

Mr. Compliance

Leitfaden zur IT-Compliance im Mittelstand

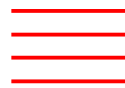
Adressaten: Unternehmensleitung, IT Leitung

Datum: 23.08.2007

Version: 1.0

Nr. 1

Grundlagen



Aus einer Anwaltskonferenz:

Anwalt B: ...

Anwalt C: „Sind in den mittelständischen Unternehmen die Grundlagen und die Zuständigkeiten für Compliance schon hinreichend bekannt?“

Anwältin A: „Es wäre ein Fehler zu glauben, wir wüssten schon alles über IT-Compliance. Das Thema steht noch am Anfang seiner Aufbereitung, und wir lernen jeden Tag dazu.“

Anwalt C: „Das Thema IT-Compliance muss auf ein allgemein verständliches Maß eingedampft und vom Mysterium zur Machbarkeit geführt werden.“

Anwalt B: „Dann lasst uns einen Leitfaden schreiben, der allgemein verständlich ist, und der an den deutschen Mittelstand adressiert ist“.

Anwältin A: „Das kann kein einzelner Leitfaden sein. Das wird eine ganze Serie zum Thema Compliance. Nennen wir die Serie schlicht Mr. Compliance und erklären, dass Mr. Compliance viele Facetten hat. Wir sollten in einem Band die Grundlagen festlegen und dann zu Spezialthemen berichten.“

Anwalt B:



Inhalt

Aus einer Anwaltskonferenz:	2
Vorwort.....	4
Einleitung	5
1. Was sind Compliance und Corporate Governance?.....	5
2. Ist Compliance Pflicht?	6
3. Ist Risikofrüherkennung Pflicht?.....	7
4. Ist Compliance gleich Compliance?.....	7
5. Wer ist zuständig für IT-Compliance?	8
6. Wen soll die Geschäftsleitung zu Compliance befragen?	9
7. Wie funktioniert die Umsetzung von Compliance?.....	9
8. Aus welchen Phasen besteht die Umsetzung?	10
9. Was bringt der Einsatz von Software?	12
10. Wie wird gestartet?	12
Factsheet / Kontaktdaten	14

Vorwort

Die Whitepaper-Serie MR. COMPLIANCE befasst sich mit den unterschiedlichsten Themenfeldern im Compliance-Bereich. Grüne Ausgaben von Mr. Compliance befassen sich schwerpunktmäßig mit technischen und organisatorischen Aspekten im Compliance-Themenfeld. Sie werden von der PRW Consulting GmbH verfasst. Rote Ausgaben von Mr. Compliance bedienen die generellen rechtlichen und managementrechtlich relevanten Aspekte. Sie werden von PRW Rechtsanwälte verfasst. Dieser erste Leitfaden zu IT Compliance (Grundlagen) befasst sich schwerpunktmäßig mit dem Thema, was IT-Compliance tatsächlich ist und wer welche Aufgaben zu übernehmen hat. Diese Publikation kann keine Rechtsberatung ersetzen. Die Whitepaper-Serie hat das Ziel aufzuzeigen, wie Lösungsmöglichkeiten für ein rechtlich abgesichertes IT-Risiko- und Compliance-Management ausgestaltet werden können.

Warum „Mr. Compliance“?

Warum nicht, denn Mr. Compliance ist männlich und weiblich, er ist jung und alt, er ist Inländer und Ausländer zugleich, er ist Datenschutzbeauftragter und leidenschaftlicher Datensammler, er ist IT-Leiter, Informatiker, Organisationstalent, Anwalt, Wirtschaftsprüfer und Topmanager in einem, er ist du, er ist ich. Vor allem ist er eines: ein Mensch, der über viele Profile verfügen muss.

