ASSURANCE MAGAZIN

Sicherheit für Unternehmen / Heft 5 / Mai 2015

Schwerpunktthema in dieser Ausgabe:

Sicherheits-management

Sicherheitsgefährdende Ereignisse in einem Unternehmen treten in der Regel unerwartet ein. Dann ist augenblicklich schnelles, durchdachtes und zielgerichtetes Handeln gefragt.

- **Gewalt am Arbeitsplatz**
  Ein unterschätztes Phänomen?!
- **Unternehmenssicherheit ist Chefsache**
  Entscheidungsträger müssen persönlich haften.
- **Advanced Cyber Defense**
  Bedrohung durch Cyberangriffe minimieren.
- **Cyber Incident Response**
  Im Ernstfall gut vorbereitet zur richtigen Entscheidung.

KPMG
cutting through complexity

Bestellen Sie Ihr kostenfreies Online-Exemplar:
www.kpmg.de/magazinassurance

Inhalt

Impressum

Herausgeber:
KPMG AG Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18, 10785 Berlin

Redaktion und Projektleitung:
Dr. Antonia Steßl (V. i. S. d. P.)
Ganghoferstraße 29
80339 München
T +49 89 9282-4276
astessl@kpmg.com

Gestaltung:
d17 Corporate Media Design, Berlin

Druck:
Druckerei Arnold, Großbeeren

Sind Sie sicher?!

Nichts ist so beständig wie der Wandel. Auch 2015 sind die Worte des Philosophen Heraklit von Ephesos hochaktuell. Gerade im Bereich der Unternehmenssicherheit – dem Schwerpunktthema dieser Ausgabe – ist ein hohes Maß an Flexibilität gefordert, um die immer neuen Gefahrenherde zu beherrschen. Das Zeitalter der Globalisierung und Digitalisierung beflügelt geradezu kriminelle Kreativität und Möglichkeiten, wenn es etwa um Produktpiraterie, Cyber Crime oder Industriespionage geht. Hinzu kommt weiterer Druck seitens des Gesetzgebers, der Entscheidungsträger für Pflichtverletzungen in die persönliche Haftung nimmt. Die Autoren unserer Schwerpunktartikel bringen es auf den Punkt: Unternehmenssicherheit muss Chefsache sein.

Wir erläutern auf den folgenden Seiten, worauf es bei Unternehmenssicherheit ankommt: ein zuverlässiges Risikomanagement und ein ganzheitlich angelegtes Security Management-System. In Verbindung bieten sie Schutz für Unternehmen, Entscheidungsträger und Kerngeschäft. Orientierung bei der Entwicklung eines Security Managements bieten zum einen die Unternehmensziele und zum anderen die Grundsätze einer ordnungsgemäßen Prüfung von Compliance Management-Systemen nach IDW PS 980. Spezielle Information Security Management-Systeme helfen Unternehmen bei der frühzeitigen Erkennung von Angriffen, der besseren Einschätzung von Schäden sowie der Schadenminimierung von Cyberangriffen. Denn: 20 Prozent der weltweiten Wertschöpfung über das Internet gehen durch Cyberkriminalität verloren.

Konzern- und Unternehmenssicherheit – das heißt auch Krisenmanagement. Ob unverschuldete oder selbst verschuldete Krise, der Ausgang lässt sich nur in den wenigsten Fällen im Vorhinein abschätzen. Unser Health Care-Autorenteam zeigt Ihnen die größten Herausforderungen an ein professionelles Krisenmanagement in Krankenhäusern auf. Wer sich vertiefend mit Compliance im Gesundheitssektor beschäftigen möchte, dem sei unser Artikel zu den neuen Transparenzregelungen für finanzielle Zuwendungen der Arzneimittelhersteller an Ärzte ans Herz gelegt. Die Einhaltung der komplexen, international heterogenen Vorschriften erfordert hier einen integrierten Compliance-Ansatz.

Auch unser Autor Florian Maciuca rückt die Bedeutung eines ganzheitlichen Compliance Management-Systems in den Vordergrund und fragt: Compliance vorhanden, Prüfung bestanden? In seinem Artikel beleuchtet er die unabhängige und wirksame Überwachung des CMS und die Rolle der Internen Revision als unternehmenseigene und prozessunabhängige Kontrollinstanz.

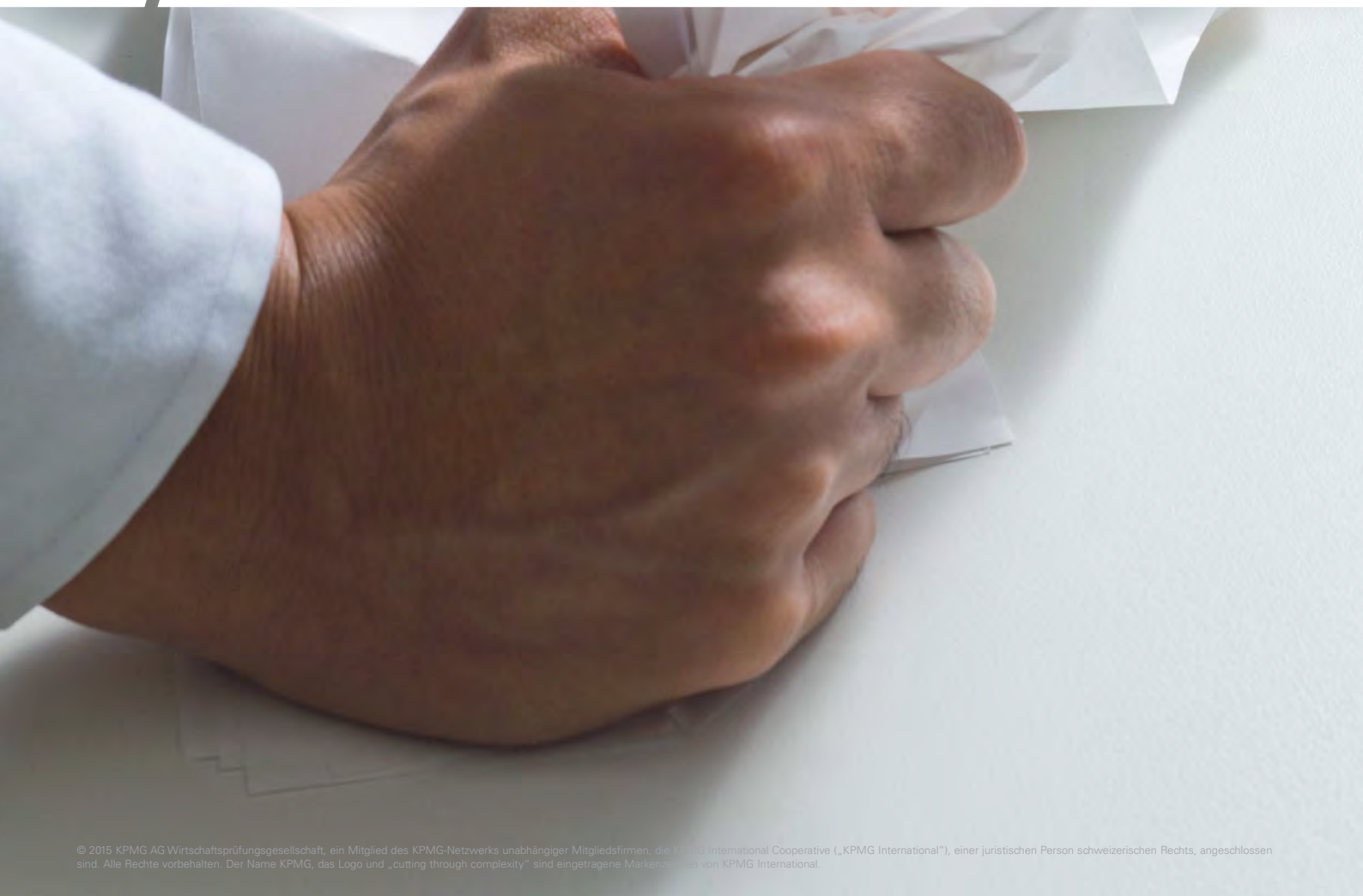
Zudem hält die aktuelle Ausgabe zwei spannende Interviews für Sie bereit: Dr. Jan-Hendrik Gnändiger, Senior Manager im Geschäftsbereich Governance & Assurance Services, beantwortet Fragen zur Steuerung von Tax Compliance-Risiken und zur Assurance durch Bescheinigungen. Everhard von Groote, Geschäftsführer der Team Psychologie & Sicherheit (TPS) GmbH, gibt Antworten zu Bedrohungsmanagement und Gewalt am Arbeitsplatz.

Schließlich betrifft der anfangs erwähnte beständige Wandel auch die Energiewende. Sie fordert Veränderungen bei Unternehmen wie Prüfern und unterstreicht mehr denn je die Bedeutung interdisziplinärer Prüfungsteams.

Ich wünsche Ihnen viel Spaß bei der Lektüre unseres Assurance Magazins.

Ihr
Jens C. Laue
Head of Governance & Assurance Services, KPMG

Der Amokläufer von Pforzheim tötete eine Kollegin mit einem Samuraischwert und verletzte drei weitere Frauen schwer. Ein Einzelfall? Immer wieder kommt es im Arbeitsumfeld zu Gewalt. Im Interview beleuchtet Dr. Everhard von Groote das oft unterschätzte Phänomen, zeigt persönliche und wirtschaftliche Konsequenzen auf und wirbt dafür, dem Thema und der Prävention von Gewalt im Unternehmen mehr Aufmerksamkeit zu schenken.



Gewalt am Arbeitsplatz Ein **unterschätztes** Phänomen?!

Interview mit Everhard von Groote,
Geschäftsführer der Team Psychologie & Sicherheit (TPS) GmbH

Kann man Amokläufe noch als amerikanisches Phänomen bezeichnen?
Dr. Everhard von Groote Nein, die oft vertretene These, dass das Phänomen Amok ein amerikanisches sei und mit Deutschland nur wenig zu tun habe, gilt unter Wissenschaftlern als nicht mehr haltbar – zu Recht: Im November letzten Jahres tötete beispielsweise eine entlassene Mitarbeiterin eines Hamburger Reisebüros ihre ehemalige Kollegin mit fünf Messerstichen. Im Februar erschoss ein 22-Jähriger zwei ehemalige Arbeitskollegen. Im März erschoss ein 23-jähriger Soldat seinen Vorgesetzten und anschließend sich selbst. Diese Einzelfälle ließen sich fortsetzen. Eine Untersuchung der Universität Würzburg zu den Amokläufen der letzten zehn Jahre kam sogar zu dem Ergebnis, dass es in diesem Zeitraum in Europa mehr Fälle gab als in Nord- und Südamerika zusammen!

„Gewalt bei der Arbeit ist **ein gleichsam verbreitetes wie tabuisiertes Phänomen**. Laut einer niederländischen Befragung werden vier Prozent aller Arbeitnehmer Opfer von Gewalt am Arbeitsplatz."

Wie macht sich Gewalt am Arbeitsplatz in Deutschland bemerkbar?
Dr. Everhard von Groote Gewalt am Arbeitsplatz muss nicht immer Amok sein: Gewalt bei der Arbeit ist ein gleichsam verbreitetes wie tabuisiertes Phänomen. Betroffen sind besonders Berufsgruppen, die Kontakt zur Öffentlichkeit haben, mit Geld umgehen oder allein arbeiten. Nach einer EU-Studie werden jedes Jahr etwa zwei Prozent aller Arbeitnehmer Opfer von Gewalt am Arbeitsplatz – sei es von Kollegen oder von Kunden. Eine niederländische Befragung geht gar von vier Prozent Betroffenen aus. Die Folgen für die Unternehmen sind beträchtlich: Leistungseinbrüche oder Fehlzeiten aufgrund von posttraumatischen Stresserkrankungen, sinkende Produktivität oder auch Reputationsschäden für das Unternehmen.

Wie äußert sich die Gewalt am Arbeitsplatz?
Dr. Everhard von Groote Gewalt am Arbeitsplatz kommt insbesondere in Form von psychischer Gewalt vor. Hier sind neben Mobbing auch das in den letzten Jahren verstärkt erforschte Stalking sowie Drohungen aller Art zu nennen. Eine noch unveröffentlichte Studie der Universität Darmstadt zeigt, dass Stalking, also besessenes Verfolgen einer Person gegen ihren Willen, sehr häufig auf den Arbeitsbereich übergreift. Die Betroffenen, häufiger Frauen als Männer, sind aufgrund der psychischen Folgen des Stalkings im Durchschnitt 60 Tage im Jahr krank-

Dr. Everhard von Groote
Geschäftsführer der
Team Psychologie & Sicherheit GmbH

Die TPS GmbH hat sich auf die Beratung von Unternehmen in der Prävention und im Umgang mit Gewalt am Arbeitsplatz spezialisiert. Die Psychologen des Unternehmens helfen Firmen, Fälle von Gewalt und Bedrohungen zu erkennen und zu managen.

„Die oft vertretene These, dass Amok ein amerikanisches Phänomen ist und mit Deutschland nur wenig zu tun hat, ist **nicht mehr haltbar**."

geschrieben! Doch auch Drohungen gegenüber Kollegen und Vorgesetzen haben in den letzten Jahren stark zugenommen. Dem Druck der heutigen Arbeitswelt sind viele nicht gewachsen. Wenn berufliche und persönliche Krisen zusammenkommen, ist die Kurzschlussreaktion vorprogrammiert.

Forscher sehen die Gründe, warum am europäischen Arbeitsplatz psychische Gewalt vorherrscht, vor allem in der Wirtschaftsstruktur. Mobbing gedeiht dort, wo Jobs relativ sicher sind, während Entlassungen mit höherer Wahrscheinlichkeit Drohungen oder Gewaltreaktionen hervorrufen. Nicht alle Drohungen sind als tatsächliche Ankündigung von Verhalten anzusehen, aber Personal- und Rechtsabteilungen sind mit der Einschätzung und dem Umgang mit dem jeweiligen Einzelfall oft überfordert. Der Grund liegt auf der Hand: Das Phänomen der Gewalt am Arbeitsplatz wurde in Deutschland bisher stark unterschätzt.

„Gewalt am Arbeitsplatz kann **Leistungseinbrüche**, **Fehlzeiten**, **sinkende Produktivität** oder auch **Reputationsschäden** für das Unternehmen nach sich ziehen."

Worin besteht die größte Herausforderung im Umgang mit Gewalt am Arbeitsplatz?

Dr. Everhard von Groote Wir reden hier nicht von einem Kavaliersdelikt. Vielmehr handelt es sich um einen strafrechtlichen Tatbestand, der entsprechend von der Rechts- und Personalabteilung eines Unternehmens erfasst und geahndet werden muss. Wie bei der öffentlichen Strafverfolgung durch die Polizei steht und fällt der Erfolg auch hier mit Zeugenhinweisen und schließlich der nachweisbaren Straftat.

Welche Maßnahmen empfehlen Sie, um Gewalt am Arbeitsplatz entgegenzuwirken?

Dr. Everhard von Groote Ein anonymes Hinweisgebersystem zur Meldung beobachteter Straftaten oder allgemeiner Missstände bildet bereits in einigen Unternehmen eine gute Voraussetzung. Über dieses Medium können die Mitarbeiter ohne Furcht vor Konsequenzen Informationen an die verantwortlichen Stellen weitergeben, sodass eine interne Ermittlung angestoßen werden kann. Da Mitarbeitern, die Opfer oder Zeugen geworden sind, die Angst vor persönlichen Konsequenzen entweder durch Kollegen oder in Form von Sanktionen durch Vorgesetzte genommen werden muss, steht die Unabhängigkeit dieser Position im Vordergrund. In der Praxis wird diese Stelle daher oft durch einen unabhängigen Dritten – den sogenannten Ombudsmann – ausgefüllt, der im klassischen Fall einen juristischen Hintergrund hat und losgelöst von Unternehmensinteressen Hinweise aufnimmt. Darauf folgt idealerweise eine erste Einschätzung von einem ausgebildeten Bedrohungsmanager.

Was sind die Aufgaben eines Bedrohungsmanagers?

Dr. Everhard von Groote Neben der Einrichtung einer solchen Stelle inklusive Aufbau- und Ablauforganisation ist ihre Zuständigkeit zu definieren und an alle Mitarbeiter des Unternehmens zu kommunizieren. Nur so kann der Bedrohungsmanager präventiv und wirksam tätig werden. Bislang wissen betroffene Mitarbeiter oft überhaupt nicht, an wen sie sich wenden können, werden im schlimmsten Fall gar von der Compliance-Hotline, die sich für nicht zuständig erachtet, abgewiesen. Mitarbeiter müssen also wissen, an wen sie sich wenden können. Sie müssen darauf vertrauen können, dass sich unternehmensintern jemand ihrer Sache annimmt und dass auch spürbare Konsequenzen erfolgen.

„Mitarbeiter müssen **wissen, an wen sie sich wenden können**. Bislang werden sie im schlimmsten Fall gar von der Compliance-Hotline abgewiesen.“

Aufseiten des Bedrohungsmanagers ordne ich vor allem der Bewertung der eingehenden Hinweise einen hohen Stellenwert zu. Denn Drohungen und Gefährlichkeit sind zwei sehr unterschiedliche Dinge, die von einem dafür fortgebildeten Mitarbeiter sorgsam bewertet werden müssen. Dann erfolgt ein Fallmanagement, also ein koordiniertes Vorgehen mit dem Ziel, Gefährdungen zu reduzieren und ein sicheres Umfeld zu gewährleisten.

