Korruptionsskandale und zum Teil horrenden Bußgelder in Kartellrechtsverfahren, dass Unternehmen ein vitales Interesse an der aktiven Vermeidung von Regelverstößen in ihrer Organisation haben. Hinzu kommt, dass neben den Behörden auch die Öffentlichkeit immer sensibler auf Unregelmäßigkeiten, wie z.B. schwere Verstöße gegen den Datenschutz, reagiert. Die Folgen für die Unternehmen sind Vermögens- und Reputationsschäden, empfindliche Straf- oder Bußgeldzahlungen sowie persönliche Haftungsfolgen für die verantwortlichen Führungskräfte.

Das rechtliche Umfeld, in dem sich Unternehmen heute bewegen, ist einer stetig dichteren Regulierung unterworfen. Die Anwendungsbereiche von spezialgesetzlichen Regelungen, wie etwa dem Außenwirtschaftsrecht, wurden erweitert, so dass sich heute deutlich mehr Unternehmen mit diesen Anforderungen auseinander setzen müssen. Beispielhaft seien auch der amerikanische Foreign Corrupt Practices Act („FCPA“) sowie der britische UK Bribery Act („UKBA“) aus dem Jahr 2011 genannt, deren vorrangiges Ziel die Vermeidung von Korruption ist. Derartige Regelungen nehmen weltweite Geltung für sich in Anspruch und betreffen daher auch grenzüberschreitend tätige Unternehmen, die nicht in den USA oder dem Vereinigten Königreich beheimatet sind. Bei Nichtbeachtung drohen erhebliche Konsequenzen.

Doch die gesetzlichen Sanktionen treffen in zunehmendem Maße nicht mehr nur die direkt am Regelverstoß Beteiligten. Wenn ein Angestellter im Rahmen seiner beruflichen Tätigkeit Straftaten begeht, dann müssen auch das betroffene Unternehmen sowie dessen gesetzlichen Vertreter mit Sanktionen rechnen.

Mit einem effektiven Compliance Management Systems („CMS“) können Führungskräfte ihr Unternehmen und sich selbst vor derartigen Folgen schützen. Dies gilt grundsätzlich sogar dann, wenn das CMS den Regelverstoß im Einzelfall nicht verhindern konnte. Mit der Einführung eines effektiven CMS kommen die Unternehmensvertreter ihren Sorgfaltspflichten in Bezug auf die Vermeidung von Regelverstößen nach und können sich im Ernstfall leichter enthaften. Die Schaffung eines effektiven CMS zum Schutz des Unternehmens, zur Entlastung der Unternehmensverantwortlichen und zur Sicherstellung von regelkonformem Handeln ist damit faktisch eine unternehmerische Notwendigkeit geworden.

Bei den Vorständen und Aufsichtsgremien setzt sich daher mehr und mehr die Erkenntnis durch, dass zur Wahrnehmung ihrer Aufgaben ein Compliance Management System unerlässlich ist. Ein CMS ist zudem eine sinnvolle Ergänzung der im Unternehmen bereits vorhandenen Maßnahmen zum Risikomanagement und verbessert die Funktionsweise des internen Kontrollsystems. Als Teil der Corporate Governance Landschaft eines Unternehmens ermöglicht ein CMS den Führungskräften, das Unternehmen besser zu kontrollieren, Risiken frühzeitig zu begegnen und den Wert des Unternehmens zu steigern.

Neben den klassischen Anwendungsbereichen eines CMS zur Vermeidung von Korruption und zur Einhaltung des Kartellrechts, sind in vielen Unternehmen auch Themen wie Datenschutz, Umweltschutz oder Produktsicherheit durch ein CMS abgedeckt. Als weitere Themenfelder kommen Arbeitsschutz, IT-Sicherheit und die Vermeidung von Geldwäsche in Betracht.

Ausgehend von historisch gewachsenen Unternehmenswerten und der von der Unternehmensführung vorgelebten Kultur („tone from the top“) kann Compliance individuell auf jene Teilbereiche (Rechtsgebiete oder Geschäftsbereiche) im Unternehmen fokussiert werden, in denen die wesentlichsten Risiken bestehen. Nach einer ersten Risikobeurteilung beginnen viele Unternehmen mit konkreten Compliance-Maßnahmen zur Korruptionsbekämpfung z.B. in den Abteilungen Einkauf und Vertrieb.