Im Jahre 2005 hat Simone Schnell auf der Informationsplattform von silicon.de in einem Artikel das Berufsbild des Chief Compliance Officers (CCO) zu beschreiben versucht. Ihr Artikel endete mit folgendem Satz: „Beim Durcheinander der Definition von Compliance geht es doch schon los. Wie soll da ein Berufsbild gerahmt werden?“¹ Inzwischen hat sich das Berufsbild des / der Compliance Beauftragten in den so genannten Enterprise oder Global Companies gefestigt. Im deutschen Mittelstand besteht dagegen noch Klärungsbedarf.

RA Wilfried Reiners, MBA

¹ <http://www.silicon.de/enid/cio/12711,1>

Einleitung

Nachhaltiger Unternehmenserfolg ist kein Zufall. Er ist vielmehr das Ergebnis strategischer Planungen und Umsetzungen, verbunden mit einem jahrelangen und fortdauernden Verbesserungsprozesses. In diesem Umfeld sollte auch das Thema IT-Compliance und IT-Risiko-Management (im Folgenden zusammen als „IT-Compliance“ bezeichnet) als Teilbereich platziert werden. Oberstes Ziel von IT Compliance ist somit eine nachhaltige Verbesserung und Sicherung des Geschäftserfolgs. In dieser Leitfaden-Reihe wird an einigen ausgewählten Beispielen modellhaft dargestellt, wie das Thema IT-Compliance bearbeitet werden kann. Das hier dargestellte Modell des sachgerechten IT-Compliance-Management orientiert sich an den so genannten T/O/R-Principles. Die T/O/R-Principles verstehen sich als die Basis des IT-Compliance-Managements in den Dimensionen **T**echnik, **O**rganisation und **R**echt. Die optimale „T/O/R“-Zusammensetzung besteht aus dem richtigen Technikeinsatzes, dem Aufbau einer angemessenen Organisation und der rechtlichen Vorsorge und Überprüfung.

1. Was sind Compliance und Corporate Governance?

„Compliance“ und „Corporate Governance“ haben die Tagespresse erreicht. Börsennotierte Unternehmen haben die Themen „Compliance“ und „Corporate Governance“ weitgehend schon im Griff oder arbeiten an deren Institutionalisierung. Die Diskussion um diese Begriffe hat nun auch den Mittelstand erreicht. Dabei herrscht Unklarheit über die praktische Bedeutung der Begriffe. Das Wort „Compliance“ (englisch für „Befolgung“) bedeutet die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien im Unternehmen. Mit „Corporate Governance“ wird ganz generell der rechtliche und faktische Ordnungsrahmen für die Leitung eines Unternehmens bezeichnet. Wesentlicher Inhalt sind somit der Aufbau einer angemessenen Unternehmensorganisation zur Umsetzung einer optimalen Unternehmensführung und -kontrolle, unter Beachtung von betrieblich oder gesetzlich vorgegebenen Regeln. Der Deutsche Corporate Governance Kodex² stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften dar und enthält international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung. Daraus und aus den allgemeinen Vorschriften - etwa zur sorgfältigen Unternehmensführung - lassen sich in angemessenem Rahmen auch Regeln für den Mittelstand ableiten. Das alles klingt schwierig,

² www.corporate-governance-code.de (aktuelle Fassung vom 17. Juni 2007)

ist es aber nicht. Vor allem ist es nicht gänzlich neu. Niemand wird ernsthaft behaupten, dass der Mittelstand bisher nicht rechtskonform geführt wurde. Ausnahmen gab es und wird es geben. Daran ändern auch neue Begriffe nichts. Dennoch hat das Recht in der IT-gestützten Welt stärkeren Einzug gehalten. Damit tauchen bekannte Regeln in neuem Licht auf und neue Regeln bringen zusätzliche Farbtupfer.