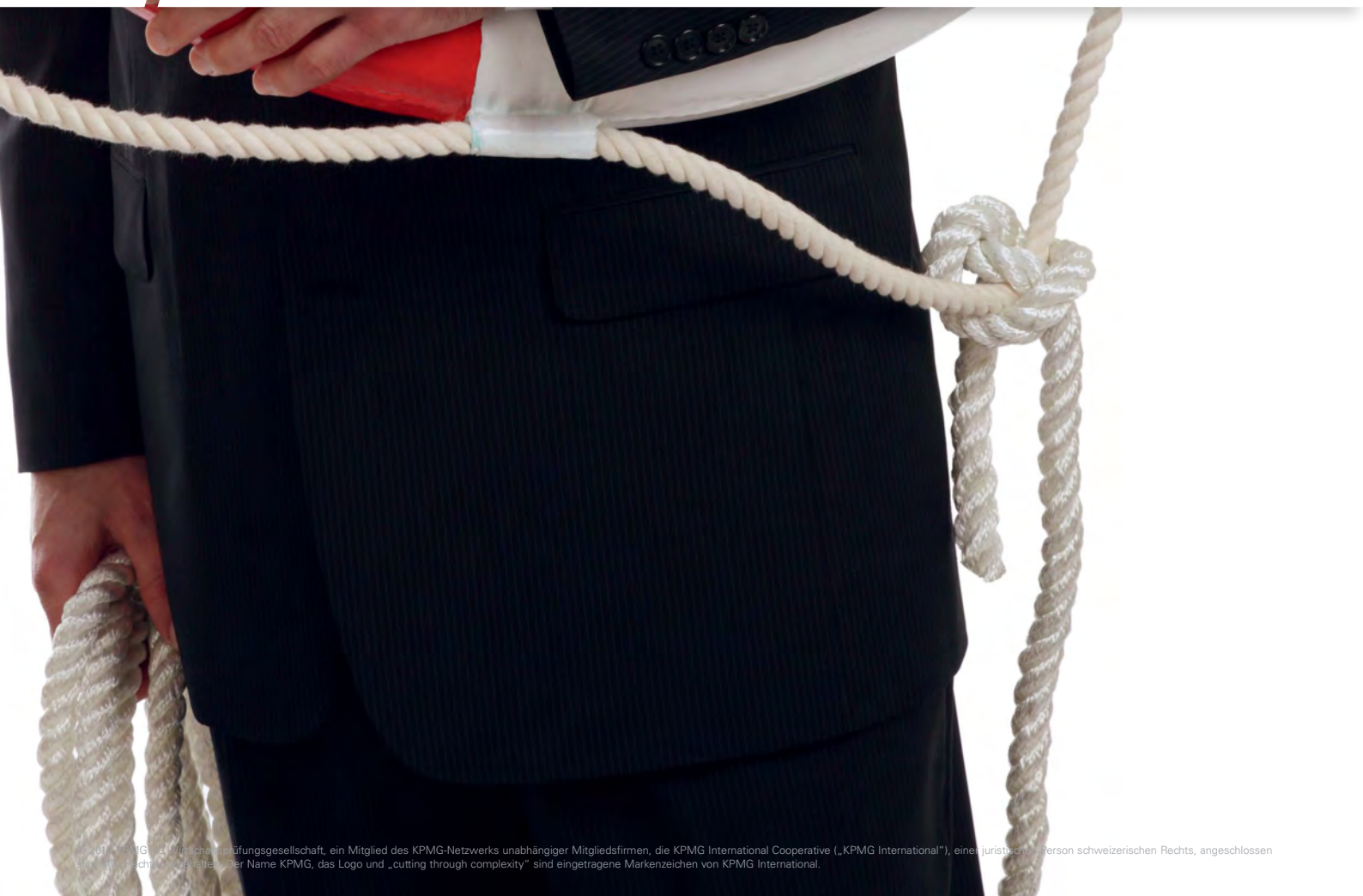
„**Mobbing** gedeiht dort, wo Jobs relativ sicher sind, während Entlassungen mit höherer Wahrscheinlichkeit **Drohungen oder Gewaltreaktionen** hervorrufen.“

Worauf ist beim Bedrohungsmanagement zu achten?

Dr. Everhard von Groote „Erkennen – Einschätzen – Entschärfen“ ist das Prinzip des psychologischen Bedrohungsmanagements. Es geht darum, Eskalationsgefahren möglichst früh zu erkennen, sie einzuschätzen und schließlich das Risikopotenzial zu entschärfen. Im Fokus stehen Eskalationsgefahren, die von einzelnen Personen oder Gruppen ausgehen. Der Empfänger der Hinweise muss die erhaltenen Informationen ganzheitlich auswerten. Er darf sich weder auf einzelne Hinweise versteifen, noch angesichts vieler Hinweise die Details aus den Augen verlieren. Das Zusammenspiel einzelner Merkmale und Auffälligkeiten bildet schlussendlich ein Muster, das der verantwortliche Ermittler auszuwerten und zu interpretieren hat.

Dr. Antonia Steßl
Manager, Governance & Assurance Services, KPMG
Stefan Trütner
Governance & Assurance Services, KPMG

Während Diebstahl, Unterschlagung, Bilanzfälschung, Industriespionage und Korruption bekannte Delikte sind, haben Globalisierung und moderne Informations- und Kommunikationstechnologien neue Delikte wie Produktpiraterie, Cyberkriminalität und Geldwäsche oder sogar Entführung und Erpressung auf den Plan der Konzernsicherheit gebracht. Ein ganzheitlich angelegtes Security Management-System schützt auch die Entscheidungsträger.



Unternehmenssicherheit ist **Chefsache**

Entscheidungsträger müssen **persönlich haften**.

Konzernsicherheit ist längst kein Synonym mehr für Betriebsfeuerwehr. Die Gefahrenherde sind vielfältig, die materiellen und immateriellen Schäden können immens sein. Und als hätten die Unternehmen damit nicht genug zu tun, erwartet der Gesetzgeber auch noch einen regelmäßigen Nachweis der Wirksamkeit der Schutzsysteme.

Gestiegene Haftungsrisiken

Bislang konzentrierten sich beinahe alle Maßnahmen der Konzernsicherheit auf die frühzeitige Identifizierung und Bewertung von Sicherheitsrisiken und -schwachstellen sowie auf die Ableitung, Entwicklung und Implementierung angemessener Maßnahmen. Schon zur Umsetzung dieser Maßnahmen bedarf es eines Umfelds, in dem alle relevanten Sicherheitsrisikobereiche identifiziert und bewertet sind – es braucht ein Security Management-System, damit die Unternehmenssicherheit nicht vom Kerngeschäft ablenkt. Das umso mehr, als die gesetzlichen Anforderungen an Unternehmen und insbesondere die gesellschaftlichen und persönlichen Haftungsrisiken steigen: So schreibt § 93 Aktiengesetz die Sorgfaltspflicht der Geschäftsführung vor, reguliert das GmbH-Gesetz die Schadensersatzpflicht bei Sorgfaltspflichtverletzungen (§ 43 GmbHG), verpflichten Bürgerliches Gesetzbuch (BGB) und Ordnungswidrigkeitengesetz (OWiG) die Unternehmen zu Schutzmaßnahmen (§ 618 BGB) und nehmen die Verantwortlichen bei der Verletzung von Überwachungspflichten (§ 130 OWiG) in persönliche Haftung.

> Ohne ein Security Management-System kann das Thema Unternehmenssicherheit schnell **vom Kerngeschäft ablenken**.

Größeres Sicherheitsbedürfnis der Stakeholder

Mit einem stabilen Risikomanagement und einer verlässlichen Kontrollstruktur können diese Reputationsrisiken sowie gesellschaftliche und persönliche Haftungsrisiken reduziert, zum Teil sogar unterbunden werden. Auch die zusätzlichen Anforderungen an Dokumentations- und Nachweispflichten im Rahmen des Security Management-Systems können dadurch erfüllt werden. Hier geht es um Transparenz und Nachvollziehbarkeit sowie Integrität und Authentizität – kurz: um das gestiegene Sicherheitsbedürfnis der Stakeholder (Investoren, Banken, Kunden und Lieferanten). Die Quintessenz ist eindeutig: ein Wettbewerbsvorteil durch eine Best Practice-Stellung.

Mit einem zuverlässigen Risikomanagement können sich Unternehmen eine Best Practice-Stellung und damit **einen Wettbewerbsvorteil verschaffen**.

Unternehmensziele als Basis für ein prüffähiges Security Management-System

Orientierung bei der Entwicklung eines wirksamen Security Managements bieten die Grundsätze einer ordnungsgemäßen Prüfung von Compliance Management-Systemen (PS 980). Eine Prüfung des Security Managements analog PS 980 stellt eine standardisierte Prüfung aller ineinandergreifenden Elemente entsprechend des Compliance Lifecycle sicher – ein wesentlicher Beitrag, um die Anforderungen an ein funktionierendes Security Management-System zu erfüllen. Hierbei spielen insbesondere das Security-Risikomanagement, die Security-Programmentwicklung und daran anschließend die kontinuierliche Überwachung und Verbesserung der Wirksamkeit des Security Management-Systems eine elementare Rolle.

Zur Festlegung von Sicherheitszielen in den ausgewählten Teilbereichen bieten sich zunächst die allgemeinen Unternehmensziele als Grundlage an. In diesem Zusammenhang werden neben der strategischen Ausrichtung des Managementsystems nach Themenbereichen und Regionen/Ländern die Sicherheitsrisikobereiche sowie weitere allgemeine Anforderungen an ein Security Management-System festgelegt. Diese Festlegungen müssen abschließend dokumentiert werden.

Nach Identifikation der wesentlichen Anforderungen werden Sicherheitsrisikoanalysen durchgeführt. Sie dienen zur Ermittlung relevanter Gefährdungspotenziale für Mitarbeiter, Liegenschaften, vertrauliche Daten und Informationen, Produktionsstätten, Energieversorgung, IT-Infrastruktur und die jeweiligen Produkte. Ausschlaggebende Faktoren für die Bewertung sind die Eintrittswahrscheinlichkeit und das Schadensmaß. Soweit sie als relevant gelten, werden entsprechend präventive und detektivische Maßnahmen abgeleitet.

Orientierung bei der Entwicklung eines Security Managements bieten zum einen die Unternehmensziele und zum anderen die Grundsätze einer ordnungsgemäßen Prüfung von Compliance Management-Systemen (PS 980).

Sarah Laur
Governance & Assurance Services, KPMG
Julia Schröder
Governance & Assurance Services, KPMG

Advanced Cyber Defense

Bedrohung durch Cyberangriffe **minimieren**.

ängst vorbei sind die Zeiten, in denen Unternehmen mit Tinte und Papier geführt wurden und die Bücher abends in einem Tresor eingeschlossen wurden. Die Unternehmen arbeiten digital – und das ist völlig selbstverständlich. Allerdings sollten die damit verbundenen Risiken vorab bedacht und entsprechend minimiert werden.

Digitale Daten können kaum verlegt, dafür aber schnell weitergegeben werden. Sie lassen sich einfach in Beziehung zueinander setzen, aber ungeschützt auch unbemerkt mitnehmen. Die Digitalisierung bietet Risiken und Chancen – von Effizienzgewinnen über neue Märkte bis zu stärkerer Vernetzung mit Partnern, Zulieferern und Kunden. Unternehmen, die diesen Weg nicht gehen, sehen sich mit enormen Wettbewerbsnachteilen konfrontiert. Allerdings muss die Digitalisierung gut vorbereitet werden. So werden in der Regel aufwendige Integrations- und Transformationsprozesse in der gesamten IT-Landschaft erforderlich, wie zum Beispiel Anpassungen an betriebliche Prozesse oder komplexe technische Umstellungen auf neue Technologien und Software.

Vorbereitung erfordert auch der richtige Umgang mit den Risiken der Digitalisierung – Stichwort Cyberkriminalität. Tag für Tag werden neue Sicherheitslücken, Angriffe und Zwischenfälle aufgedeckt. Ein Bericht des renommierten Thinktanks „The Center for Strategic and International Studies" bezifferte die dadurch entstehenden jährlichen Verluste kürzlich auf 375 bis 575 Milliarden US-Dollar. Schätzungsweise bis zu 20 Prozent der weltweiten Wertschöpfung über das Internet gehen demnach durch Cyberkriminalität wie Betrug und Spionage verloren.

#01

Bis zu 20 Prozent der weltweiten Wertschöpfung über das Internet gehen **durch Cyberkriminalität verloren**.

#02

Die klassische Abschirmung nach außen **birgt ein hohes Risiko**: Sicherheitsvorfälle werden oft erst erkannt, wenn bereits schwerer Schaden entstanden ist.

Auslaufmodell Ritterburg

Um sich gegen solche Risiken zu schützen, haben viele Unternehmen Maßnahmen ergriffen – gerne nach dem Modell „Ritterburg": Wie im Mittelalter hohe Mauern Angreifer davon abhalten sollten, eine Burg zu plündern, sollen in diesem Fall Firewalls, VPNs und ein Berechtigungsmanagement das Unternehmensnetz vor Zugriffen von außen, beispielsweise aus dem Internet, schützen. Das Stichwort hierzu lautet „Perimetersicherheit".

Allerdings birgt dieser Ansatz auch Probleme. Zum einen hat sich gezeigt, dass es Angreifern immer wieder gelingt, „über die Mauern" zu kommen, zum anderen erfolgen viele Angriffe auch durch Insider innerhalb der schützenden Mauern. So oder so sind viele Unternehmen noch relativ schlecht darauf vorbereitet, Angriffe zu erkennen und die Angreifer aufzuspüren. Das führt dazu, dass sie Sicherheitsvorfälle oft erst erkennen, wenn bereits schwerer Schaden entstanden ist. Dabei lassen sich Angreifer ausbremsen und ihre Handlungen frühzeitig erkennen. Ein anpassungsfähiger Ansatz kann durchaus verhindern, dass es zu Ausfallzeiten kommt, teure Notfallmaßnahmen erforderlich werden oder der Geschäftsbetrieb unterbrochen wird.

Cyberrisiken versus Cyberchancen

Unternehmen können die Chancen der Digitalisierung nutzen, ohne sich ihren Risiken voll auszuliefern – vor allem, wenn sie die Digitalisierung als Lernprozess verstehen (siehe Textbox auf dieser Seite).

Lernen aus Vorfällen

Die Analyse von Vorfällen hilft, sich auf zukünftige Angriffe vorzubereiten. Je mehr Informationen herangezogen werden – aus der eigenen Organisation, aber auch darüber hinaus – desto umfangreicher kann die präventive Vorbereitung ausfallen.

Bessere Einschätzung von Schäden

Durch ein effizientes Security Monitoring werden Angreifer nicht nur früh entdeckt, sondern auch ihre Einfallstore offengelegt. Das erlaubt es Unternehmen, das Ausmaß eines Cyberangriffs besser bewerten zu können.

Minimierung der Auswirkungen von Cyberangriffen

Je nach Art des Angriffs kann ein Unternehmen entweder die Folgen im Vorfeld minimieren (zum Beispiel durch Aufsetzen eines Business Continuity Management-Systems gegen Ausfälle der IT) oder durch eine schnelle Reaktion den Schaden im Nachgang begrenzen (zum Beispiel durch Einbindung eines geschulten Forensikteams bei der Ermittlung des Angreifers und der Spurensicherung).

Ganzheitlicher Ansatz gefragt
Sich erfolgreich gegen die Cyberbedrohungen behaupten kann nur, wer Cyber Security ganzheitlich angeht. Die Vorteile der verschiedenen eingesetzten Lösungen – und damit sind nicht nur die zur Abwehr von Cyberangriffen gemeint – müssen kombiniert und alle gesammelten Daten genutzt werden, indem sie konsolidiert und nach intelligenten, maßgeschneiderten Regeln ausgewertet werden. So kann ein sogenanntes Security Information and Event Management (SIEM)-System einem Unternehmen zwar helfen, bekannte Angriffsmuster frühzeitig zu erkennen, aber es kann nicht erkennen, wenn ein (legitimer, aber gehackter) Administrator-Account regelmäßig auf vertrauliche Unternehmensdaten zugreift. Diesen Angriff kann man aber erkennen, wenn zum Beispiel die Zugriffsprotokollierung mit der Human Resource-Datenbank abgeglichen und festgestellt wird, dass der genutzte Account auch aktiv war, während der eigentliche Nutzer im Urlaub war.

Beispiele wie diese gibt es viele. Die Lösungen führen immer wieder zur gleichen Erkenntnis: Mit handelsüblichen Standardlösungen kommt man nicht weit. Der „Advanced Cyber Defense"-Ansatz muss für jedes Unternehmen individuell angepasst werden, bietet dafür aber auch einen Lösungsansatz zur Cyberabwehr, der bisher nicht umsetzbar war.

#03

Digitalisierung als Lernprozess: immer frühere Erkennung von Angriffen, immer bessere Einschätzung von Schäden sowie Minimierung der Auswirkungen von Cyberangriffen.

Cyber Security – ein Wettbewerbsvorteil
Der professionelle Umgang mit Cyberrisiken macht ein Unternehmen attraktiver für Kunden und Partner. Mit einem professionellen Information Security Management-System, das anerkannte Standards wie ISO 27001 erfüllt und entsprechend zertifiziert ist, zeigt das Unternehmen Kompetenz in Sachen IT-Sicherheit und schafft damit zusätzliches Vertrauen.

