GLOBAL PERSPECTIVES AND INSIGHTS

Interne Revision und Compliance: Klarheit und Zusammenarbeit für eine bessere Governance

The Institute of Internal Auditors | Global

Frühere Ausgaben

Frühere Ausgaben von Global Perspectives and Insights finden Sie unter www.theiia.org/GPI.

Leser-Feedback

Senden Sie Fragen oder Kommentare an globalperspectives@theiia.org.

Inhalt

Danksagung

Das IIA dankt den Mitgliedern und Interessengruppen, die zu diesem Papier beigetragen haben, darunter Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sorlie, Francis Nicholson, Jill Austin, und das IIA Australien.

Über das IIA

Das Institute of Internal Auditors (IIA) ist der anerkannteste Interessenvertreter, Ausbilder und Anbieter von Standards, Leitlinien und Zertifizierungen für den Berufsstand der Internen Revision. Das IIA wurde 1941 gegründet und hat heute 200.000 Mitglieder aus mehr als 170 Ländern und Gebieten. Der weltweite Hauptsitz des Verbandes befindet sich in Lake Mary, Florida, USA. Weitere Informationen finden Sie unter www.globaliia.org.

Haftungsausschluss

Die in Global Perspectives and Insights zum Ausdruck gebrachten Meinungen sind nicht notwendigerweise die der einzelnen Autoren oder der Arbeitgeber der Autoren.

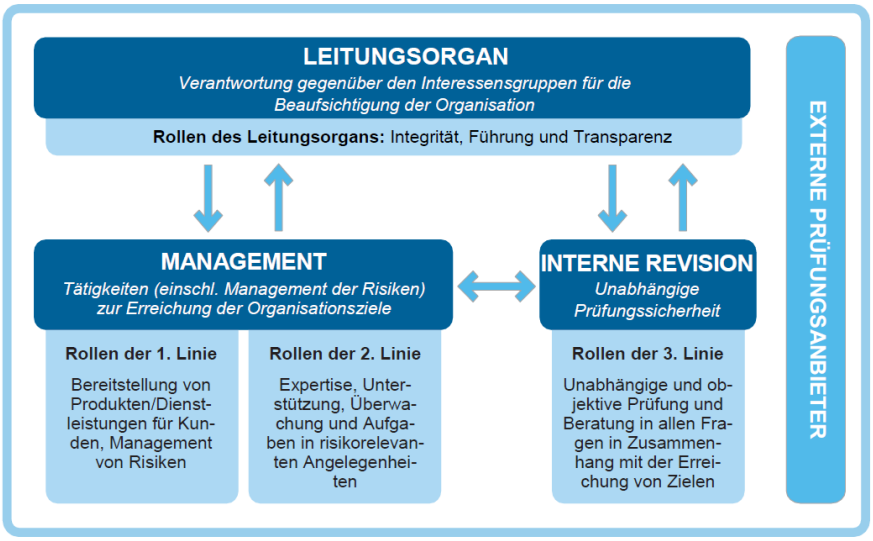
Urheberrecht

Einführung

Das Verhältnis zwischen Interner Revision und Compliance ist manchmal unklar und wirft wichtige Fragen auf: Kann die Interne Revision für Compliance verantwortlich sein? Ist eine Compliance-Funktion für die gesamte Einhaltung von Vorschriften in einer Organisation verantwortlich? Ist es in Ordnung, als Leiter der Internen Revision für Compliance zuständig zu sein?

Dieses Papier soll dazu beitragen, Klarheit in diese komplexen Zusammenhänge zu bringen und Verwirrung, Lücken und unnötige Doppelarbeit zu vermeiden. Ein klares Verständnis ist unerlässlich, zur Zusammenarbeit wird nachdrücklich aufgefordert und die Unabhängigkeit der Internen Revision ist von grundlegender Bedeutung.[1]

Dies ist *keine* Abhandlung darüber, wie man die Einhaltung von Vorschriften prüft. Vielmehr dient es als Hilfsmittel für Vorstände, Management, Compliance-Fachleute und Revisionsleitungen und verwendet das *Drei-Linien-Modell*, um die Beziehung zwischen Interner Revision und Compliance zu erklären. Die sechs Grundsätze des *Drei-Linien-Modells* und ihre Anwendung auf Compliance werden im Folgenden eingehend untersucht.