Feststeht, dass sich die IT in den letzten 20 Jahren immer stärker in die Abwicklung der Unternehmensprozesse eingebracht hat. IT-Compliance bedeutet dabei zunächst, dass auch im IT-Umfeld des Unternehmens, das heißt in allen Bereichen, in denen IT zur Anwendung kommt (z. B. im Bereich der E-Mail-Systeme), die rechtlichen Rahmenbedingungen (z. B. Post-/ Fernmeldegeheimnis und Datenschutz) eingehalten werden. Unter IT-gestützter Compliance wird hier die Überprüfung der Einhaltung von Compliance Vorschriften mittels IT (in der Regel Software) verstanden (z. B. im Rahmen des Risikomanagements oder des Monitorings von Applikationen).

Alte und neue Vorschriften werden sprachlich in den folgenden Ausführungen einheitlich als Compliance-Vorschriften bezeichnet.

2. Ist Compliance Pflicht?

In der Literatur³ wurde schon im Jahr 2005 eine allgemeine Rechtspflicht zur Einrichtung einer Compliance Organisation für alle Unternehmen behauptet. Dem wurde entgegnet, dass die existierenden spezialgesetzlichen Vorschriften nicht ausreichen, um daraus eine für alle Unternehmen existierende Verpflichtung zur Einrichtung einer Compliance-Organisation abzuleiten⁴.

Dies darf aber nicht davon ableiten, dass es sich hierbei um eine Diskussion über die Notwendigkeit der Compliance-Organisation handelt. Völlig unbestritten ist, dass die Einhaltung der Gesetze eine Unternehmenspflicht darstellt, für deren Einhaltung die Unternehmensleitung zuständig ist.

³ Schneider, ZIP 2003, 645

⁴ Hauschka, ZIP 2004, 877

3. Ist Risikofrüherkennung Pflicht?

Die gesetzliche Verpflichtung zur Risikofrüherkennung und zur Integration eines Überwachungssystems ist durch das KonTraG⁵ eingeführt worden. Das KonTraG ist ein umfangreiches Artikelgesetz, das der Deutsche Bundestag am 5. März 1998 verabschiedete. Es trat am 1. Mai 1998 in Kraft. Ziel des KonTraG ist es, die Corporate Governance in deutschen Unternehmen zu verbessern. Deshalb wurden mit diesem Artikelgesetz etliche Vorschriften aus dem Handels- und Gesellschaftsrecht verändert. Das KonTraG präzisiert und erweitert dabei hauptsächlich Vorschriften des HGB (Handelsgesetzbuch) und des AktG (Aktiengesetz). Mit dem KonTraG wurde die Haftung von Vorstand, Aufsichtsrat und Wirtschaftsprüfern in Unternehmen erweitert. Kern des KonTraG ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben, sowie Aussagen zu Risiken und Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen.⁶ So heißt es in § 91 AktG Abs. 2: *„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“*. In der Gesetzesbegründung⁷ heißt es, dass für eine GmbH je nach Größe und Komplexität ihrer Struktur nichts anderes gilt. Eine konkrete Ausprägung zur Umsetzung und Beschaffenheit eines solchen Überwachungssystems hat der Gesetzgeber nicht eingebracht. Im Zweifel verstößt somit die fehlende Umsetzung eines Risikofrüherkennungssystems schon gegen das geltende Recht. Das Unternehmen erfüllt damit auch nicht die Compliance-Anforderungen.

4. Ist Compliance gleich Compliance?

In nahezu allen Publikationen zum Thema Compliance werden Vorschriften genannt, die es gelte umzusetzen, die jedoch für über 90 % der deutschen Unternehmen nicht zutreffen. So wird etwa immer wieder auf die Notwendigkeit verwiesen SOX (Sarbanes-Oxley Act⁸) zu integrieren. SOX ist ein US Gesetz und nur relevant für Unternehmen, die an US-Börsen notiert sind, oder für deren Tochterunternehmen. Die meisten Mittelständler erfüllen diese Grundvoraussetzung der Anwendbarkeit der SOX-Vorschriften nicht. Zunächst hat ein Unternehmen also einmal festzustellen, welche Compliance-Vorschriften für das eigene Unternehmen gelten. Neben den

⁵ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

⁶ www.wikipedia.de

⁷ RegE KonTraG 1997 Begründung zu § 91 Abs. 2 AktG

⁸ Der Sarbanes-Oxley Act wurde am 30. Juli 2002 in Kraft gesetzt.

zutreffenden Gesetzen sind zudem die bereits existierenden Richtlinien und Handlungsempfehlungen von BSI⁹, ISO-Standards, ITIL¹⁰, COBIT¹¹, IDW PS 330¹² etc. zu beachten. Der Weg dahin ist nicht einfach, aber durchaus mit überschaubarem Aufwand gangbar.