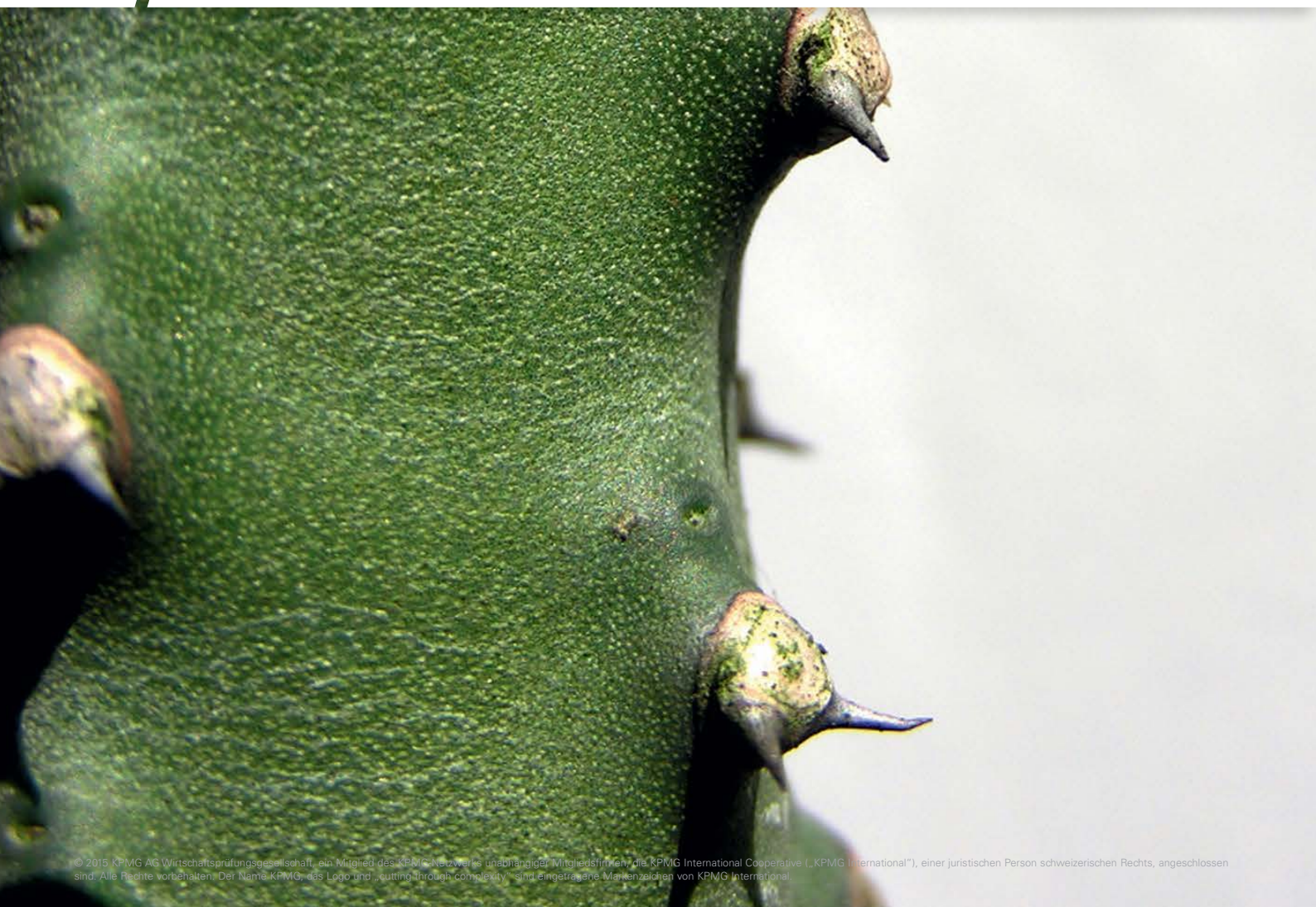
Kurz: Wir glauben, dass die Unternehmen gut für die Zukunft gerüstet sind, die Cyberangriffe als Teil der Wirtschaft akzeptieren und proaktiv individuelle Sicherheitsmechanismen und Abwehrmaßnahmen in ihr Geschäft einbauen. Die Sicherheit sollte dabei von Anfang an Bestandteil des Entwicklungs- und Lebenszyklus sein, damit Investitionen maximal wirksam und Ressourcen optimal genutzt werden.

#04

Mit einem **zertifizierten Information Security Management-System** zeigt ein Unternehmen Kompetenz in Sachen IT-Sicherheit und schafft damit zusätzliches Vertrauen bei seinen Kunden.

Uwe Bernd-Striebeck
Partner, Security Consulting, KPMG
Florian Kohlar
Security Consulting, KPMG

Immer mehr Informationen liegen digital vor, die Geschwindigkeit des Informationsaustauschs nimmt zu, die Zahl der Kommunikationskanäle wächst. Vor diesem Hintergrund müssen sensible Daten nicht nur immer besser geschützt werden. Es gilt auch, Cyberattacken als reales Risiko zu begreifen und sich bestmöglich gegen Datendiebstahl und -missbrauch zu wappnen.



Cyber Incident **Response**
Im Ernstfall **gut vorbereitet** zur richtigen Entscheidung.

Die Gefahr von Cyberangriffen wie Diebstahl oder Missbrauch wertvoller Daten und Informationen hat mittlerweile einen festen Platz in den Risikobetrachtungen von Konzernen und mittelständischen Unternehmen. Entsprechend haben viele Unternehmen Cyber Security-Strategien entwickelt, investieren in Security Operation Center und kooperieren mit anderen Playern am Markt. Während die Unternehmen ihre Sicherheit ausbauen, wollen Geheimdienste technologische Schwachstellen aufdecken und Verschlüsselungstechnologien knacken. So will der Bundesnachrichtendienst (BND) bis 2020 circa 4,5 Millionen Euro unter anderem in die Dekodierung der SSL-Verschlüsselung investieren. Dass hierfür auch vermeintlich böswillig agierende Akteure im Cyberumfeld rekrutiert werden, ist für Eingeweihte in der Branche keine erschütternde Nachricht. Einmal mehr rütteln die Neuigkeiten der letzten Wochen jedoch bei vielen Entscheidern an der Orientierung im Cyberumfeld: Müssen die eigenen Reaktionsstrategien geändert werden?

So viel Zeit muss sein

Gerade in schnellen Zeiten sollte man einen unaufgeregten Blick auf die eigenen Fertigkeiten im Ernstfall richten: Können wir/kann ich in einer komplexen Gefahrensituation angemessen entscheiden und belastbare Ergebnisse erzielen?

Umfragen und Erfahrungen aus Incident Response-Projekten zeigen, dass die Verantwortlichkeiten für die Reaktion auf einen Cybervorfall in den meisten großen und mittelgroßen Unternehmen mittlerweile klar definiert sind – mit einer entscheidenden Ausnahme: Bei internen Bedrohungen sind die Zuständigkeiten nicht immer eindeutig. Wenn beispielsweise ein Vertriebsleiter samt Kernteam, der befreundete IT-Administrator sowie der Business Development Manager die Bindung zum eigenen Unternehmen verloren haben, sind illegale Datenweitergaben keine Seltenheit.

> Die Verantwortlichkeiten für Reaktionen auf Cybervorfälle sind in den meisten Unternehmen klar definiert – nur bei internen Bedrohungen sind **die Zuständigkeiten nicht immer eindeutig**.

Kombination von Auffälligkeiten entscheidet

Mithilfe von Monitoring-Systemen können auffällige Datenbewegungen identifiziert werden. Für eine fundierte Risikobeurteilung müssen allerdings mehrere Auffälligkeiten zusammen betrachtet werden. Ein plötzlicher und massiver Download von Vertriebsdaten über eine IP-Adresse und ein Endgerät, die beide einem Mitarbeiter des oben genannten Vertriebsteams zugeordnet sind, kann bereits ein Alarmsignal sein.

Bei einschneidenden Veränderungen wie Insolvenzen oder Umstrukturierungen kann ein **Sicherheitsvorfall verbunden mit weiteren Systemauffälligkeiten** zu einer ernsten Bedrohung führen.

Neben dieser speziellen Auffälligkeit sind Unternehmen aber auch einer Reihe von täglichen Angriffsversuchen über extern zuzuordnende IP-Adressen ausgesetzt. Wenn wachsame IT-Administratoren darüber hinaus entschlüsselte Authentifizierungsdaten (SSH-Keys) für kritische Systeme festgestellt haben, zeigt sich die eigentlich gefährliche Gesamtsituation: Bei strukturell einschneidenden Veränderungen, wie beispielsweise Insolvenzen oder Umstrukturierungen, kann ein Sicherheitsvorfall verbunden mit weiteren Systemauffälligkeiten eine ernste Bedrohungslage darstellen.

Vertrauensbildung nach Vertrauensbruch

Ein Sicherheitsvorfall bedingt schnelles Handeln, doch der Standardprozess – sofern definiert – greift in diesem Fall nicht mehr, da das Vertrauen in einen Teil der Geschäftsführung, in den vom Datentransfer betroffenen Unternehmensbereich, in die IT und damit möglicherweise auch in externe IT- und Sicherheitsdienstleister, die durch die IT beauftragt wurden, gestört ist.

Richtig auf einen Cybervorfall zu reagieren, bedeutet also eine größere Zahl an handelnden Akteuren und damit einen höheren Abstimmungs- und Steuerungsaufwand, einen wachsenden Bedarf an gegenseitiger Kontrolle und nicht zuletzt die Bildung eines vertrauensvollen Response-Teams. Denn nur so sind schnelles Handeln und verlässliche Ergebnisse möglich.

Um richtig, schnell und effektiv auf einen **Cybervorfall mit internen Tätern** zu reagieren, bedarf es schnellen Umdenkens und gegenseitiger Kontrolle.

Nur die Vorbereitung auf relevante Vorfallsszenarien durch **Krisenreaktionspläne** und **unabhängige Cyber Investigation-Teams** ermöglicht eine angemessene und zeitnahe Reaktion.

Entscheidungsfähigkeit durch Notfallplan sicherstellen

Die Umsetzung von erforderlichen Maßnahmen ist allerdings insbesondere für Unternehmen, die noch nicht wissentlich Opfer komplexer Sicherheitsvorfälle waren, nicht immer einfach. Gerade die kurzfristige Bildung eines Response Teams aus mehreren Vertretern der Geschäftsführung, die Auswahl und Beauftragung eines IT-Forensik-Dienstleisters, aber auch die Vereinbarungen zur Verschwiegenheit von IT-Mitarbeitern und externen IT-Dienstleistern und ihre Begleitung durch einen Forensik-Dienstleister können viel Zeit erfordern. Um den Prozess zu vereinfachen und zu beschleunigen, sollten Sie prophylaktisch **...**

- **...** alternative Verantwortlichkeiten für integritätskritische Cyberszenarien definieren,
- **...** einen Pool externer Forensik-Dienstleister zusammenstellen und die Konditionen und Parameter im Falle einer Beauftragung abstimmen,
- **...** mit Ihren IT-Dienstleistern Vertragsklauseln festlegen, die Ihnen im Ernstfall einen Zugriff auf Ihre extern gehosteten Daten ermöglichen,
- **...** mit Ihrem internen und externen IT-Personal integritätskritische Szenarien einüben und diese Szenarien in Ihr klassisches Krisenmanagement integrieren; die Einbindung weiterer Unternehmensbereiche, wie Informationssicherheit, Konzernsicherheit, Recht und Human Resources, ist vorteilhaft,
- **...** Ihre interne Expertise zur systemübergreifenden Korrelation und Bewertung von Auffälligkeiten und Sicherheitsvorfällen pflegen.

Kurzfristige Entscheidungsfähigkeit wird insbesondere bei integritätskritischen Cybersicherheitsvorfällen weniger durch technische Fragestellungen als vielmehr durch konkrete kaufmännische, organisatorische und rechtliche Fragestellungen der Beauftragung und Kontrolle bestimmt. Nach wie vor gilt: Nur die Vorbereitung auf relevante Vorfallsszenarien durch Krisenreaktionspläne und unabhängige Cyber Investigation-Teams ermöglicht eine angemessene und zeitnahe Reaktion.

Empfehlungen aus der Praxis

In der Praxis hat sich folgendes Vorgehen bewährt:

- **Verantwortung für die Vorfallsreaktion und -aufklärung auf mehrere Vertreter der Geschäftsführung verteilen**

  Endgültige Entscheidungen können bei einem Vertreter der Geschäftsführung liegen, aber die Vorbereitung braucht die gegenseitige Kontrolle im Hinblick auf gleichberechtigten Informationsaustausch und transparente Dokumentation von Entscheidungen inklusive etwaiger Vorbehalte.

- **Unabhängige externe Forensik-Dienstleister (Cyber Investigation-Team) einbinden, um angemessene Maßnahmen und belastbare Ergebnisse zu erreichen**

  Qualifizierte Forensik-Dienstleister bieten schnelle Reaktion durch die Ortsnähe ihrer globalen Teams, technologische und analytische Fertigkeiten für die Erstreaktion, ökonomische und (datenschutz-) rechtliche Risikobetrachtung, Beweissicherung und Aufklärung. Sie verfügen zudem über Expertise in der Steuerung großer Projektteams aus unterschiedlichen Parteien. Handelt es sich bei einem Forensik-Dienstleister um eine Wirtschaftsprüfungsgesellschaft, gilt die berufsständische Verschwiegenheitspflicht.

- **IT-Administratoren und gegebenenfalls externe IT-Dienstleister weiterhin einbinden**

  Auch wenn das Vertrauen in die IT erschüttert ist, sprechen gute Gründe für ihre weitere Einbindung. Zum einen ist es mit einem enormen technischen, zeitlichen und somit finanziellen Aufwand verbunden, nicht belastete Externe in die Lage zu versetzen, so auf die IT-Systeme und Daten zuzugreifen, dass sie effizient arbeiten können – selbst wenn eine mustergültig gepflegte IT-System-Dokumentation vorliegt. Zum anderen werden damit haftungsrechtliche Fragen aufgeworfen (zum Beispiel Beeinträchtigung der Kerngeschäftsprozesse durch Zugriff auf laufende IT-Systeme). Allerdings sollten keine Personen eingesetzt werden, bei denen ein konkretes Risiko besteht, dass sie vertrauliche Informationen über die Vorfallsreaktion und -aufklärung an Verdächtige weitergeben. Zudem sollte das eingesetzte IT-Personal eine anlassbezogene Vertraulichkeitsbelehrung erhalten und eine Vertraulichkeitsvereinbarung unterzeichnen.

- **Tätigkeiten der IT-Administratoren und der externen IT-Dienstleister von einem neutralen Forensik-Dienstleister begleiten lassen**

  Je kritischer der Sicherheitsvorfall, umso frühzeitiger sollten alle arbeitsbezogenen Tätigkeiten der IT-Administratoren und externen IT-Dienstleister begleitet werden. Darunter fallen etwa die Herausgabe von Informationen über die IT-System- und Datenlandschaft, die Sicherung untersuchungsrelevanter Daten und Endgeräte von E-Mail-Accounts bis zum Smartphone, die Überwachung von Systemaktivitäten, aber auch die Deaktivierung oder Neuanlage von Systemberechtigungen. Die Überwachung reduziert das Risiko der Datenmanipulation oder -löschung. Sie kann zudem eine möglicherweise leichtfertige Weitergabe von vertraulichen Informationen korrigieren. Letztendlich entscheiden diese Aktivitäten im Nachgang darüber, ob beziehungsweise bis zu welchem Grad die Aussagen des externen Forensik-Dienstleisters belastbar und juristisch verwertbar sind.

- **Wegen des Integritätsrisikos einen höheren Abstimmungsaufwand als bei Sicherheitsvorfällen üblich einkalkulieren**

  Die Verantwortlichen der Geschäftsführung und der unabhängige Forensik-Dienstleister sollten sich engmaschig abstimmen, damit alle Beteiligten zeitnah den vollständigen Wissenstand über den Sicherheitsvorfall erlangen. Das sichert nicht nur frühzeitige Entscheidungsoptionen, sondern auch die Transparenz über die laufenden Kosten einer Untersuchung. Natürlich sollte diese Kommunikation nicht über Kanäle geführt werden, die ein Mithören wahrscheinlich werden lassen – beispielsweise Räume mit dünnen Wänden, bekannte Einwahldaten, E-Mail-Adressen und Endgeräte oder unverschlüsselte E-Mails über möglicherweise kompromittierte Netzwerke.

Alexander Geschonneck
Partner, Forensic, KPMG
Thomas Fritzsche
Senior Manager, Forensic, KPMG

Krisen in Krankenhäusern, ganz gleich, ob es um die unerlaubte Weitergabe vertraulicher Daten geht oder um einen Ärztefehler mit Todesfolge, können das Vertrauen in ein Haus zerstören. Und Medizin hat viel mit Vertrauen zu tun. Umso wichtiger ist es, Krisen zu verhindern und sie gegebenenfalls professionell zu bewältigen.

Alarm!?
Effektives **Krisenmanagement** im Krankenhaus.

Die Medizin versteht unter einer Krise ein zeitlich begrenztes Ereignis, das durch belastende äußere oder innere Faktoren hervorgerufen wird und eine akute Überforderung des gewohnten Zustands bedeutet. Die Überforderung kann Ursache einer kurzfristigen starken Belastung oder aber das Resultat eines länger andauernden Belastungszustands sein.[1]

Wie sieht eine Krise in einem Krankenhausunternehmen aus? Eine Krise stellt hier eine Situation dar, die weder geplant noch gewollt ist. Sie betrifft typischerweise die gesamte Organisation und kann die Überlebensfähigkeit eines Unternehmens oder einer Unternehmenseinheit bedrohen – im schlimmsten Fall sogar Leben fordern: Laut AOK-Krankenhausreport 2014 sterben jährlich mehr als 19.000 Klinikpatienten durch vermeidbare Behandlungsfehler. Doch es muss gar nicht zum Tod eines Patienten kommen, damit eine Krise zu empfindlichen finanziellen Einbußen für das Krankenhaus führt.

Der Ausgang einer Krise lässt sich **nur in den wenigsten Fällen** im Vorhinein abschätzen.