DER PRÜFUNGSSTANDARD 980 DES INSTITUTS DER WIRTSCHAFTSPRÜFER (IDW PS 980)

Mit dem IDW PS 980 vom April 2011 hat das Institut der Wirtschaftsprüfer einen neuen Prüfungsstandard mit dem Titel „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen" veröffentlicht, der die vom IDW-Arbeitskreis Compliance entwickelten sieben Grundelemente eines Compliance Management Systems darstellt und Anforderungen für die freiwillige externe Prüfung (Audit) eines CMS formuliert.

Interessierten Unternehmen wird mit dem IDW PS 980 eine allgemeingültige Orientierungshilfe zur Entwicklung und Implementierung eines eigenen CMS gegeben.

Nach den Vorgaben des IDW umfasst ein vollständiges CMS die folgenden sieben Compliance-Grundelemente:

Anhand dieser sieben Grundelemente kann die Unternehmensführung ein CMS aufbauen, das geeignet ist, Compliance-Risiken erfolgreich zu minimieren.

1. Compliance-Kultur

Der IDW PS 980 betont die Bedeutung einer eigenen Compliance Kultur im Unternehmen. Sie wird im Wesentlichen bestimmt durch den gelebten Wertekanon des Unternehmens sowie seiner Mitarbeiter und ist geprägt durch die Grundeinstellungen und Verhaltensweisen des Managements und des Aufsichtsorgans („tone from the top"). Die Compliance-Kultur beeinflusst die Bedeutung welche die Mitarbeiter der Beachtung von Regeln beimessen und damit deren Bereitschaft zu regelkonformem Verhalten.

2. Compliance-Ziele

Auf der Grundlage der allgemeinen Unternehmensziele und nach einer Analyse der für das Unternehmen bedeutsamen Regeln legen die gesetzlichen Vertreter die Ziele fest, die mit dem CMS erreicht werden sollen. Dies umfasst die Festlegung der relevanten Teilbereiche und der in den Teilbereichen einzuhaltenden Regelungen.

3. Compliance-Risiken

Durch eine systematische Aufnahme der Risiken für Regelverstöße in den abgegrenzten Teilbereichen, werden die Compliance-Risiken festgestellt, die eine Verfehlung der Compliance-Ziele zur Folge haben können. Es wird ein Verfahren zur Risikoerkennung, -analyse und Risiko-Berichterstattung eingeführt.

4. Compliance-Programm

Im Rahmen der Entwicklung des Compliance-Programms werden Grundsätze und Maßnahmen eingeführt, die auf die Begrenzung von Compliance-Risiken und auf die Vermeidung von Compliance-Verstößen (Prävention) ausgerichtet sind. Das Programm umfasst auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen (Reaktion).

5. Compliance-Organisation

Die Compliance-Organisation umfasst die Festlegung von Rollen und Verantwortlichkeiten durch das Management sowie die Aufbau- und Ablauforganisation. Die für ein wirksames CMS notwendigen Ressourcen sind zur Verfügung zu stellen. Zur Organisation zählt auch die Entwicklung organisatorischer und technischer Hilfsmittel wie Checklisten, Handbücher und IT-Tools.

6. Compliance-Kommunikation

Die Mitarbeiter und ggfs. auch Dritte werden über das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert (z.B. durch Schulungen). Es wird festgelegt, auf welche Weise Compliance-Risiken sowie Hinweise zu Verstößen an die zuständigen Stellen berichtet werden.

7. Compliance-Überwachung und Verbesserung

Die Compliance-Überwachung durch prozessunabhängige Stellen und die Berichterstattung von Schwachstellen und Regelverstößen an das Management oder andere hierfür bestimmte Stellen führt zu einer kontinuierlichen Weiterentwicklung des CMS. Die gesetzlichen Vertreter haben die notwendigen Maßnahmen zur Beseitigung von Mängeln und zur laufenden Überwachung und Verbesserung des Systems zu veranlassen. Die konkrete Ausgestaltung des CMS liegt in der Verantwortung der gesetzlichen Vertreter des Unternehmens und ist abhängig von den festgelegten Compliance-Zielen, der Größe des Unternehmens sowie von Art und Weise der Geschäftstätigkeit.