5. Wer ist zuständig für IT-Compliance?

Die Einhaltung von Compliance-Vorschriften und damit die Rechtskonformität des Unternehmens ist Sache der obersten Führungsebene, also in der Regel der Geschäftsführung oder des Vorstandes. Zwar kann die Einhaltung der Compliance-Vorschriften delegiert werden, die Delegation erfordert allerdings ihrerseits wieder, dass die Auswahl des/der Compliance-Beauftragten sorgfältig erfolgt, dass ein regelmäßiges Reporting an die Unternehmensspitze und eine Kontrolle dieser Schlüsselposition erfolgen. Hier einige Beispiele für die Säulen der IT-Compliance.



Abbildung 1

⁹ Bundesamt für Sicherheit in der Informationstechnik (www.BSI.de)

¹⁰ Im Auftrag der britischen Regierung entwickelter Leitfaden IT Infrastructure Library.

¹¹ Generisches Prozessmodell: Control Objectives for Information and related Technologies (COBIT)

¹² Institut der Wirtschaftsprüfer. Abschlussprüfung bei Einsatz von Informationstechnologie



6. Wen soll die Geschäftsleitung zu Compliance befragen?

Bei der Umsetzung von Compliance-Vorschriften treten für die Geschäftsleitungen und Vorstände in mittelständischen Unternehmen nicht selten folgende Konstellationen auf.

Fragt die Geschäftsleitung einen Hersteller, wie Compliance umzusetzen ist, dann bekommt sie technische Daten von Hardware, Software und Applikationen als Antwort. Fragt sie einen Consultant, erhält sie Ausführungen, in denen zumindest Begriffe wie Verfügbarkeit, Vertraulichkeit, Authentizität, Autorisierung, Integrität, Rechtskonformität, Zurechenbarkeit, Effektivität und Effizienz - mit Glück in deutscher Sprache - in der Regel aber in Anglizismen verpackt, auftauchen. Fragt sie den Hausjuristen, antwortet dieser häufig, dass er sich im IT-Recht nicht auskenne. Fragt sie ihren eigenen IT-Verantwortlichen, erntet sie schon mal ein Lächeln, verbunden mit dem Hinweis, dass die Firma mit Blick auf das IT-Budget sich das, was sie gerne hätte, nicht leisten könne. Schließlich schaut die Geschäftsleitung nach im Markt verfügbaren technischen Tools und stellt fest, dass diese zwar existieren, aber auf die Größe ihres Unternehmen nicht anwendbar sind. Das was bleibt, sind Frustration und Ärger auf die Gesetzgebung. Das muss nicht sein. Die erste Erkenntnis, die sich durchsetzen muss, ist, dass Compliance Teamarbeit ist.

Nach der hier vertretenen Auffassung ist die Umsetzung von Compliance-Regelungen eine Aufgabe, die mehrere Personen inhaltlich befassen muss. Dem Compliance-Verantwortlichen müssen dabei unterschiedliche Profile zur Aufgabenerledigung beigelegt werden.

7. Wie funktioniert die Umsetzung von Compliance?

Das Wichtigste zuerst: Die Umsetzung von Compliance ist ein Projekt. An diesem Projekt, das aus drei Phasen und einer ständigen Nachkontrolle (Audit) besteht, sind mehrere Personen beteiligt. Der Autor empfiehlt, dass sich das Management gemeinsam mit der IT-Leitung, der Rechtsabteilung (oder einem erfahrenen IT-Anwalt oder -Anwältin), dem/der Datenschutzbeauftragten und gegebenenfalls den Leitern/Leiterinnen der Fachabteilungen einen Überblick verschafft und die für das eigenen Unternehmen relevanten Regelungen benennt. Dann folgen die weiteren Schritte der Umsetzung und die Abbildung der spezifischen Anforderungen in konkrete IT-Aktivitäten und regelmäßige Audits.