Schwer absehbare Folgewirkungen

Wesentliches Merkmal einer Krise im Krankenhaus ist die extreme Ambivalenz der Folgewirkungen. Ein kleiner Hygienevorfall im Krankenhaus kann schnell wieder vergessen sein. Unter Umständen kann er aber auch zu einer ernsten Bedrohung für die Bettenauslastung und damit für die wirtschaftliche Lage werden. Und eine Krise hat ein weiteres Merkmal: Der Ausgang lässt sich nur in den wenigsten Fällen im Vorhinein abschätzen. Umso wichtiger ist es für ein Krankenhausunternehmen, die Ursachen für die Entstehung einer Krise zu verstehen, um sie in einem möglichst frühen Stadium zu überwinden oder gar nicht erst zuzulassen.

Krankenhäuser sind mit medizinischen Krisen konfrontiert – ausgelöst etwa durch ärztliche Kunstfehler, nachlässigen Umgang mit Vorschriften und Standards (Non-Compliance) oder prekäre Hygienesituationen. Doch Krankenhäuser sind auch außerhalb des medizinischen Bereichs krisenanfällig: Liquiditätskrisen entstehen zum Beispiel, wenn Kliniken aufgrund einer angespannten finanziellen Situation Löhne und Gehälter nicht mehr auszahlen können. Auch Abrechnungsbetrug, sogar wenn er nicht vorsätzlich war, oder die Bestechung von Zuweisern können weitreichende Folgen für ein Haus haben. Schließlich können auch technische, infrastrukturell bedingte Ereignisse den Arbeitsablauf stören und zu operativen Beeinträchtigungen führen.

Eine Krise **betrifft die gesamte Organisation** und kann die Überlebensfähigkeit eines Unternehmens oder einer Unternehmenseinheit bedrohen.

1 Simmich, Thomas, et al.: Empfehlungen zur Behandlungspraxis bei psychotherapeutischen Kriseninterventionen. In: Psychotherapeut, 44 (6) 1999, S. 394–398

Auch **unverschuldete Krisen**, etwa als Folge von Unwettern oder politischen Umwälzungen, müssen vom Krankenhaus bewältigt werden.

Manche Krisen sind vom Krankenhaus nicht zu beeinflussen – wenn etwa externe Auslöser wie Unwetter, Stromausfälle oder Epidemien, politische oder gesellschaftliche Umwälzungen zur Krise führen. Bewältigt werden müssen sie dennoch. Oftmals sind Krisen im Krankenhaus jedoch selbstverschuldet und auf (häufig unentdeckte) Fehler in den operativen und technischen Abläufen eines Krankenhausunternehmens zurückzuführen.

Von der potenziellen zur unbeherrschbaren Krise

Die Textbox zeigt die Entwicklung einer Krise über vier Phasen.[2]

Kritischer Punkt im Vier-Phasen-Modell ist der Übergang von einer latenten Unternehmungskrise zu einer akuten Krise. Im Stadium der latenten Krise werden die Auslöser sichtbar und können noch unterbunden bzw. kontrolliert werden, um das Eintreten einer akuten Krise zu vermeiden.

„Normalisierung von Abweichungen" als Krisenursache

Krisen werden in der Regel nicht durch einen Einzelnen verursacht, sondern durch mehrere Menschen, die mehrere, teilweise unbewusste Fehler begehen. Fehler meinen dabei Abweichungen von den Standards und Vor-

1 Potenzielle Krise

Das Unternehmen befindet sich noch in seinem Normalzustand. Dann kommt es zu einem Ereignis, nach dem sich eine baldige Krise abzeichnet. Dieses Ereignis kann zum Beispiel eine strategische Fehlentscheidung sein, die zu einer Verschlechterung der finanziellen Situation des Unternehmens führt; es können ausgebliebene interne Kontrollen sein, die sonst Fehlverhalten seitens der Mitarbeiter aufgedeckt hätten; es kann aber auch mangelhafte Kommunikation oder erhöhter Produktivitätsdruck sein, der Nachlässigkeit in den operativen Abläufen bewirkt. Hier sind die Früherkennungsanforderungen an eine Krise sehr hoch, denn noch ist die destruktive Wirkung der Krise nur potenziell vorhanden und nicht direkt sichtbar.

2 Latente Krise

Das Unternehmen befindet sich schon nicht mehr im Normalzustand. Die Krise ist bereits verdeckt vorhanden und wird bei ausbleibenden Krisenvermeidungsanstrengungen mit hoher Wahrscheinlichkeit bald eintreten. Handlungsmöglichkeiten sind trotz erster destruktiver Auswirkungen noch vorhanden, wenn die Früherkennung funktioniert. Eine latente Unternehmungskrise liegt zum Beispiel vor im Falle eines Erlösrückgangs infolge einer strategischen Fehlentscheidung, bei Aufdeckung fehlerhafter Abrechnungen im Zuge nicht regelkonformen Verhaltens der Mitarbeiter oder bei Auftreten erster Keime, die auf Schwachstellen in der Hygienesituation eines Krankenhauses hinweisen. Werden diese Warnhinweise nicht beachtet und keine Gegenmaßnahmen eingeleitet, wird die Krise akut.

3 Akute, beherrschbare Krise

Wenn Frühwarnsysteme und Gegenmaßnahmen nicht funktioniert haben, wird die Krise akut. In dieser Phase ist die Krise zwar eingetreten, befindet sich allerdings in einem frühen Stadium und ist damit noch beherrschbar. Die destruktive Wirkung ist spürbar vorhanden, die Krisenbewältigungsanforderungen steigen. Beispiele für diese Phase sind akute Liquiditätsengpässe, öffentlich gewordener Abrechnungsbetrug oder Krankenhauskeime, die bereits übertragen wurden.

4 Akute, nicht beherrschbare Krise

Dieses Stadium tritt ein, wenn die Krise nicht eingedämmt oder bewältigt werden konnte bzw. bisher keine Maßnahmen ergriffen wurden. Die Krise kann jetzt ihre ganze destruktive Wirkung entfalten. Die Überlebensfähigkeit des Unternehmens kann bedroht sein, in jedem Fall tritt ein Reputationsschaden ein – wahrscheinlich verbunden mit erheblichen finanziellen Auswirkungen für das Unternehmen. Sofern noch möglich, muss versucht werden, die Krise zu bewältigen oder zu verarbeiten. Beispiele für nicht mehr beherrschbare Krisen im Krankenhaus sind Zahlungsunfähigkeit, Todesfälle durch mangelnde Hygiene, Aufdeckung eines Abrechnungsbetrugs in großem Stil oder ärztliches Fehlverhalten mit tödlichen Folgen.

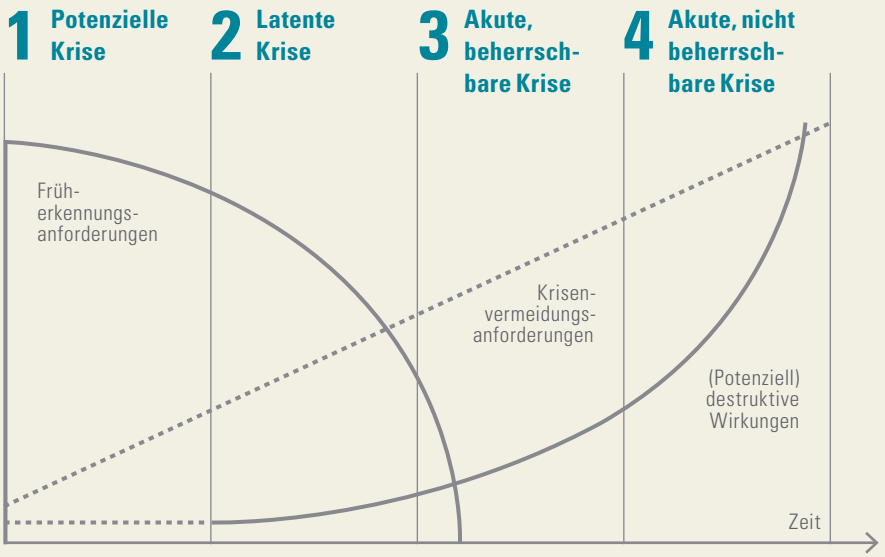
2 In Anlehnung an Krystek, Ulrich: Unternehmungskrisen, Wiesbaden 1987

schriften einer Organisation. Was als Abweichung von einem vorgeschriebenen Standard beginnt, kann durch regelmäßige Wiederholung zu einem scheinbar neuen „Normalzustand“ werden.[3] Die Abweichung vom Standard oder von der Regel ist dann nicht mehr bewusst und bleibt folglich unbemerkt. Bestehende Warnhinweise auf eine Krisensituation werden dadurch nicht mehr als solche wahrgenommen. Beispiele für diese unterschätzten Abweichungen von Standards in Krankenhäusern sind nicht ausreichendes Händewaschen, nicht konforme sterile Kleidung, ungenügende Sicherheitschecks vor Operationen oder auch die Nichteinhaltung von Abrechnungsvorschriften. Abweichungen resultieren dabei selten aus bösem oder kriminellem Willen, sondern unbewusst, aus Nachlässigkeit oder aufgrund scheinbarer Notwendigkeit, das heißt:

- Abweichungen von Vorschriften und Regeln werden zum Teil als notwendig dargestellt, oft sind Produktivitätsdruck und Stress ein Faktor: Perfekte Compliance mit allen Vorschriften und Regeln steht für viele Mitarbeiter im Widerspruch zu Produktivitätszielen, sodass häufig an den falschen Stellen im operativen Prozess Zeit eingespart wird.
- Regeln sind teilweise nicht bewusst oder werden nicht ausreichend verstanden: Unzureichende Kommunikation oder fehlende Kontrollen führen dazu, dass die Notwendigkeit zur Einhaltung bestimmter Vorschriften unter den Mitarbeitern nicht erkannt wird. Nachlässigkeit ist dann die Folge.

Vier-Phasen-Modell einer Krise

Quelle: 4-Phasen-Modell (eigene Darstellung, in Anlehnung an Krystek 1987)



Krisenmanagement braucht Vorsorge und Bewältigung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe definiert den Begriff in seinem Leitfaden „Schutz kritischer Infrastruktur – Risikomanagement im Krankenhaus, Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in kritischen Infrastrukturen des Gesundheitswesens“ als die „Schaffung von konzeptionellen, organisatorischen, verfahrensmäßigen und physischen Voraussetzungen, die eine bestmögliche Bewältigung einer Krise im Hinblick auf die zur Verfügung stehenden Ressourcen und Informationen ermöglichen und eine schnellstmögliche Zurückführung in den Normalzustand unterstützen.“ Andere Autoren fassen den Begriff noch weiter auf und beziehen auch Aspekte der Krisenvorsorge mit ein.[4]

> Was als **Abweichung** von der Vorschrift beginnt, kann **durch Wiederholung zum „Normalzustand“** werden.

3 In Anlehnung an Vaughan, Diane: The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA. Chicago/London 1996; Banja, John: The normalization of deviance in healthcare delivery. In: Business Horizons, 53 (2) 2010, S. 139–148

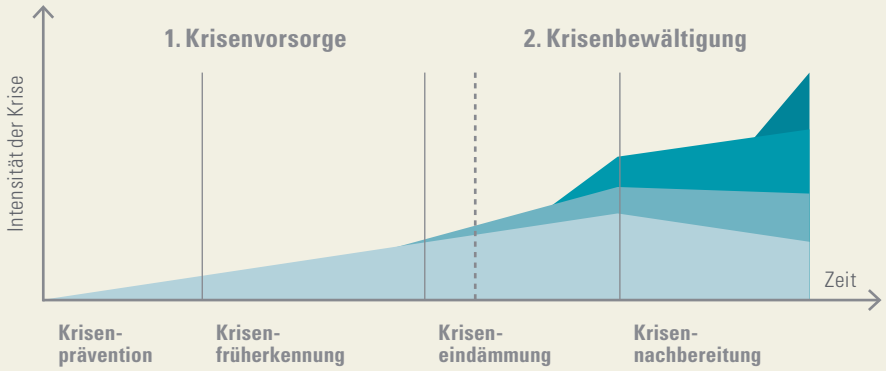
4 Eiff, Wilfried von (Hg.): Risikomanagement – Kosten-/Nutzenbasierte Entscheidungen im Krankenhaus, Schriftenreihe Gesundheitswirtschaft, Band 2, kma-Reader, Wegscheid 2007

Krisenmanagement reicht von der **Prävention** über die **Früherkennung** und **Eindämmung** bis zur **Nachbereitung**.

Das Krisenmanagement lässt sich nach der weiter gefassten Definition (siehe Abbildung) in die Phase der Krisenvorsorge und der Krisenbewältigung gliedern. Die einzelnen Schritte orientieren sich dabei an den Phasen des Krisenverlaufs. Das Krisenmanagement weist in seiner prozessualen Gestaltung starke Parallelen zum Risikomanagement auf und kann nicht losgelöst von den bestehenden Governance-Systemen in der jeweiligen Einrichtung gesehen werden.[5]

Phasen von **Krisenverlauf** und **Krisenmanagement**[6]

Quelle: Friedrich, S./Schneuwly, S.: Wie groß ist das Risiko, wenn kein Eisberg in Sicht ist? Wenn Krankenhäuser von Krise überrascht werden. In: KPMG Gesundheitsbarometer 2/2013, S. 4 ff.



Kontinuierliche Medienarbeit kann zu einem Vertrauensvorschuss oder Reputationsgewinn sowohl in der Öffentlichkeit als auch bei den Pressekontakten führen – **im Krisenfall ein wertvolles Asset**.

In die Krisenvorsorge fallen die Krisenprävention und die Krisenfrüherkennung. Im Rahmen der Krisenprävention erfolgt zunächst die Identifikation möglicher Krisen. Eine Analyse der potenziellen Krisenfelder sollte Aufschluss über generelle Eigenschaften der möglichen Gefahren, ihre Intensität, Zeitdauer und mögliche Wirkungen geben. Die Ergebnisse fließen dann in das Krisenfrüherkennungssystem ein – die Erarbeitung und kontinuierliche Aktualisierung eines Krisenplans. Regelmäßige Krisenübungen und Praxisschulungen sollten das vorgesehene Vorgehen im Sinne der Krisenprävention fest im Unternehmen verankern.

Vertrauen durch Kommunikation aufbauen

Ein weiterer Aspekt der Krisenvorsorge ist die Planung der Krisenkommunikation nach innen und nach außen. Ein stringenter, festgelegter interner Informationsfluss sowie die koordinierte Zusammenarbeit mit den Medien sind im Falle einer Krise von zentraler Bedeutung. Mithilfe kontinuierlicher Medienarbeit kann ein Vertrauensvorschuss bzw. Reputation sowohl in der Öffentlichkeit als auch bei den Pressekontakten aufgebaut werden. Im Falle einer Krise wird die rufschädigende Auswirkung durch diesen Vorschuss abgefedert.

5 Friedrich, Stefan/Schneuwly, Stefanie: Wie groß ist das Risiko, wenn kein Eisberg in Sicht ist? Wenn Krankenhäuser von Krisen überrascht werden. In: KPMG-Gesundheitsbarometer 2/2013, S. 4–7
6 Ebenda

Ziel des Risikomanagements ist es, mögliche Krisensituationen früher zu erkennen und aufwendiges Krisenmanagement zu vermeiden.

Krisenerfahrungen für Krisenfrüherkennung nutzen

Aussagekräftige Krisenindikatoren bzw. Toleranzgrenzen bilden die Basis für die Krisenfrüherkennung: Hier geht es darum, eine potenzielle Krise in einem frühen Stadium zu erkennen und zu überwachen, aber auch darum, neue Krisenfelder aufzudecken und neue Erkenntnisse kontinuierlich in ein Krisenfrüherkennungssystem sowie den Krisenplan einzubeziehen. Gerade hier sollten die Wechselwirkungen mit dem Risikomanagement Beachtung finden. So beeinflussen Art und Umfang der Restrisiken die Ausprägung der Krisenfrüherkennung.

Fehler als Chance sehen

Ein zusätzliches Element des modernen Krisenmanagements ist eine positive Fehler- und Beschwerdekultur. Fehler und Beschwerden werden bei dieser Herangehensweise als Chancen interpretiert, aus denen eine Organisation lernen und damit ihre operativen Tätigkeiten optimieren kann. Die Voraussetzung dafür schafft ein institutionalisiertes Berichts- bzw. Beschwerdesystem über kritische Zwischenfälle.[7]

Ein **institutionalisiertes Berichts- oder Beschwerdesystem** über kritische Zwischenfälle ist ein unverzichtbarer Teil modernen Krisenmanagements.

Zeit für den Krisenplan

Kommt es zur Krise, gilt es, sie bestmöglich zu bewältigen – und zwar im Sinne einer Kriseneindämmung und einer Krisennachsorge.[8] Wird eine Krise akut, sollte zur Kriseneindämmung der vorab erarbeitete Krisenplan zum Einsatz kommen. Oberstes Ziel ist die schnelle und nachhaltige Schadensbegrenzung. Aufgrund der oben beschriebenen extremen Ambivalenz der Entwicklungsmöglichkeiten einer Krise im Krankenhausumfeld braucht es allerdings unbedingt ein gewisses Maß an Flexibilität. Und neben den Bemühungen um die Krisenbewältigung darf die Fortführung des Regelbetriebs im Krankenhaus mitsamt der hierfür notwendigen Ressourcen nicht vernachlässigt werden. Die Öffentlichkeit sollte parallel transparent, offen, geordnet und zeitnah informiert werden. Entsprechend sollten sich auch kompetente Interviewpartner zur Verfügung stellen. Der Wille zur Aufklärung muss deutlich werden, Raum für Spekulationen darf es nicht geben.

Die Krisenbewältigung darf **nicht zu einer Vernachlässigung des Regelbetriebs** im Krankenhaus führen.

7 Gigerenzer, Gerd: Risikokompetenz im Krankenhaus – die Medizin steht sich selbst im Weg! In: KPMG-Gesundheitsbarometer 2/2013, S. 2–3; Gigerenzer, Gerd: Risiko. Wie man die richtigen Entscheidungen trifft, München 2013, S. 70 ff.