Als weitere Hilfestellung enthält der IDW PS 980 im Anhang allgemein anerkannte Rahmenkonzepte, die ebenfalls bei der Erstellung eines eigenen CMS herangezogen werden können.

COMPLIANCE-DIENSTLEISTUNGEN DER BDO, INSBESONDERE FÜR MITTELSTÄNDISCHE UNTERNEHMEN

Im Zusammenhang mit Compliance bietet BDO interessierten Unternehmen aller Branchen und Größenordnungen die vollständige Palette Compliancebezogener Dienstleistungen an. Im Einzelnen sind dies:

1. Compliance-Beratung und Aufbau eines CMS

Wenn Sie beabsichtigen in Ihrem Unternehmen erstmalig ein Compliance System zu installieren, ist zunächst das individuelle Compliance-Risikoprofil zu ermitteln. Dabei sind die Unternehmensgröße, Branche, Tätigkeitsfelder und Rechtsform wichtige Faktoren. Das Ergebnis dieser Risikoanalyse gibt Ihnen einen Überblick über die im Rahmen des CMS vorrangig zu adressierenden Themen und Bereiche. Nach Möglichkeit stellen wir Ihnen auf Wunsch Compliance-Konzepte vergleichbarer Unternehmen als Benchmark vor.

Gemeinsam mit Ihnen erstellen wir ein Compliance-Konzept mit dem ein strukturiertes und den Anforderungen Ihres Unternehmens entsprechendes CMS entwickelt und implementiert werden kann. Hierfür ermitteln wir die Anforderungen (Soll) unter Beachtung der sieben Grundelemente des IDW PS 980 sowie die bestehenden Compliance-relevanten Maßnahmen in Ihrem Unternehmen (Ist). Durch einen Soll-Ist-Abgleich leiten wir die erforderlichen nächsten Schritte ab und halten diese in einem Maßnahmenplan fest. Verfügen Sie bereits über Teile eines CMS, können wir im Wege einer Vorprüfung (Quick Check) noch bestehende Lücken ermitteln und Vorschläge zur sinnvollen Ergänzung des CMS und Ihres Risikomanagements unterbreiten.

1. Zielfestlegung: individuelle Bestimmung der relevanten Unternehmensbereiche, Regionen und Themenfelder
2. Risikoanalyse: systematische Ermittlung und Bewertung der Compliance-Risiken auf Prozessebene in den identifizierten Bereichen
3. Ermittlung SOLL-Zustand, z.B. nach IDW PS 980, unter Berücksichtigung der spezifischen Eigenschaften und Kultur des Unternehmens
4. Erhebung der bestehenden Grundsätze und Maßnahmen (IST-Zustand) sowie SOLL-IST-Abgleich und Ableitung eines Maßnahmenplans
5. Konzeption von Compliance-Organisation, -Programm und -Kommunikation sowie der Überwachung und Verbesserung des CMS
6. Implementierung und Dokumentation des Compliance-Konzepts