Der Umsetzung von Compliance-Projekten werden häufig Schwachstellen-Audits sowie Security-Strategie- und Prozessberatung oder technische Risikoanalysen vorgeschaltet. Dies dient vor allem der Klärung, welche Applikationen sich auf welchem Sicherheitsniveau befinden.

8. Aus welchen Phasen besteht die Umsetzung?

In der ersten Phase (Analyse) müssen zunächst die für das Unternehmen relevanten Compliance-Vorschriften ermittelt werden. Dabei gilt folgende aus der Erfahrung gewonnene Faustregel, etwa 70 % der relevanten Vorschriften sind für alle Unternehmen gleich, die restlichen 30 % ergeben sich aus dem betrieblichen Zweck des Unternehmens. Die rechtliche Anforderungen an die Unternehmen, die Unternehmensleitungen sowie an die Mitarbeiterinnen und Mitarbeiter ergeben sich entweder aus formellen Gesetzen (z. B. GmbHG, Aktiengesetz, Steuergesetzen, HGB bzw. Handelsgesetzbuch), aus Anforderungen der Verwaltung (etwa Rundschreiben, Richtlinien) oder aber aus allgemeinen Richtlinien und Standards (wie zum Beispiel DIN und ISO). Zwar haben gerade letztere Vorschriften keinen unmittelbaren Rechtscharakter, sie können aber sehr wohl zur Auslegung und als Maßstab herangezogen werden, zum Beispiel bei der Frage des Verschuldens, ob bestimmte IT-Infrastrukturen ein angemessenes IT-Sicherheitsniveau aufweisen.

Vergleichen wir ein Krankenhaus, einen Online-Computerhändler und einen Verlag, der ein Gesellschaftsmagazin verlegt. Alle drei Betriebe werden als GmbH geführt.

Für alle drei Betriebe gelten z.B. die gleichen Vorschriften aus dem GmbHG, dem Steuerrecht, aus dem Datenschutzrecht und aus den allgemeinen Vorschriften etc. Für das Krankenhaus gelten darüber hinaus gesetzliche Vorschriften aus dem ärztlichen Berufsrecht. So entspricht etwa ein per einfacher E-Mail vom Krankenhaus an den niedergelassenen Arzt gesendeter Arztbrief nicht der gesetzlich vorgeschriebenen Form, denn hier ist die persönliche Unterschrift des Arztes notwendig. Diese Unterschrift kann nur durch eine qualifizierte Signatur abgebildet werden. Zudem könnte die unverschlüsselte Übertragung gegen das gesetzliche Verschwiegenheitsgebot des § 203 Strafgesetzbuch verstoßen. Für den Online-Computerhändler ist es wichtig, dass er z. B. die Vorschriften zum Fernabsatzgesetz kennt. Für den/die Journaliste(i)n des Gesellschaftsmagazins wird es wichtig sein, dass bei einer Online-Kommunikation der Informantenschutz und die Pressefreiheit gewahrt werden.

Daraus ergibt sich die Erkenntnis, dass Compliance sich nicht aus einem immer gleichen Gesetzkatalog zusammensetzt, sondern dass die einschlägigen Vorschriften erst in der Analyse ermittelt werden.