8 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus, Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens, Bonn 2008

Kommt es zur Krise, sollte sie als **Chance für Verbesserungen** genutzt werden.

Clara Kozak
Governance & Assurance Services, KPMG
Franziska Holler
Governance & Assurance Services, KPMG

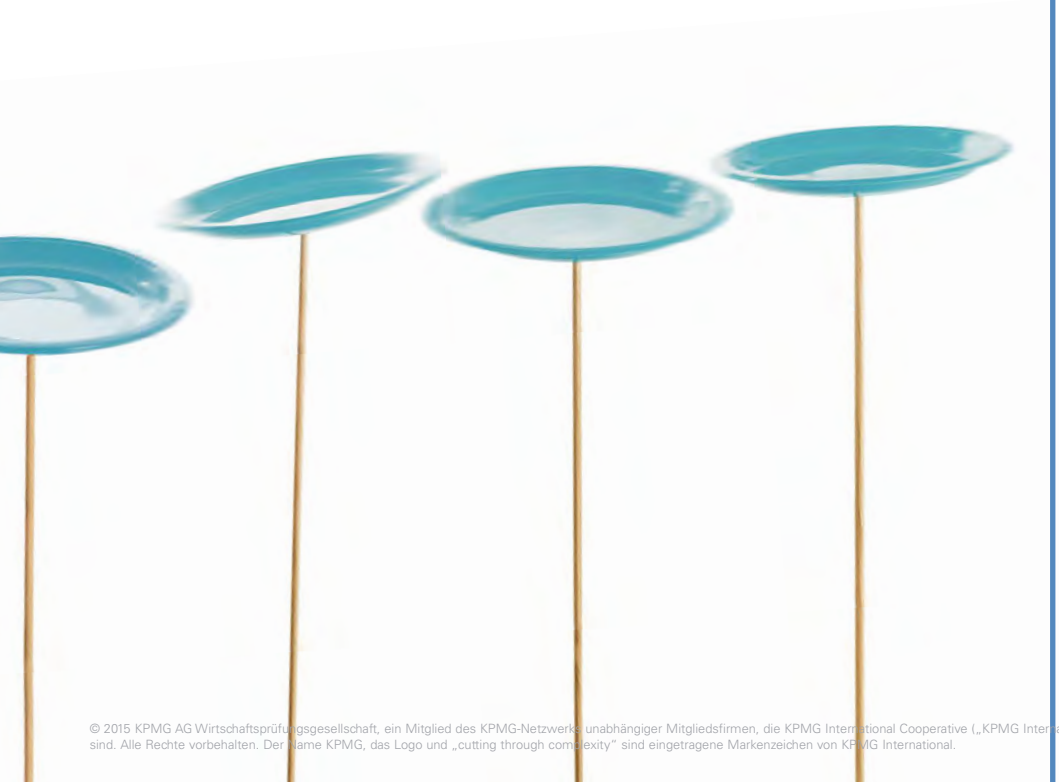
In der Krisennachbereitung muss das Krisenmanagement überprüft und bewertet werden: Wie ist die Effektivität einzuschätzen? Wo gibt es Defizite oder Verbesserungspotenzial? Im Sinne kontinuierlicher Verbesserung und der Vermeidung einer weiteren Rufschädigung sollte eine Krise transparent aufgearbeitet werden. Auch in diesem Prozessschritt ist die Kommunikation nach innen und außen von zentraler Bedeutung.

Kontinuierliche Verbesserung und Aktualisierung sicherstellen

Losgelöst vom konkreten Krisenfall sollte das Krisenmanagement regelmäßig evaluiert werden. Hierbei sind zum einen Änderungen in der Gefahrenlage – beispielsweise durch Umbauten in der Einrichtung – zu überwachen und zu berücksichtigen. Auch externe Faktoren verändern die Gefahrensituation. So zeichnet es sich ab, dass etwa Naturgefahren, kriminelle Handlungen oder auch terroristische Aktionen an Bedeutung gewinnen könnten.

Auch auf regelmäßige Aktualisierung des Krisenplans ist zu achten. So kann es bei einer Krise beispielsweise durch Fluktuation oder neue Telefonnummern zu einer Unterbrechung des Informationsflusses kommen. Der Wechsel von Ansprechpartnern und Verantwortlichen oder Änderungen im Bewältigungs- und Kommunikationsprozess müssen daher schnellstmöglich in den Krisenplan übertragen und kommuniziert werden. Ein geeignetes Instrument zur systematischen Überprüfung des Krisenmanagements sind Checklisten.[9]

Sinnvoll eingesetzt bildet das Krisenmanagement eine wichtige Ergänzung zu Risiko- und Compliance Management-Systemen, die in Anlehnung an den IDW PS 980 in ihrer Wirksamkeit geprüft und bescheinigt werden können.



Neue Ansprechpartner durch Fluktuation, geänderte Telefonnummern oder Überarbeitungen im Bewältigungs- und Kommunikationsprozess müssen **umgehend in den Krisenplan übertragen** werden.

9 Gigerenzer, Gerd: Risikokompetenz im Krankenhaus – die Medizin steht sich selbst im Weg! In: KPMG-Gesundheitsbarometer 2/2013, S. 2–3; Gigerenzer, Gerd: Risiko. Wie man die richtigen Entscheidungen trifft, München 2013, S. 70 ff.

Tax Compliance Management **Erfolgreich** gegen steuerliche Risiken vorgehen.

Interview mit Dr. Jan-Hendrik Gnändiger, Senior Manager im Geschäftsbereich Governance & Assurance Services von KPMG

Compliance Management-Systeme gelten als wirksames Mittel, um Compliance-Verstöße zu verhindern oder aufzudecken. Bislang standen dabei die Risiken und Verstöße hinsichtlich Korruption, Kartellrecht oder Datenschutz im Fokus. Nun wird die systematische Risikosteuerung auch für steuerliche Fragestellungen relevant. Dr. Jan-Hendrik Gnändiger erläutert die Chancen einer Steuerung von Tax Compliance-Risiken und stellt Möglichkeiten der Assurance durch Bescheinigungen vor.

Assurance Magazin: Wie unterscheidet sich der Begriff Tax Compliance vom gängigen Compliance-Begriff?

Dr. Jan-Hendrik Gnändiger Die Praxis hat sich lange mit dem Begriff Compliance schwergetan. Dabei ist er eigentlich nicht neu. Compliance steht für die Einhaltung von Gesetzen, unternehmensinternen Richtlinien und gegebenenfalls freiwilligen Selbstverpflichtungen. Damit werden in der öffentlichen Wahrnehmung derzeit noch primär Themen wie Korruption oder Kartellrechtsverstöße verbunden. Unter die Einhaltung von Gesetzen fällt aber natürlich auch und gerade das Steuerrecht. Tax Compliance ist in den Steuerabteilungen der Unternehmen ein gängiger Begriff und bedeutet nichts anderes als die Einhaltung der steuerrechtlichen Vorschriften. Das in einem Unternehmen oder Konzern effektiv zu organisieren, wird durch die zunehmende Komplexität der Vorschriften und Anforderungen schwieriger. Gleichwohl wird es notwendiger, da Tax Compliance-Verstöße zunehmend verfolgt werden.

Welche Pflichten haben die Organe eines Unternehmens in Bezug auf Tax Compliance?

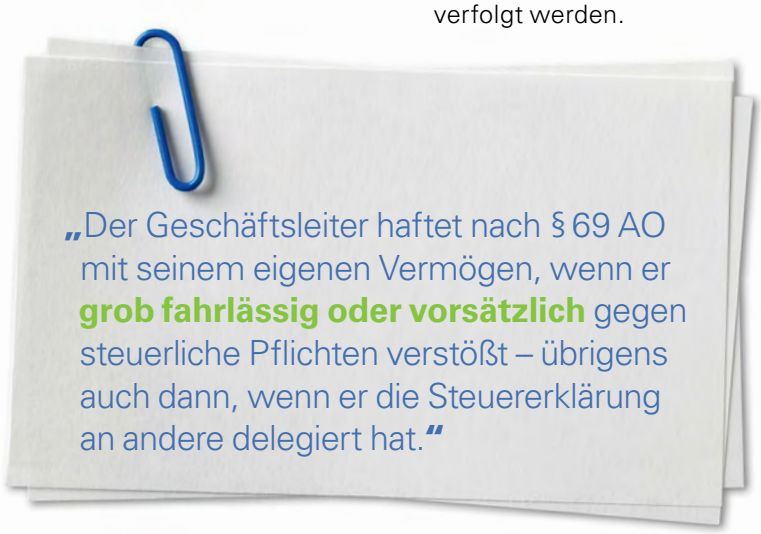
Dr. Jan-Hendrik Gnändiger Eine juristische Person kann nur durch die Organe handeln. Ihnen obliegt daher auch die ordnungsgemäße Erfüllung der steuerlichen Pflichten, insbesondere die Abgabe der Steuererklärungen und die Bezahlung der Steuern nach § 34 Abgabenordnung (AO). Der Geschäftsleiter haftet nach § 69 AO mit seinem eigenen Vermögen, wenn er grob fahrlässig oder vorsätzlich gegen steuerliche Pflichten verstößt und dadurch Steuern nicht rechtzeitig festgesetzt oder entrichtet werden können. Begeht der Geschäftsleiter

Dr. Jan-Hendrik Gnändiger
Senior Manager,
Governance & Assurance Services

Dr. Jan-Hendrik Gnändiger, Wirtschaftsprüfer und Steuerberater, begleitet Unternehmen in allen Fragen rund um das Thema Compliance. Neben Prüfungen nach IDW PS 980 erbringt er im Rahmen der zunehmend aufkommenden Fragestellungen zum Thema Tax Compliance Assurance Leistungen und stellt darüber Bescheinigungen auf der Basis von ISAE 3000 aus.

„Compliance bedeutet **Einhaltung von Gesetzen, unternehmensinternen Richtlinien** und **freiwilligen Selbstverpflichtungen**. Tax Compliance bezieht sich dabei auf die spezifischen Vorgaben im steuerlichen Bereich."

im Interesse der Gesellschaft Steuerhinterziehung oder wirkt er hieran mit, dann haftet er ebenfalls persönlich für die Steuern gemäß § 71 AO – und zwar in voller Höhe. Ein Geschäftsleiter ist daher gut beraten, bei den steuerrechtlichen Anforderungen des Unternehmens die eigene Haftung nicht aus den Augen zu verlieren. Das gilt umso mehr, als diese Anforderungen stetig komplexer werden, Pflichtverstöße aber gleichzeitig immer konsequenter verfolgt werden.



Und es kommt noch eine weitere Facette hinzu. In den seltensten Fällen kümmert sich nämlich ein Vorstand oder Geschäftsführer selbst um die Steuererklärung. Vielmehr wird diese Aufgabe in der Regel in die Steuer- oder Finanzabteilung delegiert, was bei internationalen Konzernen mit vielen Tochtergesellschaften zu einem komplexen System wird – für das in letzter Instanz immer der Geschäftsleiter verantwortlich bleibt. Gesellschaftsrechtlich sind ein Vorstand gemäß § 91 (2) Aktiengesetz (AktG) und auch ein Geschäftsführer verpflichtet, für angemessene und wirksame Überwachungsmaßnamen zu sorgen. Sie müssen sicherstellen, dass die unternehmerisch bedeutenden Vorgaben der Geschäftsleitung auch eingehalten werden. Hierzu gehören verschiedene Anforderungen, aber natürlich auch Compliance und gerade Tax Compliance. Bei Zweifeln an der Angemessenheit und Wirksamkeit dieser Überwachungsmaßnahmen dreht sich die Beweislast um. Dann ist es an der Geschäftsleitung, diesen Nachweis zu erbringen. Gelingt das nicht, droht auch hier die persönliche Haftung.

Wie kann eine solche Überwachung sichergestellt werden?

Dr. Jan-Hendrik Gnändiger Mit dieser Frage sind wir bei der allgemeinen Unternehmensüberwachung, also der Corporate Governance. Eine Möglichkeit ist ein Compliance Management-System. Mit einem solchen System können bestimmte Compliance-Risiken minimiert und Verstöße verhindert werden. Und das schließt natürlich auch die Minimierung von Tax Compliance-Risiken ein!

Was sind denn die typischen Risikofelder im Bereich Tax Compliance?

Dr. Jan-Hendrik Gnändiger Das lässt sich nicht pauschal bestimmen. Dafür muss man die unternehmensindividuellen steuerlichen Risiken kennen. In einem ersten Schritt sollten dazu die steuerlichen Themenfelder abgegrenzt werden und anschließend szenariobasiert Risikoüberlegungen angestellt werden. In der Praxis zeigt sich aktuell großer Beratungsbedarf zum Thema § 37b Einkommensteuergesetz (EStG), natürlich zum Thema Umsatzsteuer bzw. Vorbereitung und Abgabe von Steuererklärungen insgesamt, aber auch zu Transfer Pricing und zu den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).

„Ein risikoorientierter Prozess sowie organisatorische Sicherungs- und Kontrollmaßnahmen tragen zur Risikominimierung bei und werden **vom Gesetzgeber in aller Regel auch explizit gefordert**."

Wie können derartige Risiken minimiert werden?

Dr. Jan-Hendrik Gnändiger Mit einem risikoorientierten Prozess und angemessenen und wirksamen Maßnahmen – sprich: betriebswirtschaftlichen, organisatorischen Sicherungsmaßnahmen und Kontrollaktivitäten. Sie werden vom Gesetzgeber in aller Regel auch explizit in steuerrechtlichen Vorschriften gefordert und in Teilen auch ausgeführt.

Welche Möglichkeiten zur Assurance gibt es?

Dr. Jan-Hendrik Gnändiger An dieser Stelle unterscheidet sich ein Tax Compliance Management-System tatsächlich etwas vom klassischen Compliance-System bei Antikorruption oder Kartellrecht. Während für diese Compliance Management-Systeme der IDW-Prüfungsstandard PS 980 gute Dienste leistet, führen wir Prüfungen von Tax Compliance Management-Systemen in der Regel nach dem internationalen Standard ISAE 3000 durch.

ISAE steht für International Standard on Assurance Engagements. Dieser internationale Prüfungsstandard betrifft in Abgrenzung zu anderen International Standards of Auditing (ISA) Prüfungsleistungen, die nicht Konzern- und Jahresabschlussprüfungen sind. In den Anwendungsbereich des ISAE 3000 fallen insbesondere das Interne Kontrollsystem (IKS) und Prozessprüfungen sowie Systemprüfungen.

Im Rahmen der Prüfung wird das Tax Compliance Management-System mit seinen relevanten organisatorischen Sicherungsmaßnahmen und Kontrollen anhand geeigneter Kriterien (Suitable Criteria) beurteilt. In der Regel bestimmen die gesetzlichen Vorgaben diese Kriterien.

Die im Rahmen des ISAE 3000 durchgeführten Prüfungen können mit hinreichender Sicherheit (Reasonable Assurance) oder mit begrenzter Sicherheit (Limited Assurance) durchgeführt werden. Eine Prüfung mit hinreichender Sicherheit führt zu einer Positivaussage in der Bescheinigung, bei der Prüfung mit begrenzter Sicherheit wird das Prüfungsurteil negativ formuliert. Im Fall der hinreichenden Sicherheit erlangt der Prüfer höhere Sicherheit etwa durch umfangreichere Stichproben und Prüfungsnachweise.

Am Ende einer ISAE 3000-Prüfung steht eine Bescheinigung (ISAE 3000 Report) eines unabhängigen Wirtschaftsprüfers zur Angemessenheit und Wirksamkeit einer organisatorischen Vorgehensweise aus dem Bereich Tax Compliance. Diese Bescheinigung ist nicht nur gegenüber dem Gesetzgeber wertvoll. Die Geschäftsleiter und Aufsichtsorgane erhalten eine Abbildung des Status quo, was die Erfüllung der steuerrechtlichen Vorschriften und der gesellschaftsrechtlichen Überwachungsverpflichtungen angeht, sowie Hinweise auf mögliche Verbesserungen.

„Ein **zertifizierter ISAE 3000-Report zur Tax Compliance** ist nicht nur gegenüber dem Gesetzgeber wertvoll, sondern gibt den Verantwortlichen auch wertvolle Hinweise zur Erfüllung der steuer- und gesellschaftsrechtlichen Überwachungsverpflichtungen."

Dr. Antonia Steßl
Manager, Governance & Assurance Services, KPMG

Die regulatorischen und gesetzlichen Vorgaben zum Thema Compliance werden immer komplexer, internationaler und vielschichtiger. Selbstverpflichtungen der Mitarbeiter zur Einhaltung von Regeln reichen nicht mehr aus. Daher ist es verständlich, dass immer mehr Unternehmen Compliance Management-Systeme installieren. Doch wer überwacht diese Systeme und stellt ihre Funktionsfähigkeit sicher?

Compliance vorhanden, Prüfung **bestanden**? Der Blick der **Internen Revision**.

Compliance Management-System (CMS) eingerichtet und zurück zum Tagesgeschäft? Nein, so leicht kommen Geschäftsleitung und Aufsichtsrat nicht aus ihren Kontroll- und Überwachungspflichten heraus. Das CMS muss auch funktionieren. Um eine unabhängige und wirksame Überwachung des CMS im Sinne guter Unternehmensführung (Corporate Governance) zu erreichen, wird gerne die Interne Revision (IR) als unternehmenseigene und prozessunabhängige Kontrollinstanz herangezogen.