Die Leser sollten dieses Papier nutzen, um innerhalb einer Governance-Struktur – unabhängig von Rechtsprechung, Branche, Komplexität, Reifegrad oder Größe – wirksame Compliance- und Compliance-Risikomanagement in ihren verschiedenen Aspekten in Bezug auf das *Drei-Linien-Modell* klar zu erkennen, zu verstehen, zu bewerten und anzuwenden.[2] Praktische Darstellungen von Risiko- und Compliance-Beauftragten und Internen Revisoren zu Compliance-Problemen in der Praxis helfen bei der praktischen Anwendung der sechs Grundsätze des Modells, wenn es darum geht, die Ausrichtung der Compliance-Aktivitäten im Einklang mit dem *Drei-Linien-Modell zu* bewerten (s. Seiten 8-16.)

[1] Der integrale Charakter der Compliance als Teil der nachhaltigen Governance ist ein zentraler Schwerpunkt und eine politische Maßnahme, die B20 Italien den G20-Ministern im *B20 Italy Integrity & Compliance Policy Paper 2021* empfiehlt. Insbesondere die politische Maßnahme 2.1 auf S. 11 erwähnt ausdrücklich die Rolle der Internen Revision, wie sie im Drei-Linien-Modell beschrieben wird.

[2] In bestimmten Rechtsordnungen und Branchen sind die Rollen und Verantwortlichkeiten im Zusammenhang mit Compliance und Compliance-Risikomanagement genau definiert und Gegenstand umfangreicher Gesetze, Vorschriften, Rechtsprechung und wissenschaftlicher Untersuchungen. Detaillierte Studien sind verfügbar, und die Nutzer dieses Praxispapiers werden gebeten, dies zu konsultieren. Siehe zum Beispiel vom American Law Institute, *Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 und *Principles of the Law, Compliance and Enforcement* No. 2.

Rechenschaftspflicht, Tätigkeiten und Prüfungssicherheit

Das *Drei-Linien-Modell* beschreibt, wie die Rechenschaftspflicht des Leitungsorgans, die Tätigkeiten des Managements und die unabhängige Prüfung durch die Interne Revision die Grundlage für eine wirksame Governance bilden. Es zeigt auch, wie die sechs Grundsätze bei der Bewertung der jeweiligen Rollen und Verantwortlichkeiten in einer Organisation helfen. Die Anwendung der Kernelemente des Modells und der sechs Grundsätze ist für jede Organisation unterschiedlich, je nach ihren Zielen, Ressourcen und Umständen. Das Modell hilft Organisationen bei der Ermittlung von Strukturen, der Gestaltung von Prozessen und der Zuweisung von Verantwortlichkeiten, die das Erreichen der Ziele am besten unterstützen. Dazu gehört auch das Management des Compliance-Risikos, das in der Verantwortung des Managements liegt, aber nur durch gemeinsame Anstrengungen gelingt.[3]

Das Spektrum der Compliance-Anforderungen und -Erwartungen, die eine Organisation berücksichtigen muss, umfasst sowohl extern auferlegte Anforderungen, wie Gesetze, Regeln und Vorschriften, als auch intern auferlegte Anforderungen, wie Richtlinien, Standards, Verfahren und Verhaltenskodizes. Sie können formell und explizit definiert sein oder eher implizit, wie z. B. soziale, ethische und kulturelle Erwartungen. Dieses breite, dynamische Spektrum von Überlegungen wird in diesem Papier als „Anforderungen und Erwartungen“ bezeichnet.