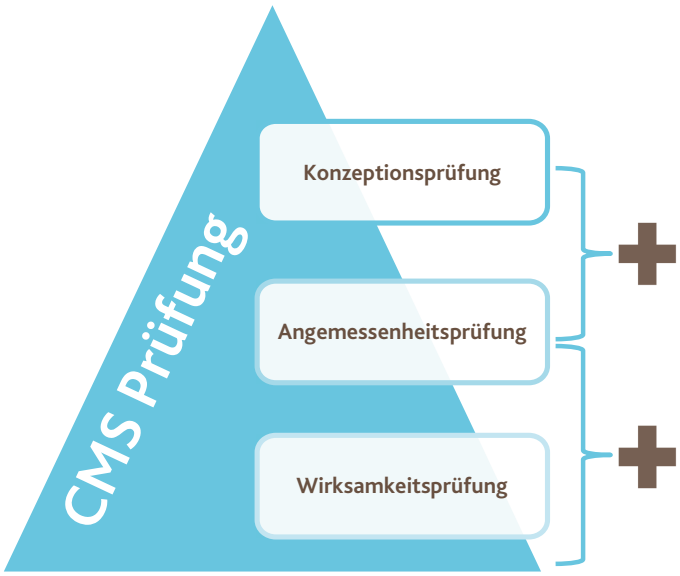
Auch bei der Implementierung Ihres Konzepts stehen wir Ihnen mit unserer Expertise zur Seite, etwa bei der Ermittlung und Dokumentation der Unternehmenswerte (Compliance-Kultur), bei der Festlegung von Compliance-Zielen und beim Aufbau einer auf die Unternehmensgröße zugeschnittenen Ablauforganisation. Wir erstellen maßgeschneiderte Entwürfe für Ihre Richtlinien, Verfahrensanweisungen und Schulungsunterlagen.

2. Prüfungen des CMS nach IDW PS 980

Für die Weiterentwicklung Ihres CMS und zum Nachweis der Erfüllung der diesbezüglichen Sorgfaltspflichten der gesetzlichen Vertreter ist es sinnvoll, das CMS durch einen unabhängigen Prüfer überprüfen zu lassen, der einen Prüfungsbericht erstellt und ein Prüfungsurteil gemäß IDW PS 980 abgibt.

Gegenstand der Prüfung sind die von den gesetzlichen Vertretern in einer CMS-Beschreibung zusammengefassten Aussagen über das CMS des Unternehmens.

Ziel einer umfassenden Prüfung gemäß IDW PS 980 ist es, eine Aussage mit hinreichender Sicherheit darüber zu erhalten, ob die in der CMS-Beschreibung enthaltenen Aussagen über Grundsätze und Maßnahmen des CMS angemessen dargestellt sind (Konzeptionsprüfung). Ferner soll eine Aussage darüber getroffen werden, ob diese Grundsätze und Maßnahmen geeignet sind, mit hinreichender Sicherheit Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen und zu verhindern und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind (Angemessenheitsprüfung). Prüfungsgegenstand ist darüber hinaus, ob die Grundsätze und Maßnahmen in den laufenden Geschäftsprozessen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und beachtet werden (Wirksamkeitsprüfung). Die drei Prüfungsstufen bauen aufeinander auf.



Im Zuge der Entwicklung und Einführung eines CMS können Prüfungen durchgeführt werden, die ausgewählte Teilbereiche betreffen. Bei Teilbereichen kann es sich um Themen (z.B. Anti-Korruption), Regionen, etc. handeln. Bei der Prüfung nach IDW PS 980 handelt es sich um eine freiwillige Prüfung, die von den gesetzlichen Vertretern in Auftrag gegeben wird und die separat, aber auch in engem zeitlichen Zusammenhang mit der Jahresabschlussprüfung durchgeführt werden kann.

3. Schulungen

Ein wesentlicher Aspekt der Compliance-Kommunikation sind Schulungen von Mitarbeitern und Führungskräften, um die relevanten gesetzlichen Bestimmungen und internen Regelungen (z.B. Verhaltenskodex und Anti-Korruptionsrichtlinie) zu vermitteln und um die gesamte Compliance-Organisation des Unternehmens vorzustellen. Schulungen dienen darüber hinaus der Prävention von Regelverstößen. Mit Hilfe von praktischen Beispielen wird Problembewusstsein erzeugt und die Beteiligten werden für das Erkennen von Unregelmäßigkeiten (sog. „red flags") sensibilisiert. Gemeinsam mit Ihnen entwickeln wir Schulungskonzepte und schulen direkt Ihre Mitarbeiter national und international. Alternativ übernehmen wir das Training Ihrer Multiplikatoren, damit diese die Compliance-Inhalte im Unternehmen verbreiten.