Compliance – ein Teil der unternehmerischen Sorgfaltspflicht

Das Gesellschaftsrecht verlangt vom Vorstand bzw. der Geschäftsführung bei der Führung der Geschäfte die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Die hieraus abzuleitende Sorgfaltspflicht ist somit Grundlage jeglichen Handelns im Geschäftsverkehr. Danach ist die Geschäftsleitung verpflichtet, ein funktionsfähiges Überwachungssystem zur Früherkennung bestandsgefährdender Entwicklungen einzurichten. Wenngleich das CMS im Gesetz nicht explizit genannt wird, lässt sich aus dem beschriebenen Regelungsumfang des Risikomanagementsystems ein unmittelbarer Compliance-Bezug herleiten. Über den Grad der Ausgestaltung entscheidet die Geschäftsleitung, wobei sich einer Pflichtverletzung schuldig machen kann, wer kein CMS einrichtet. Im Zweifelsfall trifft den Vorstand die Beweislast. Sofern ein Aufsichtsrat besteht, hat er den Pflichtenrahmen der Geschäftsleitung wirksam zu überwachen. Verstoßen Vorstand oder Aufsichtsrat gegen ihre Pflichten, kann das zu Haftung und Schadensersatz führen.

Verstoßen Vorstand oder Aufsichtsrat gegen ihre Pflichten, kann das zu **Haftung und Schadensersatz** führen.

In der Praxis hat sich der Aufbau eines Compliance Management-Systems nach dem **IDW-Prüfungsstandard PS 980** bewährt.

Diese Sorgfalts- und Aufsichtspflichten lassen sich in der Praxis mit der kombinierten Anwendung eines Compliance Management-Systems (CMS), eines Risikomanagementsystems (RMS) und eines Internen Kontrollsystems (IKS) umsetzen, deren Funktionsfähigkeit durch die IR überwacht werden sollte.

Jedes der Instrumente hat seine Funktion: Das RMS soll Unternehmensrisiken (frühzeitig) erkennen, bewerten und mit geeigneten Maßnahmen und Kontrollen des IKS steuern. Aus Regelverstößen resultierende Risiken werden in der Regel an das CMS „ausgelagert“ und mit eigenen Bewertungs- und Steuerungsmaßnahmen

Die Interne Revision sollte zwischen **prozessunabhängigen und prozessintegrierten** Compliance-Maßnahmen und -Kontrollen unterscheiden.

hinterlegt. Zu den Aufgaben der IR gehört somit auch die Überwachung des CMS im Sinne einer fortlaufenden Überprüfung der damit verbundenen Prozesse und Maßnahmen, sogenannte Compliance Audits.

Compliance systematisch verpackt

Ein CMS definiert sich über die Gesamtheit an Grundsätzen, Maßnahmen und Kontrollen, die der Einhaltung von Gesetzen und internen Vorgaben dienen. Sein Ziel ist es, Compliance-Verstöße (Zuwiderhandlungen gegen Gesetz und interne Vorgaben) zu vermeiden oder aufzudecken. In der Praxis hat sich der Aufbau eines CMS nach dem allgemein anerkannten Prüfungsstandard PS 980 des Instituts der Wirtschaftsprüfer (IDW) bewährt.

Ausgangspunkt für Aufbau und Inhalt eines CMS sind in der Regel die jeweils relevanten juristischen Teilbereiche von Korruption über Kartellrecht bis Datenschutz, aus denen Risiken und Maßnahmen erwachsen können. Durch diesen Fokus haben die Unternehmen die Chance, die Compliance-Risiken effizient und effektiv mittels Compliance-Programmen zu reduzieren. Eine weitere Voraussetzung für effektives Compliance-Management ist natürlich, dass Compliance-Themen fester Teil der Kommunikation sind und mit der Zeit eine Compliance-Kultur entstehen lassen.

Prüfungsgegenstände definieren

Unabhängig von der formalen Deklaration dieser Elemente und dem organisatorischen Aufbau des CMS ist für die Tätigkeiten der IR entscheidend, wie und in welchem Umfang sie im Rahmen ihrer Compliance-Überwachung Prüfungsgegenstände für ein Prüfungsprogramm ableiten muss.

Die Compliance-Abteilung kann aus systemischer Sicht sowohl selbst Initiator von Compliance-Maßnahmen und Kontrollen sein als auch beratend auf Prozessebene die operativen Abteilungen unterstützen und zudem am bereits bestehenden IKS oder RMS anknüpfen. Für Zwecke der IR-Systematisierung lässt sich das CMS in zwei grundsätzliche Kategorien einteilen (siehe Abbildung auf Seite 33). Die geschäftsprozessunabhängigen und somit auf Unternehmensebene gelagerten Prozesse, Maßnahmen und Kontrollen sind übergeordnet und liegen in der Regel im Verantwortungsbereich der Compliance-Abteilung. Hierzu gehören insbesondere Maßnah-

Elemente des **IDW PS 980**

Quelle: KPMG

1 Compliance-Kultur
- Bewusstsein für die Bedeutung von Regeln als Grundlage für die Angemessenheit und Wirksamkeit des CMS
- Wesentlicher Einflussfaktor: Grundeinstellung und Verhaltensweisen des Managements („Tone at the Top")

2 Compliance-Ziele
- Festlegung wesentlicher zu erreichender CMS-Ziele auf Grundlage der allgemeinen Unternehmensziele
- Festlegung der relevanten Teilbereiche und der darin einzuhaltenden Regeln

3 Compliance-Organisation
- Bestimmung der Aufbau- und Ablauforganisation
- Festlegung von Rollen, Verantwortlichkeiten und Berichtswegen
- Bereitstellung notwendiger Ressourcen

4 Compliance-Risiken
- Identifikation wesentlicher Compliance-Risiken
- Einführung systematischer Verfahren zur Risikoerkennung und -berichterstattung
- Analyse der Risiken

5 Compliance-Programm
- Einführung von Grundsätzen und Maßnahmen zur Begrenzung von Risiken und Vermeidung von Verstößen
- Dokumentation (zum Beispiel Leitlinien, Regelwerke etc.)

6 Compliance-Kommunikation
- Information betroffener Mitarbeiter und gegebenenfalls Dritter über das Compliance-Programm sowie die Rollen/Verantwortlichkeiten
- Festlegung der Berichtswege für Compliance-Risiken und für Hinweise auf Regelverstöße

7 Compliance-Überwachung und -Verbesserung
- Überwachung der Angemessenheit und Wirksamkeit
- Voraussetzung: ausreichende Dokumentation
- Berichterstattung über Schwachstellen und Verstöße
- Management trägt Verantwortung und sorgt für die Durchsetzung und Verbesserung des CMS

Beispielhafte **Systematisierung des CMS** für den Teilbereich Korruption

Quelle: KPMG in Deutschland, 2015

men zum Aufbau einer Compliance-Kultur, das Compliance-Risikomanagement und Compliance-Schulungen. Das Compliance-Risikomanagement ist der wesentliche Treiber einer Compliance-Organisation und bestimmt maßgeblich den Umfang der Compliance-Programminhalte. Die im Compliance-Programm enthaltenen Maßnahmen und Kontrollen können sowohl einen geschäftsprozessunabhängigen als auch geschäftsprozessintegrierten Charakter aufweisen. Typischerweise zählen zu den geschäftsprozessunabhängigen Maßnahmen ein Vorfallmanagement, ein Hinweisgebersystem oder Compliance-Richtlinien (zum Beispiel gegen Korruption). Dagegen stellen etwa Berechtigungskonzepte, Funktionstrennungen und Genehmigungsverfahren in der Regel prozessintegrierte Kontrollen mit einem Compliance-Bezug dar.

Compliance-Prozesse analysieren und Verantwortlichkeiten zuweisen

Die Klassifizierung und Verantwortungszuweisung derartiger Prozesse und Maßnahmen ist entscheidend, um einen eindeutigen Prozessinhaber zu identifizieren. Die Relevanz dieser Zuordnung zeigt sich insbesondere dann, wenn die IR gleichzeitig die Compliance-Verantwortung übernimmt.
Zur Ableitung eines risikoorientierten Prüfungsprogramms sollte die IR daher beide Ebenen berücksichtigen. Dazu muss sie erstens ein Verständnis dafür gewinnen, welche der für Compliance relevanten Maßnahmen bereits durch Prozessprüfungen in typischen Themenbereichen wie Einkauf, Verkauf oder Finanzen regelmäßig abgedeckt werden. Zweitens muss sie festlegen, welche zusätzlichen Prüfungserfordernisse auf Ebene der Compliance-Abteilung zur Sicherstellung einer umfänglichen Systemprüfung notwendig sind. Häufig beschränkt sich der Revisionsumfang auf prozessintegrierte Maßnahmen und Kontrollen, die im Regelfall nur einen begrenzten Ausschnitt aus dem gesamten CMS darstellen. Die Angemessenheit und Wirksamkeit des ganzheitlichen CMS kann durch eine Beschränkung der Prüfung auf prozessintegrierte Maßnahmen und Kontrollen nicht hinreichend sichergestellt werden. Vielmehr sind sie lediglich Ergebnis übergeordneter Maßnahmen wie dem Compliance-Risikomanage-

> Die Angemessenheit und Wirksamkeit eines ganzheitlichen CMS kann durch eine Beschränkung der Prüfung auf prozessintegrierte Maßnahmen und Kontrollen **nicht hinreichend sichergestellt** werden.

Die **Intensität der Zusammenarbeit** zwischen Interner Revision und Compliance-Abteilung wird zunehmen.

ment, die den Umfang und die Intensität solcher Kontrollen festlegen.

Eine Analyse dieser prozessunabhängigen Maßnahmen im Austausch mit der Compliance-Abteilung kann sinnvoll erscheinen, um unter anderem nachstehende, beispielhafte Prozesse in den CMS-Prüfungsumfang zu integrieren:

1 Compliance-Risikomanagementprozess
2 Compliance-Schulungsprozess
3 Eskalationsprozess
4 Sanktionierungsprozess
5 Vorfallmanagement
6 Evaluierungsprozess von Compliance-Anfragen

Compliance-Zuständigkeit nimmt Einfluss auf den Prüfungsumfang

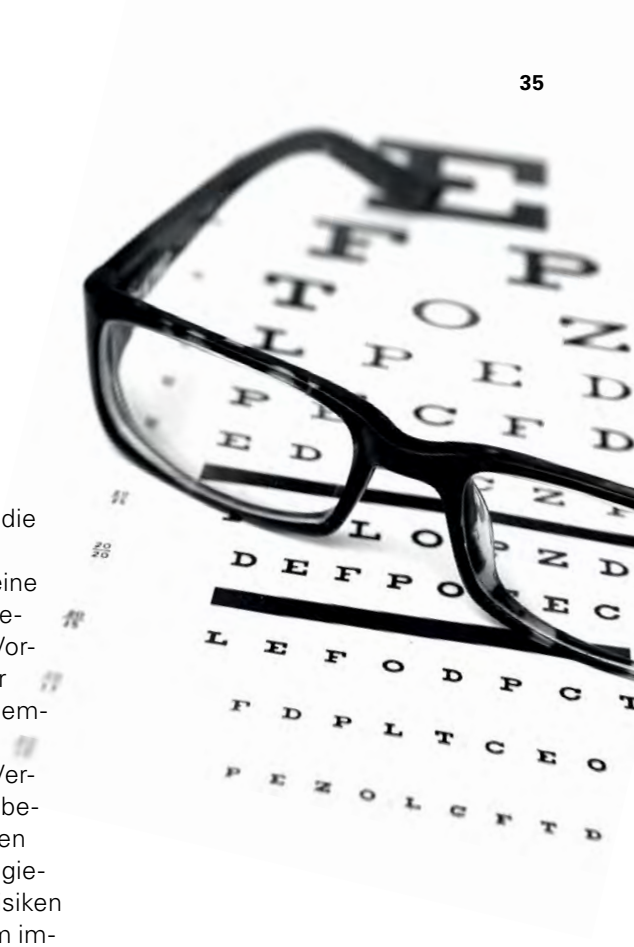
In Abhängigkeit von der Risikoexposition, Größe und Komplexität des Unternehmens kann die Verantwortung zur Steuerung eines CMS in einer dafür eigens geschaffenen Abteilung liegen oder von einer themenverwandten Abteilung, zum Beispiel der IR, übernommen werden. Die Compliance-Organisation ist somit ein weiterer wesentlicher Parameter zur Bestimmung des Prüfungsumfangs. Sofern die IR gleichzeitig das Compliance Management übernimmt, können Prozesse, deren Konzeption und Durchführung im Verantwortungsbereich der IR liegen, grundsätzlich nicht mehr geprüft werden (Selbstprüfungsverbot). Eine Identifikation eigeninitiierter Prozesse und Maßnahmen sowie ihre regelmäßig unabhängige Prüfung sind in einer solchen Organisationskonstellation zusätzlich sicherzustellen.

Wenn das Compliance Management in eine eigene Organisationseinheit mit separaten Berichtswegen ausgegliedert ist, ist eine Zusammenarbeit mit der IR zum Zwecke eines effizienten Prüfungsprogramms zu empfehlen. Hierbei ist ein gemeinsames Verständnis von Compliance-Risiken und ihrer Bewertung sowie der abgeleiteten Steuerungsmaßnahmen wichtig, um prozessunabhängige, aber auch prozessintegrierte Compliance-Maßnahmen und -Kontrollen eindeutiger als Prüfungsgegenstände zu definieren (Abbildung auf Seite 33).

Dieser Austausch ersetzt keinesfalls die Selbsteinschätzung von Risiken und Prüfungsinhalten durch die IR, er kann jedoch die Prüfungsprogramme der IR risikoorientiert ergänzen. Die Intensität der Zusammenarbeit mit der Compliance-Abteilung wird zunehmen.

Qualitätssicherungsprogramme der Compliance-Abteilung können die Interne Revision sinnvoll ergänzen

Zusätzlich zur unabhängigen Überwachung durch die Interne Revision können eigenständige Compliance-Organisationen Qualitätssicherungsprogramme (Quality Assurance) auferlegen, um die Wirksamkeit der durch sie eingeführten Prozesse zu überwachen. Maßgeblicher Treiber eines solchen Programms sind internationale und dezentrale Compliance-Organisationsstrukturen. Ihre konkrete Ausgestaltung ist von der Größe, Internationalität und Komplexität des Konzerns abhängig. In der Praxis haben sich sogenannte Selbsteinschätzungen (Self-Assessments), Compliance Reviews und punktuelle Überprüfungen (Spot Checks) etabliert. Zum Zwecke der Selbsteinschätzung werden Fragebögen an dezentrale Geschäftseinheiten versandt, um den Umsetzungsstand von Compliance-Maßnahmen zu verfolgen und nachzuhalten. Die systematische und regelmäßige Auswer-



tung dieser Fragebögen kann den Compliance-Reifegrad von dezentralen Geschäftseinheiten aufzeigen, zusätzlichen Überprüfungsbedarf (Reviews) auslösen und somit das Compliance Management zusätzlich verbessern. Zur Förderung der wirksamen Umsetzung können punktuelle und stichprobenartige Überprüfungen ausgewählter Prozesse und Maßnahmen in dezentralen Geschäftseinheiten physisch vor Ort oder per Fernabfrage stattfinden.

Zunehmende Regulierungsdichte stellt Interne Revision vor neue Herausforderungen

Die Notwendigkeit zur Implementierung von Compliance-Strukturen in einem Unternehmen ist keineswegs neu. Die vergangenen Jahre waren jedoch geprägt durch steigende Aufmerksamkeit der Öffentlichkeit gegenüber Wirtschaftskriminalität, durch fortlaufende Rechtsprechung sowie neue (inter)nationale Gesetze und Gesetzgebungsverfahren. Sie haben zu einer stetig wachsenden Vorsicht in den Unternehmen geführt. Im Ergebnis wurden die bereits vorhandenen Compliance-Maßnahmen systematisiert und neue geschaffen. Ihre Funktionsfähigkeit ist nun durch die IR fortlaufend sicherzustellen. Die IR hat demnach die Compliance-Prozesse und -Maßnahmen in bestehende Prüfungsansätze und -programme zu integrieren und die Funktionsfähigkeit des CMS als Ganzes risikoorientiert und regelmäßig zu prüfen. Hierbei sind insbesondere die prozessübergreifenden Compliance-Maßnahmen zu identifizieren und in einen risikoorientierten Prüfungsplan überzuleiten. Üblicherweise ergänzen sie bereits bestehende, prozessintegrierte Maßnahmen und Kontrollen mit Compliance-Bezug im Prüfungsprogramm. Insgesamt ist sicherzustellen, dass alle wesentlichen Prozesse und Maßnahmen durch die IR abgedeckt werden.

Das CMS ist bedingt durch seine Orientierung an Rechtsgebieten respektive internen oder externen Vorgaben dynamisch. Ein besonderer Schwerpunkt der Prüfung sollte demnach auch darauf gelegt werden, inwieweit das bestehende CMS Veränderungsrisiken in einzelnen Teilbereichen durch Gesetzesänderungen erkennt und darauf rechtzeitig reagieren kann. Werden Veränderungsrisiken systematisch und regelmäßig vom implementierten CMS verfolgt, kann sich das prüfungsreduzierend auswirken.

> Es muss sichergestellt werden, dass **alle wesentlichen Compliance-Prozesse und -Maßnahmen** durch die Interne Revision abgedeckt werden.