Die Stakeholder erwarten von einer Organisation, dass sie ihren Zweck erfüllt und ihren Wert rechtlich und ethisch maximiert. Dementsprechend investieren Organisationen in die genaue Überwachung der Einhaltung von Vorschriften in Schlüsselbereichen wie Gesundheit und Sicherheit, Beschäftigung, Datensicherheit und Datenschutz, Gesetze und Kodizes für juristische Personen und Unternehmen, Branchenvorschriften, Qualitätsstandards, Bestechungs- und Korruptionsbekämpfung, Anleger- und Verbraucherschutz, Finanzberichterstattung und Besteuerung sowie individuelle Verhaltenskodizes. Die Liste lässt sich fortsetzen. Compliance kann im Kontext von Rechenschaftspflicht, Tätigkeiten und Prüfungssicherheit, wie im *Drei-Linien-Modell* beschrieben, als Teil eines Gesamtkonzepts für eine wirksame Governance verstanden und umgesetzt werden.

Was ist Compliance?

Organisationen müssen geltende Gesetze und andere externe Anforderungen einhalten, die eine Voraussetzung für die Ausübung ihrer Geschäftstätigkeit sind. Diese Compliance-Anforderungen reichen von den Beziehungen zu den Mitarbeitern bis hin zur Zahlung von Steuern. In bestimmten Branchen gibt es eine Reihe von regelsetzenden Behörden, Aufsichtsbehörden und Regulatoren sowie definierte Anforderungen, aber in anderen Sektoren gibt es weniger von außen auferlegte rechtliche und regulatorische Grenzen und Zwänge. Dennoch dürfte es schwierig sein, im öffentlichen oder privaten Sektor eine Organisation zu finden, die keine externen Compliance-Anforderungen hat.

Gleichzeitig entwerfen, entwickeln und implementieren Organisationen interne Erwartungen in Form von Richtlinien und Verfahren und setzen Standards für ethisches Verhalten. In bestimmten regulierten Branchen schreiben externe Anforderungen vor, dass ein Unternehmen bestimmte interne Richtlinien, Standards und Verhaltenskodizes aufstellen und einhalten muss. Mit diesem vielschichtigen Netz von Anforderungen nimmt das Konzept der „Compliance“ in einer Organisation eine Reihe von Dimensionen an. Dementsprechend ist es sinnvoll, den Begriff „Compliance“ in all seinen weit gefassten, verwandten, aber unterschiedlichen Aspekten

[3] Für die Zwecke dieses Papiers wird der Begriff „*Management“* im weitesten Sinne zur Bezeichnung von Aufgaben verwendet, die nicht in die Zuständigkeit des Leitungsorgans oder der Internen Revision fallen.

zu betrachten und zu untersuchen, wie er in Organisationen diskutiert wird: Als Ergebnis, als Risikokategorie,[4] als organisatorische Rolle, Abteilung oder Funktion usw. und als eine Reihe von Tätigkeiten.[5]

Jeder dieser Punkte wird im Folgenden erläutert.

Compliance als Ergebnis

Organisationen führen verschiedene Maßnahmen durch, um Gesetze, Vorschriften, Richtlinien, Kodizes usw. einzuhalten oder um „compliant" zu sein. Die Erfüllung bestimmter Compliance-Anforderungen und -Erwartungen ist oft eine notwendige Voraussetzung für die Ausübung der Geschäftstätigkeit und die Verfolgung strategischer Ziele.

Compliance als Risikokategorie

Das International Professional Practices Framework definiert Risiko als die *Möglichkeit, dass ein Ereignis eintritt, das sich auf das Erreichen der Ziele einer Organisation auswirkt*. Diese Auswirkungen können günstig oder ungünstig sein. Bei der Risikobewertung ist es daher wichtig, die Anforderungen und Erwartungen an die Einhaltung der Vorschriften zusammen mit der Wahrscheinlichkeit einer Nichteinhaltung und den möglichen Auswirkungen auf die Ziele zu berücksichtigen.