4. Business Partner Screenings

Als Bestandteil der Compliance-Aktivitäten wird die Überprüfung von Geschäftspartnern immer wichtiger. Insbesondere Unternehmen, die unter den Geltungsbereich des amerikanischen FCPA oder des englischen UKBA fallen, sind verpflichtet, in risikoangemessenem Umfang Business Partner Screenings durchzuführen. Das Prinzip „know your client" gehört mittlerweile zum Standardprogramm risikobewusster Unternehmensführung. In die Überprüfungen sind auch die für das Unternehmen als Vermittler tätigen Agenten, Handelsvertreter und Makler einzubeziehen. Auf der untersten Risiko-Stufe mag es ausreichen, den Kunden und Lieferanten die Compliance-Standards des eigenen Unternehmens mitzuteilen und sie aufzufordern, diese im Rahmen der Geschäftsbeziehung zu beachten. Bei Geschäftsbeziehungen oder Branchen mit höherem Risiko-Potential kann es angezeigt sein, Background-Checks durchzuführen, um die Seriosität des jeweiligen Partners verlässlich zu überprüfen. Auf diese Weise verringern Sie in erheblichem Maße die allgemeine Risikoexposition Ihres Unternehmens und können so vermeiden, in Schmiergeldzahlungen oder Verstöße gegen Ausfuhrbestimmungen (z.B. Lieferungen von „dual-use" Produkten in Embargoländer) verwickelt zu werden. Darüber hinaus lassen sich Zahlungsausfälle und weitere Probleme in der Auftragsabwicklung minimieren.