Compliance-Audits können vielfältig sein

Der Begriff Compliance-Audits ist weit gefasst und kann in Abhängigkeit von den Compliance-Risiken im Unternehmen vielfältige Formen annehmen. Auch wenn solche Risiken durch Gesetze, Verordnungen oder sonstige Verpflichtungen des Unternehmens ausgelöst werden, liegt die Verantwortung zur Steuerung dieser Risiken nicht immer zwangsläufig in einer eigens hierfür geschaffenen Compliance-Abteilung. Je enger Compliance-Risiken mit konkreten Unternehmensprozessen, wie zum Beispiel Technik, Produktion und Umwelt sowie Steuern und Nachhaltigkeit, verzahnt sind, desto wahrscheinlicher ist die Steuerung dieser Compliance-Risiken in den entsprechenden Fachabteilungen. In

Die Interne Revision muss das Compliance Management-System **als ganzheitliches System** betrachten.

solchen Konstellationen obliegt der Compliance-Abteilung vielmehr die Bewältigung „prozessuniverseller" Compliance-Risiken, wie Korruption, Fraud oder Kartellrecht, deren Auswirkungen einen abteilungsübergreifenden Charakter haben. Welche Compliance-Risiken durch die Compliance-Abteilung gesteuert werden, hängt von der organisatorischen Ausrichtung und den bereitgestellten Kapazitäten ab.

Die Interne Revision hat mit Bezug zur unternehmensindividuellen Compliance-Risikolandkarte und in Abhängigkeit von den zugewiesenen Verantwortlichkeiten Compliance-Audits zu definieren und fachspezifisch zu besetzen. Die Durchführung von Compliance-Audits in all ihren Ausprägungen hat das gemeinsame und fundamentale Prüfungsziel, die Angemessenheit und Wirksamkeit prozessübergreifender und prozessintegrierter Maßnahmen und Kontrollen zu beurteilen und daraus Handlungsempfehlungen zur Verbesserung des CMS für die Organisation abzuleiten. Die Zuweisung einzelner Prüfungstypen und -gebiete ist nicht trivial und hängt stark vom Unternehmensumfeld, den Compliance-Risiken und der Organisationsausgestaltung ab.

Komplexität des CMS fordert die Interne Revision

Die zunehmende Komplexität des CMS führt gleichermaßen zu einer steigenden Prüfungsintensität. Die hierfür zur Verfügung stehenden Ressourcen innerhalb der IR sind üblicherweise beschränkt und stellen die IR sowohl personell als auch fachlich vor neue und sich fortlaufend ändernde Herausforderungen. Vor allem die Prüfung der Angemessenheit eines CMS setzt sowohl betriebswirtschaftliches als auch juristisches Fachwissen voraus, um beurteilen zu können, ob und inwieweit die vorhandenen Compliance-Maßnahmen und -Kontrollen die unternehmensspezifischen Compliance-Risiken wirksam reduzieren. Die Sicherstellung der Wirksamkeit des CMS hat sowohl gegenwärtig als auch zukünftig eine hohe Bedeutung für die IR.

Mögliche **Compliance-Audit-Typen**

Bezeichnung
Compliance-Audit als Revisionsaufgabe in verschiedenen Risikofeldern
Compliance-Audit in Form eines Self-Assessments
Compliance-Reviews als Qualitätssicherungsmaßnahme
Fraud-Audits
Investigationen
Technische/umweltbezogene Compliance-Audits
Tax Compliance-Audits
IT Compliance-Audits
Soziale und Nachhaltigkeits-Audits
Compliance-Audits nach IDW PS 980

durchgeführt von	Zeitpunkt	Methodik/Prüfungsziele
Interne Revision/extern	Regelmäßig	– System- und Stichprobenprüfung vor Ort – Einhaltung interner und externer Vorgaben – Angemessenheit und Wirksamkeit vorhandener Maßnahmen und Kontrollen – Aufdeckung von Verbesserungspotenzialen
Interne Revision/ Compliance-Abteilung	Regelmäßig	– Konzernweite Befragung – Einhaltung interner und externer Vorgaben – Kenntnis über vorhandenes Kontrollumfeld und Ableitung von (neuen) Prüfungs-/Risikofeldern
Compliance-Abteilung	Regelmäßig	– Stichprobenprüfung und Befragung – Einhaltung der vorgegebenen Kontrollstrukturen – Angemessenheit und Wirksamkeit von Kontrollmaßnahmen – Aufdeckung von Verbesserungspotenzialen
Interne Revision/extern	Anlassbezogen	– Stichprobenprüfung vor Ort – Aufdeckung von dolosen Handlungen ohne konkrete Verdachtsmomente
Interne Revision/ Compliance-Abteilung/extern	Anlassbezogen	– Investigative Untersuchung von Compliance-Verstößen – Aufdeckung und Konkretisierung von Verdachtsmomenten
Interne Revision/Umwelt-beauftragte/Energiebeauftrage/ Produktionsleiter/extern	Regelmäßig oder anlassbezogen	– Befragung, Vor-Ort-Erhebung – Stichprobenprüfung – Einhaltung relevanter Gesetze, Verordnungen und Bescheide – Aufdeckung von Verbesserungspotenzialen
Interne Revision/Compliance-Abteilung/Steuerabteilung/extern	Regelmäßig oder anlassbezogen	– System- und Stichprobenprüfung der Steuerfunktionen – Compliance-konforme Sicherstellung von Steuerprozessen (zum Beispiel UStG-Anforderungen)
Interne Revision/Compliance-Abteilung/Datenschutzbeauftragte/ IT-Abteilungen/extern	Regelmäßig	– System- und Stichprobenprüfung vor Ort – Einhaltung interner und externer Vorgaben mit IT-Bezug – Aufdeckung von Verbesserungspotenzialen
Interne Revision/Nachhaltigkeits-abteilung (CSR-Abteilung)/extern	Regelmäßig	– System- und Stichprobenprüfung vor Ort – Einhaltung interner und externer Vorgaben zu sozialen Aspekten und Nachhaltigkeitsthemen – Aufdeckung von Verbesserungspotenzialen
Externer Prüfer	Periodisch	– System- und Stichprobenprüfung auf Konzern- und Einheitsebene – Unabhängige Beurteilung der Konzeption, Angemessenheit und Wirksamkeit des Compliance Management-Systems – Aufdeckung von Verbesserungspotenzialen

Das Ganze sehen!

Die Überwachung des CMS und somit auch die Aufdeckung von Verbesserungspotenzialen obliegen innerbetrieblich der IR. Sie hat durch geeignete Prüfungspläne und -programme die fortlaufende Funktionsfähigkeit des CMS zu überprüfen. Hierbei ist es entscheidend, das CMS als ganzheitliches System zu betrachten. Die beschränkten Kapazitäten der IR, die CMS-immanenten Besonderheiten sowie der hohe Objektivierungs- und Sicherheitsgrad führen immer wieder dazu, dass sich Unternehmen für eine externe Prüfung des CMS entscheiden.

Florian Maciuca
Manager, Governance & Assurance Services, KPMG

Bitte **wenden**!

Energiewende fordert **Veränderung** bei Unternehmen wie Prüfern.

Wir alle sind Teil eines spannenden Experiments mit offenem Ausgang: der Energiewende. Durch Glühlampenverbot oder EEG-Umlage sind ihre Auswirkungen für jeden Verbraucher spürbar. Aber insbesondere die Folgen für Unternehmen sind ein großes Thema. Befürworter versprechen sich neue Wachstumsmöglichkeiten und geringere Energiekosten, Gegner fürchten hohe zusätzliche Kosten.

Die Marschrichtung ist klar, und auch über die Ziele herrscht weitgehende Einigkeit: Das Klima soll geschützt werden, die Abhängigkeit von fossilen Energieträgern reduziert und ein effizienterer Umgang mit Energie erreicht werden. Die konkrete Umsetzung der Ziele ist jedoch ein Dauerthema in Politik und Presse.

Mit der Energiewende ist die Zahl der Instrumente gestiegen; die Regulierungsdichte in den Bereichen Energie und Klimaschutz hat deutlich zugenommen. Einerseits werden damit Innovationsanreize geschaffen, andererseits sind enorme Herausforderungen für die Unternehmen damit verbunden. Nicht zuletzt müssen Wirtschaftsprüfungsgesellschaften ihr Kompetenzspektrum erweitern, um diese Entwicklungen prüferisch begleiten zu können.

Wirtschaftsprüfungsgesellschaften müssen ihr **Kompetenzspektrum erweitern**, um die Energiewende prüferisch begleiten zu können.

Spitzenlastausgleich erfordert Energiemanagement

Klimaschutz setzt in sehr vielen Fällen bei einem effizienten Umgang mit Energie an. Das Bundeskabinett wird daher in Kürze den dritten Nationalen Aktionsplan Energieeffizienz verabschieden. Bereits in den letzten Jahren haben Energiemanagementsysteme aufgrund von regulatorischen Anreizen stark an Bedeutung gewonnen. So setzt das Erneuerbare-Energien-Gesetz (EEG) für die Besondere Ausgleichsregelung nach § 40 EEG ein zertifiziertes Energiemanagementsystem voraus. In ähnlicher Weise können Unternehmen des produzierenden Gewerbes den Spitzenlastausgleich im Rahmen der Energie- und Stromsteuer in Anspruch nehmen, wenn sie über das Umweltmanagementsystem EMAS, ein Energiemanagementsystem nach ISO 50001 oder ein vergleichbares System verfügen bzw. an dessen Einführung arbeiten. Kleine Unternehmen können alternativ auch Energieaudits durchführen. Anders als beim EEG geht in die Berechnung des Spitzenlastausgleichs neben der zu entrichtenden Steuerlast für Strom und andere Energien auch der Arbeitgeberanteil in die allgemeine Rentenversicherung ein.

Ein **Energiemanagement-system** als systematischer Ansatz zur Verbesserung der energetischen Leistung ermöglicht neben finanziellen Vorteilen deutliche Energieeinsparungen und Transparenz über die Energieströme.

Die Besondere Ausgleichsregelung und der Spitzenlastausgleich haben viele Unternehmen veranlasst, ein Energiemanagementsystem zu implementieren. Dieser systematische Ansatz zur Verbesserung der energetischen Leistung bringt aber mehr als finanzielle Vorteile. Die Unternehmen erzielen auch deutliche Energieeinsparungen und erreichen eine höhere Transparenz über ihre Energieströme.

Neues Energiedienstleistungsgesetz verpflichtet zu Energieaudits

Auch auf der europäischen Ebene geht der Trend hin zu mehr Energieeffizienz. Bereits 2012 hat die EU-Kommission in der Richtlinie 2012/27 zur Energieeffizienz vorgeschrieben, dass alle Unternehmen, die nicht unter die kleinen und mittelständischen Unternehmen (KMU) fallen, bis zum 5. Dezember 2015 ein Energieaudit nach DIN EN 16247-1 durchführen müssen. Dieses Audit soll dann im Vierjahresrhythmus erneuert werden. Die Bundesregierung reagiert nun darauf mit der Überarbeitung des Energiedienstleistungsgesetzes. Im Dezember 2014 hat auch der Bundesrat zu dem Entwurf Stellung genommen; insofern ist mit einem Inkrafttreten in der ersten Jahreshälfte 2015 zu rechnen. Die Bundesregierung geht davon aus, dass etwa 50.000 Unternehmen von dem neuen Gesetz betroffen sein werden. Ausgenommen von der Regelung sind neben den KMU nur Unternehmen, die bereits ein Energiemanagementsystem gemäß ISO 50001 betreiben oder ein Umweltmanagementsystem nach EMAS besitzen.

Energieaudits können Effizienzpotenziale in Unternehmen identifizieren und so einen wichtigen Beitrag zur Energiewende leisten. Es ist eine Herausforderung für die Unternehmen, die Vorgaben zu erfüllen, und für die Prüfer, die Masse an Audits durchzuführen. Ein Engpass an Auditoren ist zu erwarten, sodass es unwahrscheinlich ist, dass wirklich alle Unternehmen es schaffen, bis zum 5. Dezember 2015 ein Energieaudit durchzuführen. Entsprechend regt sich Widerstand in der Industrie und anderen betroffenen Sektoren wie etwa dem Handel; die Forderung nach Fristverlängerung wird laut. An der grundsätzlichen Vorgabe, dass große Unternehmen sich des Themas Energieaudits annehmen müssen, wird sich jedoch aufgrund der europäischen Vorgaben nichts ändern.

Emissionsberichte für mehr als 11.000 Anlagen jährlich

Ein etabliertes Tool zur Umsetzung der Energiewende ist der EU-Emissionshandel. Die Relevanz dieses Instruments ist hoch, da der Handel mit Emissionsberechtigungen als das wichtigste klimapolitische Instrument der EU gilt und der Teilnehmerkreis mit Beginn der dritten Handelsperide 2013 auf

Das neue Energiedienstleistungsgesetz wird etwa **50.000 Unternehmen zu regelmäßigen Energieaudits verpflichten**. Die Bundesregierung rechnet insgesamt mit Kosten von 200 Millionen Euro in den nächsten vier Jahren.

Joachim Ganse
Geschäftsführer KPMG Cert GmbH
Frieder Frasch
Manager, Governance & Assurance Services, KPMG

Die EU-Kommission geht davon aus, dass durch die Finanz- und Wirtschaftskrise ein **Überschuss von mehr als einer Milliarde Emissionsberechtigungen** entstanden ist.

europaweit mehr als 11.000 Anlagen ausgeweitet wurde. Die EU-Kommission geht davon aus, dass durch die Finanz- und Wirtschaftskrise ein Überschuss von mehr als einer Milliarde Emissionsberechtigungen entstanden ist. Der Überschuss drückt die Preise der Berechtigungen, sodass aktuell verschiedene Eingriffe in den Emissionshandel diskutiert werden, um den Preis der Emissionsberechtigungen zu stützen. Sehr wahrscheinlich wird in den nächsten Jahren eine Marktstabilitätsreserve eingeführt, die die Zahl der zu versteigernden Zertifikate an die jeweilige Marktentwicklung anpasst.

Energieaudits erfordern **interdisziplinäre Teams**, in denen Spezialisten aus dem technischen und naturwissenschaftlichen Bereich mit Wirtschaftsprüfern zusammenarbeiten.

Unverändert gilt, dass die Treibhausgasemissionen jeder dieser Anlagen im Rahmen jährlicher Emissionsberichte dokumentiert werden müssen. Die Deutsche Emissionshandelsstelle als zuständige Behörde akzeptiert dabei nur Emissionsberichte, die von einer akkreditierten Prüfstelle mit hinreichender Prüfungssicherheit (Reasonable Assurance) geprüft wurden.

Ökonomisches und technisches Know-how gefragt

Neben den regulären Aufgaben sehen sich Prüfer vor dem Hintergrund der Energiewende immer häufiger mit hochspezialisierten Prüfungen konfrontiert. Joachim Ganse, Geschäftsführer der KPMG Cert GmbH: „In unseren Gesprächen mit Mandanten beobachten wir deutlich, dass technische Fragestellungen mit hoher ökonomischer Tragweite immer häufiger an externe Prüfer weitergegeben werden. Dadurch verändert sich auch unsere Arbeitsweise. Kollegen aus den unterschiedlichsten Disziplinen, vor allem aus dem technischen und naturwissenschaftlichen Bereich, bilden heute das Experten-Team der KPMG Cert GmbH und arbeiten eng mit den Wirtschaftsprüfern zusammen."

Ein Beispiel für die interdisziplinäre Zusammenarbeit ist die Prüfung der Anträge zur Strompreiskompensation, bei der Produktionsmengen und Stromverbräuche zu prüfen sind. An komplexen Industriestandorten sind interdisziplinäre Prüfungsteams aus Wirtschaftsprüfern und technischen Sachverständigen erforderlich, um die notwendige Expertise sicherzustellen. Umgekehrt ist es für die Unternehmen wichtig, Komplettlösungen aus einer Hand zu bekommen und sich dabei sowohl auf das ökonomische als auch das technische Know-how der Prüfteams verlassen zu können.

KPMG

cutting through complexity

Social Media in Deutschland ist schon lange kein Hype mehr, sondern **Teil unseres Alltags**.

Welcher Social Media-Typ sind Sie?

In der letzten Ausgabe des Assurance Magazins zum Schwerpunktthema „Digital Assurance" baten wir unsere Leser um Teilnahme an einem Test zur Ermittlung des **individuellen Social Footprint**.

Kennen Sie die Antwort?

Der **Power User** versteht es, seine Geschäfts- und Arbeitsprozesse zu digitalisieren, und kann dadurch gezielt Kosten sparen. Zudem ist er immer up to date, aktuelle Neuigkeiten entgehen ihm nicht.

Der **Fan** kennt Neuigkeiten und Trends meist, bevor sie sich viral verbreiten. Er erfasst aktuelle Neuigkeiten schnell und weiß genau, über welche Kanäle sie am besten verbreitet werden sollten.

Der **Netzwerker** vermag es selbst bei hoher Arbeitsbelastung, den Kontakt mit Freunden und Familie zu pflegen. Beruflich besteht jedoch noch offenes Potenzial, um Kundenbindungen noch effizienter zu gestalten.

Der **Skeptiker** legt Wert auf persönlichen Kontakt und vermag es, in dezentem Rahmen im sozialen Netz zu interagieren.

Vielen Dank für Ihre engagierte Teilnahme an der Umfrage! Freuen Sie sich auf **eine eingehende Betrachtung** der vier Social Media-Typen, der damit verbundenen Möglichkeiten und der Risiken **in der nächsten Ausgabe** des Assurance Magazins!

Finanzielle Zuwendungen der Arzneimittelhersteller an die Ärzte müssen nun auch in Deutschland offengelegt werden. Die Vereine FSA und AKG haben dazu neue Transparenz-regelungen veröffentlicht. Pharmaunternehmen, die diesen Verbänden angehören, müssen unter bestimmten Bedingungen seit dem 1. Januar 2015 Daten sammeln und sie ab 2016 veröffentlichen.

Verordnete Transparenz

Neue Regeln rücken **Patienten-wohl** wieder ins Zentrum.