Es gibt Risiken für Organisationen, die sowohl mit der Einhaltung als auch mit der Nichteinhaltung von Vorschriften verbunden sind. Sie können sich in Form von Belohnungen oder Strafen auswirken, die materiell oder immateriell sein können. Die Einhaltung der Normen der Internationalen Organisation für Normung (ISO) z. B. soll betriebliche Effizienz und andere Vorteile bringen sowie die positive Aufmerksamkeit, die die Befolgung eines freiwilligen Kodex mit sich bringt. Die Nichteinhaltung macht diese positiven Vorteile zunichte und kann zu direktem Schaden sowie zu Strafen wie Geldbußen, Lizenzentzug, Sanktionen, Einstellung des Betriebs, zivil- oder strafrechtliche Verfolgung und Verlust von Finanzmitteln oder Unterstützung führen. Darüber hinaus kann die Nichteinhaltung von Vorschriften ein Reputationsrisiko in Form von potenzieller Unzufriedenheit der Interessengruppen, öffentlicher Kritik oder anderen Schäden verursachen.

Die Identifizierung, Messung und Beurteilung des Compliance-Risikos sowie die Festlegung der Risikobereitschaft und -toleranz helfen bei der Bestimmung angemessener Maßnahmen, einschließlich Richtlinien, Verfahren, Limite und Kontrollen.[6]

Compliance als Rolle oder organisatorische Abteilung

Häufig wird der Begriff „Compliance" auch verwendet, um eine Funktion oder Abteilung zu bezeichnen, die zur Erfüllung bestimmter Anforderungen und Erwartungen eingerichtet wurde, oder die Aufsicht, Fachwissen, Kontrolle und Überprüfung, Überwachung, Tests oder Prüfungssicherheit in Bezug auf Compliance-Angelegenheiten bietet. Diese sind charakteristisch für verschiedene Rollen in der ersten oder zweiten Linie, wie sie im *Drei-Linien-Modell* beschrieben werden. Sie bleiben im Rahmen des allgemeinen Zuständigkeitsbereichs und der Verantwortlichkeiten des Managements und bieten, je nach den spezifischen Merkmalen der Rolle, potenziell

[4] Unter der weit gefassten Kategorie des Compliance-Risikos in einer Organisation identifiziert eine Risikotaxonomie eine Kaskade von Unterkategorien, die sowohl spezifische Risiken als auch damit verbundene Risiken in Bezug auf Gesetze, Regeln, Vorschriften, Richtlinien oder Verhaltensweisen betreffen.

[5] Die Rollen können so definiert werden, dass sie spezifische Risiken abdecken, wie z. B. der Beauftragte für Verhaltensrisiken, der Beauftragte für Datenschutzrisiken usw.

[6] Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) bietet Rahmenwerke für das Risikomanagement und Denkanstöße, darunter neue Leitlinien zur Anwendung des ERM-Risikorahmens auf das Management von Compliance-Risiken.

fachliche Unterstützung und Risikomanagement für diejenigen mit Rollen in der ersten Reihe und für die Geschäftsleitung.