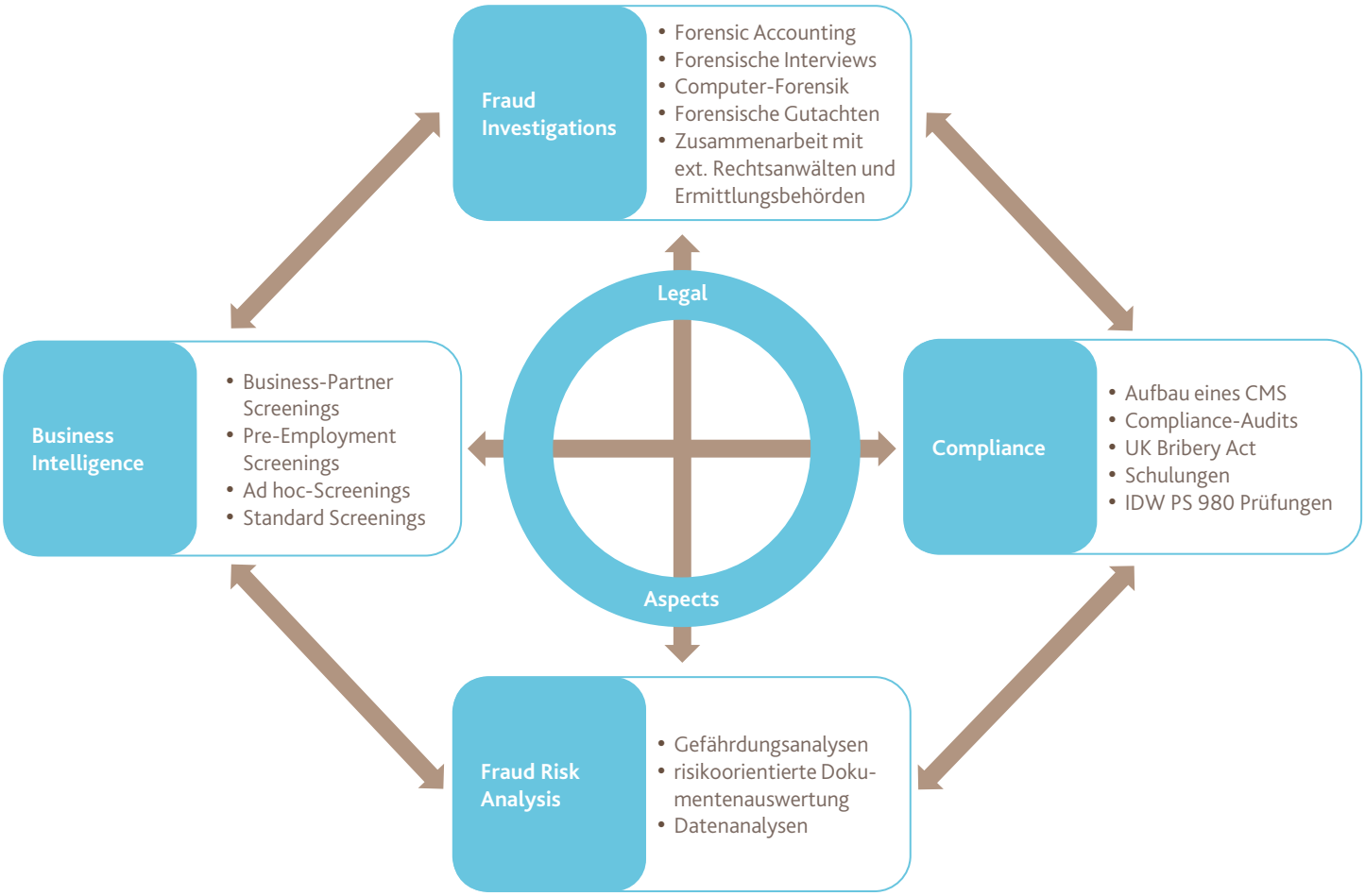
5. Compliance Due Diligence

Vor dem Erwerb anderer Unternehmen oder von Beteiligungen empfehlen wir, neben der bisher üblichen Financial Due Diligence auch die Durchführung einer Untersuchung, die die Praxis der Einhaltung von Gesetzen und Richtlinien im Zielunternehmen zum Gegenstand hat. Eine solche Compliance Due Diligence soll verhindern, dass Sie sich mit dem neuen Unternehmensteil Risiken „ins Haus" holen, die in Ihrem Unternehmen bislang verlässlich kontrolliert wurden oder dass die Aufstockung der Mitarbeiterzahl zu problematischen Veränderungen bei der Unternehmenskultur führt. Ferner erhalten Sie einen aufschlussreichen Überblick über die bei der Zielgesellschaft bestehenden Compliance-Strukturen und Maßnahmen. Nach Abschluss der Compliance Due Diligence benennen wir Ihnen sämtliche von uns erkannten Risikofelder und geben Empfehlungen zur Bewältigung der Risiken, die aus der Nichteinhaltung von Gesetzen oder Richtlinien im Zielunternehmen drohen.

6. Forensic Services

Auch das beste Compliance-Management-System kann Rechtsverstöße nicht zu 100 Prozent verhindern. Wir bieten Ihnen eine Reihe von Leistungen an, wenn es dennoch einmal zu Verstößen, Straftaten o.ä. in Ihrem Unternehmen gekommen ist. Die forensischen Teams der BDO unterstützen Sie bei der Aufdeckung von wirtschaftskriminellen Handlungen (Betrug, Unterschlagung, Bilanzfälschung, Mobbing etc.). Die betriebswirtschaftliche, juristische und (immer wichtiger werdende) IT-forensische Expertise von BDO ermöglicht eine umfassende Sachverhaltsaufklärung und Sicherung von Beweismitteln einschließlich der Überprüfung von Computerdateien und E-Mail-Korrespondenz. Mit unseren Untersuchungsergebnissen sind Sie in der Lage, über das weitere Vorgehen eigenverantwortlich zu entscheiden und die aus Ihrer Sicht geeigneten Maßnahmen zu treffen. Das kann z.B. die rein interne Ziehung von arbeitsrechtlichen Konsequenzen, die Einschaltung von Staatsanwaltschaft und Polizei oder ein Schadensersatzprozess vor den Zivilgerichten sein. Nicht zuletzt hilft Ihnen die Klärung der Fakten und Beweismittel bei der Abwehr von Ansprüchen Dritter. Im weiteren Verlauf unterstützen wir Sie bei der Identifikation und Behebung der Schwachstellen im internen Kontrollsystem und im Compliance Management System, die den aufgetretenen Regelverstoß ermöglicht oder begünstigt haben.