Spekulationen darüber, dass manche Ärzte ihre Verordnungsentscheidung weniger am Wohl der Patienten als an Vergünstigungen der Pharmaindustrie festmachen, gab es immer wieder. Und das längst nicht nur in Deutschland. Viele andere Länder haben darauf bereits reagiert und verlangen mehr Transparenz über die Zusammenarbeit zwischen Industrie und Medizinern. Ein Beispiel ist der Physician Payment Sunshine Act aus den USA, nach dem einige deutsche Pharmahersteller bereits finanzielle Zuwendungen an US-Ärzte veröffentlichen müssen. In Ländern wie Frankreich, Japan und Großbritannien wurden ähnliche Regelungen erlassen.

Vertrauen in objektive Verordnungsentscheidungen stärken

Während manipulierte Verordnungsentscheidungen im Sinne des Patientenwohls zu Recht verhindert werden müssen, bleibt die Zusammenarbeit zwischen Pharmaunternehmen einerseits und Ärzten, Apothekern und anderen Fachkreisangehörigen andererseits unverzichtbar. Nur so kann die Industrie Praxiserfahrungen bei der Entwicklung von Arzneimitteln berücksichtigen und die Anwender nach erfolgreicher Zulassung später optimal schulen. Die neuen Regelungen sollen die Transparenz dieser Zusammenarbeit erhöhen – mit der Erwartung, dass die Allgemeinheit wieder darauf vertrauen kann, dass sich die Auswahl des Arzneimittels an den Vorteilen und den gesundheitlichen Bedürfnissen des Patienten orientiert. Damit würde auch Spekulationen hinsichtlich einer unlauteren Beeinflussung der Verordnungsentscheidung vorgebeugt werden.

Gemäß dem Transparenzkodex des Vereins Freiwillige Selbstkontrolle für die Arzneimittelindustrie (FSA) müssen die direkten oder indirekten Zuwendungen an Angehörige der Fachkreise oder Organisationen nun dokumentiert und ab 2016 öffentlich zugänglich gemacht werden. Erfassungspflichtige Zuwendungsempfänger können neben Ärzten, Apothekern, Krankenhäusern und Universitätskliniken auch Mitarbeiter von öffentlichen Stellen sein, die Einfluss auf die Verschreibung oder den Bezug von verschreibungspflichtigen Arzneimitteln haben.

Die **Zusammenarbeit** zwischen Pharmaindustrie und Ärzten, Apothekern sowie anderen Fachkreisangehörigen bleibt **unverzichtbar**. Nur so kann die Industrie Praxiserfahrungen berücksichtigen und die Anwender optimal schulen.

Schon die **Identifizierung und Dokumentation aller Zuwendungen und Zuwendungsempfänger** ist für viele Unternehmen eine große Herausforderung.

Anpassungsbedarf bei Prozessen und internen Kontrollen

Aus den neuen Regelungen ergibt sich eine Reihe von Herausforderungen. Eine der ersten ist es in der Regel, konzernweit alle relevanten Zuwendungsempfänger überhaupt zu identifizieren und in einer einheitlichen, zentralen Liste zusammenzuführen. Dies erfordert erfahrungsgemäß eine Anpassung der IT-Landschaft oder Implementierung eines zusätzlichen IT-Tools bzw. klare Definitionen und Vorgaben zur Identifikation und Pflege der Liste. Hier kann auf Daten des Rechnungswesens (zum Beispiel Kreditorensaldenlisten) bzw. auf Informationen des Customer Relationship Management-Systems (CRM) zurückgegriffen werden.

Darüber hinaus müssen laut Kodex auch indirekte geldwerte Leistungen angegeben werden, die über Intermediäre der Pharmaunternehmen – wie Vertragspartner, Agenturen oder Unternehmensstiftungen – fließen, sofern sie im Namen des Pharmaunternehmens erfolgen. Auch Zahlungen durch diese Intermediäre müssen also identifiziert und die entsprechenden Vorgänge nachgehalten werden. Das Pharmaunternehmen wiederum muss sicherstellen, dass die Informationen regelmäßig eingeholt und in einer Datenbank konsolidiert werden. Hierfür sollte ein Musterformular entwickelt werden und eine Rücklaufkontrolle eingerichtet werden, die die Meldungen auf Vollständigkeit und Plausibilität überprüft. Außerdem muss anschließend sichergestellt werden, dass die Liste der Fachkreisangehörigen und -organisationen kontinuierlich gepflegt wird.

Im IKS müssen die geldwerten Leistungen nach den gängigen Transparenzkodizes bei der Veröffentlichung in verschiedene Kategorien unterteilt werden – im Falle des FSA-Kodex sehen die Kategorien so aus:

- Forschung und Entwicklung im Zusammenhang mit der Planung und Durchführung von nichtklinischen Studien, klinischen Prüfungen der Phasen I bis IV und nichtinterventionellen Studien im Sinne von § 19 FSA-Kodex „Fachkreise“
- Spenden
- Geldwerte Leistungen im Zusammenhang mit Fortbildungsveranstaltungen
- Dienstleistungs- und Beratungshonorare

Dazu muss die neue IT-Plattform ebenfalls entsprechend programmiert werden bzw. das bestehende Enterprise Resource Planning-(ERP-)System um diese Funktion und Informationen erweitert werden. Das heißt, im ersten Schritt muss analysiert werden, welche Stammdaten bereits im System vorliegen und welche noch zusätzlich benötigt werden. Bei Zahlungen an einen Fachkreisangehörigen sollte also sichergestellt werden, dass sie nur nach Auswahl einer entsprechenden Kategorie möglich sind. Diese Kategorisierung sollte mit Freigabeprozessen und Kontrollen verbunden werden, die den zentralen Grundsätzen der Zusammenarbeit zwischen Industrie und medizinischen Einrichtungen Rechnung tragen:

Trennungsprinzip
Zuwendungen an Mitarbeiter medizinischer Einrichtungen dürfen nicht in Abhängigkeit von Umsatzgeschäften mit der medizinischen Einrichtung erfolgen.
Transparenz- und Genehmigungsprinzip
Zuwendungen sind gegenüber allen Beteiligten offenzulegen und vom Dienstherrn bzw. Arbeitgeber zu genehmigen.
Dokumentationsprinzip
Leistungsbeziehungen werden nachvollziehbar ausgestaltet und entsprechend schriftlich dokumentiert.
Äquivalenzprinzip
Leistung und Gegenleistung müssen in einem angemessenen Verhältnis zueinander stehen (zum Beispiel im Verhältnis zum Zeitaufwand, zum Schwierigkeitsgrad oder zur Kompetenz des Vertragspartners).

Die Chance besserer Entscheidungen

Der Anpassungsprozess ist arbeitsintensiv, doch er eröffnet auch eine Chance: Mit der größeren Datenbasis wird es möglich zu beurteilen, in welchen Bereichen und mit welchen Personen eine Kooperation überhaupt sinnvoll ist bzw. fortgeführt werden sollte. Die Steuerung der Interaktion mit den sogenannten Key Opinion Leaders wird optimiert.

Ein zusätzlicher Nutzen besteht in den erweiterten Analysemöglichkeiten, die im Zusammenhang mit dem Äquivalenzprinzip genutzt werden können. So können die Zahlungen für bestimmte Leistungen analysiert werden oder es können Durchschnittswerte ermittelt werden, die dann wiederum für eine Abweichungsanalyse verwendet werden können, was „Ausreißer" schnell enttarnt. Sofern die Zuwendungen an Ärzte und medizinische Einrichtungen auf einen bestimmten Betrag im Jahr limitiert werden sollen, kann vor Überschreitung eines festgelegten Schwellenwerts eine Warnmeldung im System vorgesehen werden.

Leichtere Umsetzung der Dokumentationspflicht

Sofern noch kein (elektronisches) Vertragsmanagement existiert, bietet es sich an, Verträge usw. in diesem Tool zu dokumentieren, um dem Dokumentationsgrundsatz gerecht zu werden.

Zur Kontrolle, ob alle geldwerten Leistungen vollständig erfasst wurden, kann man darüber hinaus regelmäßig einen Abgleich der Zahlungen gemäß Transparenzbericht mit den Konten einer entsprechend detaillierten Gewinn- und Verlustrechnung durchführen. Bei der kostenlosen Überlassung von medizinischen Geräten für Forschungszwecke wird das jedoch oft nicht möglich sein. Mitarbeiter, die in Kooperationen mit Fachkreisangehörigen und medizinischen Einrichtungen involviert sind, müssen daher ausreichend geschult werden, um die notwendigen Informationen regelmäßig an die für den Transparenzbericht verantwortlichen Stellen weitergeben bzw. selbst im IT-Tool erfassen zu können.

Mehr Transparenz bietet die Chance einer **optimierten Auswahl** der Zuwendungsempfänger sowie der **Analyse und Bewertung der Zuwendungen** im Hinblick auf interne Vorgaben.

Lediglich bei Zuwendungen im Zusammenhang mit **Forschungs- und Entwicklungsleistungen** ist eine namentliche Offenlegung der Empfänger nicht vorgeschrieben.

Die Einhaltung der komplexen, international heterogenen Vorschriften erfordert einen **integrierten Compliance-Ansatz**.

Personalisierte Transparenzberichte

Im Transparenzbericht müssen grundsätzlich Name, Adresse und Arztnummer des Empfängers offengelegt werden. Lediglich bei Zuwendungen im Zusammenhang mit Forschungs- und Entwicklungsleistungen kann die Offenlegung aggregiert ohne Namensnennung erfolgen. Die Veröffentlichung personenbezogener Daten erfordert in Deutschland die vorherige schriftliche Einwilligung der Person. Für das Kontrollsystem bedeutet das: Es wird ein Musterformular zur Einholung der Zustimmung benötigt, oder die Verträge müssen um eine entsprechende Klausel ergänzt werden. Darüber hinaus muss auch hier eine Rücklaufkontrolle integriert sein und vor Veröffentlichung geprüft werden, ob von allen aufgelisteten Personen die Erklärung vorliegt.

Beachtung international verschiedener Vorgaben

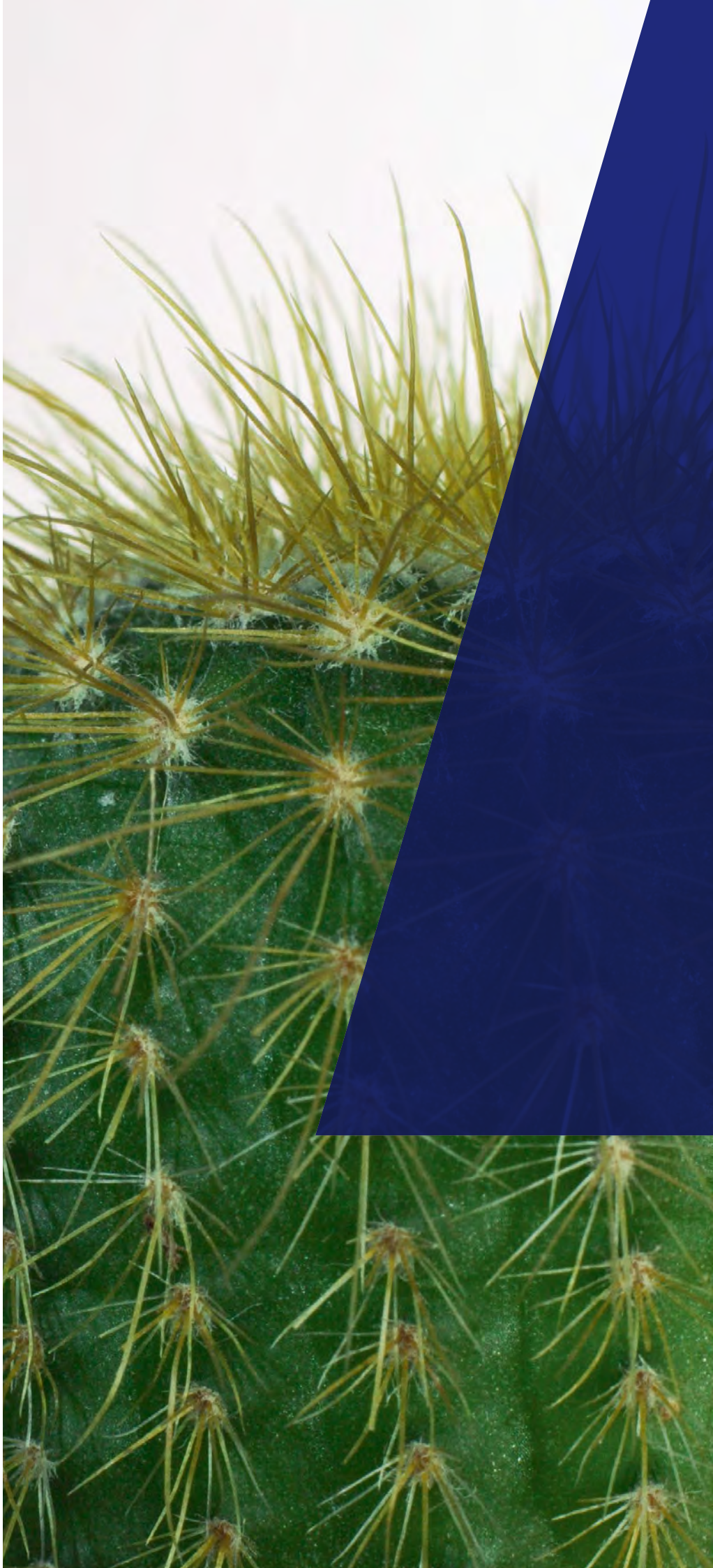
Bei Pharmaunternehmen, die weltweit tätig sind und mit unterschiedlichen Transparenzvorschriften konfrontiert werden, sollte eine IT-Lösung angestrebt werden, aus der die verschiedenen Berichte gemäß den lokalen Vorgaben soweit wie möglich generiert werden können. In diesem Zusammenhang muss sowohl zentral als auch dezentral ein Verantwortlicher bestimmt werden. Auf dezentraler Ebene gilt es dabei sicherzustellen, dass die Zentrale über alle Änderungen im Bereich der Transparenzregelungen informiert wird (durch regelmäßige Meldepflicht von Änderungen in Gesetzen und Transparenzkodizes), um System und Abläufe gegebenenfalls anpassen zu können. Außerdem sollte im Rahmen eines Vieraugenprinzips beispielsweise anhand einer Checkliste die Vollständigkeit der nach gültigem Recht notwendigen Informationen kontrolliert werden.

Integrierte Prüfung auf Compliance

Nach ihrer Einführung sollten Prozesse und Kontrollverfahren regelmäßig daraufhin überprüft werden, ob alle Vorgaben eingehalten werden und ob eventuell noch Lücken bestehen, die geschlossen werden müssen. Die Prüfung kann entweder intern – zum Beispiel durch die Interne Revision – oder extern durch einen unabhängigen Berater/Prüfer erfolgen. Hierdurch zeigt sich auch, ob der Prozess in der Praxis gelebt wird und eine effektive Risikoreduzierung bzw. -vermeidung stattfindet.

Ausgewählte Herausforderung	Maßnahmen
Identifizierung der Fachkreisangehörigen	• Abgleich mit bestehenden Debitoren-/Kreditorenlisten • Meldeprozess für Intermediäre • Konsolidierung der Informationen zu einer Liste der relevanten Empfänger • Sicherstellung der regelmäßigen Aktualisierung der Listen • Erstellung einer Richtlinie
Aufteilung der Leistungen in verschiedene Kategorien	• Einführung/Anpassung eines IT-Tools mit den entsprechenden Kategorien der Zuwendungen • Systemseitige Sicherstellung, dass bei Freigabe bzw. spätestens bei Zahlungsausgang eine entsprechende Kategorisierung erfolgen muss • Abgleich der Zuwendungen mit anderen im Unternehmen verfügbaren Informationen bezüglich der Vollständigkeit der Daten, zum Beispiel Rechnungswesen • Schulung der relevanten Mitarbeiter
Detaillierte Angaben zu den Empfängern	• Prozess zur Einholung der Einwilligungserklärungen etablieren • Erstellung eines Musterformulars und Rücklaufkontrolle
Veröffentlichung	• Vieraugenprinzip vor Freigabe • Prüfung der Angaben auf Plausibilität und Vollständigkeit der Informationen nach dem jeweiligen Recht (zum Beispiel Checkliste) • Überwachung regulatorischer Änderungen (Etablierung eines regelmäßigen Meldeverfahrens)

Dirk Krieger
Senior Manager,
Governance & Assurance Services, KPMG



Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Jens C. Laue
Partner, Head of
Governance & Assurance Services
T +49 211 475-7901
jlaue@kpmg.com

www.kpmg.de/assurance

Bildnachweis: © iStock.com/photokey (Titel); © iStock.com/shulz (S. 2, 7), © iStock.com/mrPliskin (S. 2, 20, 23, 25, 26), © iStock.com/thomasd007 (S. 2, 38, 39, 40); © iStock.com/kokouu (S. 4), © iStock.com/Ekkapon (S. 5); © iStock.com/humbak (S. 6); © iStock.com/rtiom (S. 7); © iStock.com/skodonnell (S. 8, 10); © babimu/fotolia.com (S. 9); © iStock.com/popovaphoto (S. 11, 12); © iStock.com/zoom-zoom (S. 11, 12, 13); © iStock.com/calvinng (S. 14); © iStock.com/UroshPetrovic (S. 15); © iStock.com/Shirinov (S. 16); © iStock.com/GlobalP (S. 16); © iStock.com/Horimono_F (S. 17); © iStock.com/only_fabrizio (S. 18); © iStock.com/Dimijana (S. 19); © iStock.com/studiocasper (S. 27, 28, 29); © contrastwerkstatt/fotolia.com (S. 30); © iStock.com/AnthonyRosenberg (S. 31); © iStock.com/Nastco (S. 33); © iStock.com/esseffe (S. 33); © iStock.com/EdnaM (S. 34); © iStock.com/mattjeacock (S. 35, 36); © iStock.com/Peshkova (S. 41); © iStock.com/Floortje (S. 42, 43, 44, 45, 46, 47)