In der zweiten Phase (Transformation) müssen die relevanten Vorschriften auf die IT-gestützten Prozesse übertragen werden. Am Ende werden eine Richtlinie oder ein Rechtskatalog erstellt, der für alle Mitarbeiterinnen und Mitarbeiter als gültiger Kodex für gesetzmäßiges und verantwortungsbewusstes Handeln im Unternehmen festgelegt wird. Damit bekennen das Unternehmen und die Mitarbeiterinnen und Mitarbeiter sich zur Rechtstreue. Dieser Schritt ist aber eine Herausforderung für das Compliance-Team, denn während es einige Gesetze gibt, die ihre Anforderungen an die IT recht präzise definieren (z. B. das Bundesdatenschutzgesetz in § 9 mit Anlage), sind andere Vorschriften schwieriger umsetzbar. Hierzu gehört etwa die Klärung der Frage, welches IT-Sicherheitsniveau den Anforderungen „der Sorgfalt eines ordentlichen Geschäftsmannes“ im Sinne von § 43 GmbHG oder § 93 AktG entspricht.

In der dritten Phase (Integration) wird die Einhaltung der relevanten Vorschriften als ge- und überprüfte Selbstverständlichkeit in den Regelbetrieb überführt.

Da sich auch Gesetze und Vorschriften ändern, sollte nach einer gewissen Zeit ein Audit durchgeführt werden.

Danach ergibt sich folgender Regelkreislauf:

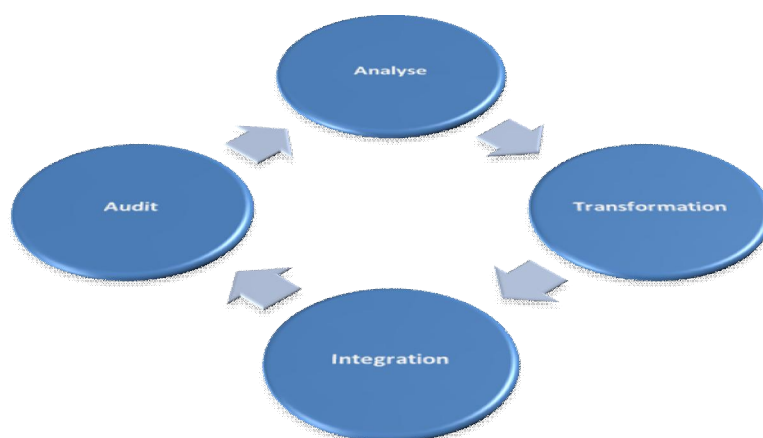
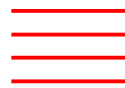


Abbildung 2



9. Was bringt der Einsatz von Software?

Für die mittelständischen Unternehmen wird die einfache Umsetzung der relevanten Compliance-Vorschriften im Vordergrund stehen. Zumindest für den Bereich der Risikofrüherkennung drängt sich daher die Frage auf, ob der Einsatz von Software zu empfehlen ist. Nach den heutigen gesetzlichen Anforderungen müssen gravierende Risiken so früh erkannt werden, dass noch geeignete Maßnahmen zu Abwehr getroffen werden können. Dazu müssen die relevanten Informationen nicht nur frühzeitig vorliegen, sondern sie müssen auch aktuell und abrufbar sein. Hier bleiben nur wenige Organisationsmittel übrig, um diese Anforderungen nicht nur unter rechtlichen, sondern vor allem auch unter betriebswirtschaftlichen Gesichtspunkten zu erfüllen¹³. Der Einsatz einer geeigneten Software ist dabei das wohl effektivste Mittel. Damit stellt sich also nicht die Frage, ob der Einsatz einer Software sinnvoll ist, sondern vielmehr welche Software in jeweiligen Fall die richtige Lösung ist. Dies lässt sich pauschal nicht im Vorhinein feststellen, für das kleinere Unternehmen kann hier schon ein clever entwickeltes Eigenprodukt ausreichen, für größere Unternehmen sind dies auch schnell Tools, die bei weit über EUR 100.000,00 liegen.