Je nach gesetzlichen und aufsichtsrechtlichen Anforderungen, Branche, Größe und Komplexität der Organisation kann eine leitende Funktion in der Compliance, abhängig von ihren spezifischen Aufgaben, an eine der verschiedenen Funktionen in der Organisation berichten. Dazu gehören die Geschäftsleitung (z. B. der Chief Executive Officer, der Chief Risk Officer, der Chief Operating Officer, der Chefsyndikus oder andere), ihre jeweiligen Managementketten und/oder direkt das Leitungsorgan oder ein bestimmter Unterausschuss. In bestimmten Fällen, wiederum vorbehaltlich der oben genannten Faktoren und eines Mechanismus zur Gewährleistung der Unabhängigkeit der Internen Revision, kann eine Compliance-Funktion oder -Abteilung der Revisionsleitung (CAE) oder einer Person unterstellt sein, die sowohl die Compliance-Abteilung als auch die Interne Revision beaufsichtigt. Es sollten die im *Drei-Linien-Modell* beschriebenen sechs Grundsätze angewandt werden, um zu prüfen, inwieweit die Zuständigkeiten der einzelnen Funktionen für Compliance mit den Anforderungen und Erwartungen übereinstimmen. Wie im Modell beschrieben, sollten Abhilfemaßnahmen getroffen werden, wenn die Zuständigkeiten einen potenziellen Interessenkonflikt oder eine Beeinträchtigung der Objektivität oder Unabhängigkeit darstellen. Der potenzielle oder tatsächliche Interessenkonflikt oder die Beeinträchtigung der Objektivität sollte auch dem Leitungsgremium berichtet werden, um mögliche Maßnahmen zu prüfen und ggf. den Regulator zu unterrichten.

Compliance als eine Reihe von Tätigkeiten

Compliance kann sich auf die Prozesse und Kontrollen beziehen, die dazu dienen, Compliance zu erzielen, zu unterstützen, zu überwachen, zu prüfen, zu testen, in Frage zu stellen oder zu bestätigen. Die Personen, die diese Maßnahmen durchführen, tragen dazu bei, dass die Organisation und ihre Mitglieder die Anforderungen und Erwartungen erfüllen.

Compliance in einer Organisation wird durch die Handlungen und Verhaltensweisen aller Mitarbeiter der Organisation erreicht, die ihrer Rolle und ihrer Seniorität entsprechen.

Die Verantwortung für Routineprozesse, -verfahren und -kontrollen, die dazu dienen, bestimmte Anforderungen und Erwartungen auf einem bestimmten Niveau und mit einem akzeptablen Grad an Sicherheit zu erfüllen, kann an verschiedenen Stellen innerhalb der Organisation angesiedelt und auch ausgelagert sein. Das *Drei-Linien-Modell* legt fest, dass ein Schlüsselelement bei der Beurteilung der Ausgestaltung darin besteht, die Entscheidungsbefugnisse im Zusammenhang mit Compliance-Aktivitäten zu ermitteln. (Siehe dazu die detaillierten Rollen und Tätigkeiten, die Compliance umfassen, im Anhang.)

Das Drei-Linien-Modell

Compliance

Das Leitungsorgan ist letztendlich für die Governance verantwortlich, die durch die Handlungen und das Verhalten des Organs durch das Management und die Interne Revision erreicht wird.[7]

Da jede Organisation die Zuständigkeiten für die Compliance-Aspekte nach ihren eigenen Gegebenheiten und vorbehaltlich vorgeschriebener externer Anforderungen zuweist, muss sie analysieren, inwieweit die spezifischen Rollen und Zuständigkeiten, die innerhalb der Organisation zugewiesen wurden, mit den sechs Grundsätzen des *Drei-Linien-Modells* übereinstimmen. Die Beurteilung kann zeigen, dass einige Zuständigkeiten zu den Aufgaben des Leitungsorgans, andere zu den Aufgaben des Managements, einschließlich Compliance und Risikomanagement, und wieder andere zu den Aufgaben der Internen Revision passen.

Zu den Aufgaben der ersten Linie gehören die Bereitstellung von Produkten und Dienstleistungen für Kunden und der erforderlichen Unterstützung, um dies in Übereinstimmung mit den Anforderungen und Erwartungen zu tun. Die Aufgaben der zweiten Linie umfassen die fachliche Aufsicht und Beratung, die Risikobeurteilung (insbesondere auf aggregierter oder Portfoliobasis) und die Durchführung von Risikomanagementaktivitäten (einschließlich Überwachung, Kontrolle und Test), wodurch die erste Linie glaubwürdig hinterfragt wird. Die Interne Revision als dritte Linie liefert unabhängige Prüfungssicherheit, einschließlich der Prüfungssicherheit, wie gut die zweite Linie die erste Linie glaubwürdig hinterfragt. Alle müssen durch eine angemessene Koordination, Kommunikation und Zusammenarbeit effektiv zusammenarbeiten, um sicherzustellen, dass ihre Tätigkeiten ohne unangemessene Überschneidungen, Doppelarbeiten oder Lücken sowie ohne Konflikte oder Unvereinbarkeiten aufeinander abgestimmt sind.