FORENSIC SERVICES – LEISTUNGSSPEKTRUM



Effektive Unterstützung durch BDO

Unser Team aus Experten mit kaufmännischem, juristischem Hintergrund und IT-Experten unterstützt Sie individuell bei allen Fragestellungen zu unseren Serviceleistungen. Wir stellen jedes unserer Teams entsprechend den Besonderheiten einzelner Aufträge und den Anforderungen des jeweiligen Auftraggebers zusammen. Höchste Professionalität und das Ziel, optimale Ergebnisse für unsere Mandanten zu erreichen, bestimmen unser Vorgehen.

ÜBER BDO

BDO auf einen Blick

- 1920 in Hamburg gegründet
- Umsatz im Geschäftsjahr 2013: ca. € 195 Mio.
- 24 Standorte
- Über 1.900 Mitarbeiter
- 245 Wirtschaftsprüfer
- 476 Steuerberater
- 112 Rechtsanwälte
- führende mittelständisch geprägte Gesellschaft für Prüfungs-, Steuerberatungs- und Beratungsdienstleistungen
- Gründungsmitglied des internationalen BDO Netzwerks
- Meinungsbildner in den berufsständischen Gremien und Fachausschüssen

Unsere Unternehmensbereiche

Ein wesentlicher Erfolgsfaktor unserer täglichen Arbeit ist, unsere Mandanten dabei zu unterstützen, die Chancen und Risiken entlang der gesamten Wertschöpfungskette jederzeit zu überblicken. Zuverlässige Zahlen und Daten, Leistungen und Lösungen sind unser Angebot. Sie helfen unseren Mandanten, Handlungsoptionen abzuwägen und Maßnahmen zu ergreifen, die es ihnen ermöglichen, ihre Position im Markt zu festigen und auszubauen – für eine optimale Vorbereitung auf künftige Herausforderungen.

Unsere interdisziplinären, sehr versierten und branchenkundigen Teams stehen unseren Mandanten in folgenden Unternehmensbereichen zur Seite:

- Wirtschaftsprüfung und prüfungsnahe Dienstleistungen
- Steuerberatung und wirtschaftsrechtliche Beratung
- Advisory Services

Unsere Standorte in Deutschland

Unsere weltweite Vernetzung

Internationalität ist Teil unserer Tradition. Die BDO wurde 1920 mit Hauptsitz in Hamburg gegründet. Wir sind Gründungsmitglied des internationalen BDO Netzwerkes, das einzige der weltweit tätigen Accountant-Netzwerke mit Sitz in Europa.

Heute ist unser weltweites Netzwerk in weit über 144 Ländern aktiv. Die internationalen Liaison Partner in den jeweiligen Ländern sorgen für schnelle Kontakte rund um den Erdball.

Hinweise an den Leser

Dieses Dokument wurde mit Sorgfalt erstellt, ist aber allgemein gehalten und kann daher nur als grobe Richtlinie gelten. Es ist somit nicht geeignet, konkreten Beratungsbedarf abzudecken, so dass Sie die hier enthaltenen Informationen nicht verwerten sollten, ohne zusätzlichen professionellen Rat einzuholen. Bitte wenden Sie sich an die BDO AG Wirtschaftsprüfungsgesellschaft, um die hier erörterten Themen in Anbetracht Ihrer spezifischen Beratungssituation zu besprechen. BDO AG Wirtschaftsprüfungsgesellschaft, deren Partner, Angestellte, Mitarbeiter und Vertreter übernehmen keinerlei Haftung oder Verantwortung für Schäden, die sich aus einem Handeln oder Unterlassen im Vertrauen auf die hier enthaltenen Informationen oder darauf gestützte Entscheidungen ergeben.

SPRECHEN SIE UNS AN

BDO AG
Wirtschaftsprüfungsgesellschaft

Markus Brinkmann
Partner
Leiter Forensic, Risk & Compliance
Hamburg
Telefon: +49 40 30293-355
markus.brinkmann@bdo.de

Christoph Wunsch
Senior Manager
Forensic, Risk & Compliance
Düsseldorf
Telefon: +49 211 1371-410
christoph.wunsch@bdo.de

www.bdo.de

07/2014