10. Wie wird gestartet?

Architekturstufe

In der ersten Phase ist das Projektteam zu bestimmen, das für die IT-Compliance verantwortlich ist. Der nächste Schritt ist eine umfassende Überprüfung der IT-Infrastruktur und ihrer Prozesse. Dabei ist der T/O/R-Ansatz eine pragmatische und in der Praxis erprobte Methode. Darin werden zunächst systematisch die technischen und organisatorischen Bereiche der IT aufgenommen und analysiert. Sodann werden die Möglichkeiten der Verbesserung der Planungssicherheit im Sinne einer Früherkennung der Risiken aufgezeigt und mit dem unter Kostengesichtspunkten Machbaren in Relation gesetzt. Es folgt die rechtliche Überprüfung mit dem Ziel, die rechtlich relevanten Bereiche zu identifizieren und ein Konstrukt zu erreichen, bei dem die Haftungsrisiken ausgeschlossen werden.

Entscheidend für die Priorität bei der Umsetzung von Maßnahmen ist die konsolidierte Risikoanalyse, die sich aus den Einzelanalysen der Bereiche Technik, Organisation und Recht zusammensetzt. Auf diese Art wird mit einer konsolidierten IT-Sicherheitsanalyse der Grundstein für

¹³ vgl. Schlaghecke S. 296 in Hauschka, Corporate Compliance (Beck Vlg.)



ein IT-Risiko-Management gelegt, worüber die Einhaltung der für die IT relevanten Compliance-Vorschriften sichergestellt wird.

Umsetzungsstufe

In der nächsten Stufe ist zu prüfen, welche Softwaretools für die Umsetzung der definierten Anforderungen die beste Unterstützung leisten können. In der Folge werden Testbetrieb, Echtbetrieb und Auditierungen die nächsten Meilensteine markieren.

Hinweis:

Wenn Sie Anregungen haben, anderer Meinung sind oder Fragen zur Umsetzung haben, nehmen Sie bitte Kontakt zu uns auf. Wir freuen uns auf den Dialog.

Factsheet / Kontaktdaten

PRW Rechtsanwälte

PRW RECHTSANWÄLTE hat sich auf ausgewählte Gebiete des nationalen und internationalen Wirtschaftsrechts spezialisiert, der in erheblichem Umfang auch den Bereich der Compliance-relevanten Vorschriften umfasst. Der Branchenfokus der Kanzlei liegt auf der Informationstechnologie in den Bereichen Hardware, Software und Dienstleistungen. Die Anwältinnen und Anwälte können alle auf eine Zusatzausbildung verweisen, die meisten davon basieren auf dem IT-Umfeld (Fachanwalt für Informationstechnologie, LL.M., MBA). Profile der einzelnen Anwältinnen und Anwälte können gerne bereitgestellt werden.

Autor

Rechtsanwalt Wilfried Reiners, MBA

Studium der Rechts- und Wirtschaftswissenschaften in München und San Diego (MBA).

Nach einer mehrjährigen Tätigkeit für eine internationale Unternehmensberatung ist er seit 1989 zur Anwaltschaft zugelassen. Wilfried Reiners ist heute Managing Partner von PRW Rechtsanwälte in München und Geschäftsführer der PRW Consulting GmbH.

RA Reiners ist seit 18 Jahren auf die Beratung im die IT-Umfeld spezialisiert und hat zahlreiche Veröffentlichungen zum IT-Recht publiziert. Seit 1998 ist er Lehrbeauftragter an der Europäischen Privathochschule MUNICH BUSINESS SCHOOL für die Fächer IT Law and Management Liability.

Mitgliedschaften:

EuroITcounsel Ltd. London (Director of the board)

Arbeitsgemeinschaft IT-Anwälte im Deutschen Anwaltsverein

Deutsche Gesellschaft für Recht und Informatik e.V.

Computer Law Association; (heute TechLaw)

Kontakt Daten

PRW Rechtsanwälte

Steinsdorfstraße 14

D-80538 München

Telefon: +49 - (0) 89 - 21 09 77-0

Telefax: +49 - (0) 89 - 21 09 77-77

E-Mail: office@prw.de; web: www.prw.info