Die Grafik, die zur Darstellung des Modells verwendet wird, weist weder eine Compliance-Rolle oder -Abteilung noch andere spezifische Rollen, Abteilungen oder Verantwortlichkeiten in der zweiten Linie aus. Sie zeigt die Beziehungen zwischen den zentralen Rollen der Governance und nicht eine vorgeschriebene Organisationsstruktur.

Festlegung der Zuständigkeit für Compliance-Rollen und -Tätigkeiten

Verantwortlichkeit, Tätigkeiten und Prüfungssicherheit sind die wesentlichen Bestandteile der Governance. Die Einrichtung und Merkmale von Fachabteilungen für Risikomanagement, Compliance, Ethik, Nachhaltigkeit, Sicherheit, Datenschutz, Rechtsberatung, Finanzkontrolle usw. hängen von vielen Faktoren ab. Dazu gehören die Komplexität der Organisation, die Größe, die Branche, die Ressourcen, die Vorschriften, die Gesetzgebung, die Unternehmenskultur, die Risikotoleranz/-bereitschaft des Leitungsorgans und, was besonders wichtig ist, die Ziele und Zuständigkeiten der Funktionen innerhalb der jeweiligen Fachabteilung.

[7] Die Strukturen der Leitungsorgane variieren je nach Rechtsprechung, regulatorischen Anforderungen und der individuellen Gestaltung der Organisation. Wenn wir uns auf Leitungsorgane beziehen, schließen wir das breite Spektrum von Leitungsorganstrukturen ein, die in verschiedenen Rechtsordnungen, Branchen und im öffentlichen und privaten Sektor anzutreffen sind. Das Leitungsorgan kann folgende Aufgaben haben: Festlegung der Ausrichtung der Organisation, Definition von Vision, Auftrag, Werten und Risikobereitschaft, Entgegennahme von Berichten des Managements über geplante, tatsächliche und erwartete Ergebnisse sowie über Risiken und Risikomanagement.

Vorbehaltlich spezifischer gesetzlicher Vorgaben in bestimmten Branchen verfügen Organisationen möglicherweise nicht über eine eigene Compliance-Abteilung. Viele haben auch keine Mitarbeiter, deren Titel oder Stellenbeschreibung Compliance beinhaltet.

Aber auch Organisationen ohne eine bestimmte Compliance-Funktion oder -Abteilung können eine wirksame Governance haben und die Anforderungen und Erwartungen erfüllen, vorausgesetzt, dass sie Rollen und Verantwortlichkeiten zuweisen, die der Organisation angemessen sind, um die Einhaltung der geltenden Anforderungen und Erwartungen zu erreichen, und dass die einzelnen Personen ihre definierten Rollen einhalten.

Je größer, komplexer, ressourcenreicher oder stärker reguliert eine Organisation ist, desto eher kann sie sich dazu entschließen oder gezwungen sein, einzelnen Rollen und Abteilungen getrennte Zuständigkeiten und Ressourcen für verschiedene Aspekte der Compliance zuzuweisen.

Außerdem kann ein Mitarbeiter für mehr als eine Rolle verantwortlich sein. In diesem Fall sollte eine angemessene Beurteilung der Vereinbarkeit dieser Mehrfachrollen vorgenommen werden, und es sollte eine klare Definition der Zuständigkeiten jeder Rolle sowie der Beaufsichtigung und der Prüfungssicherheit bezüglich dieser Rollen erfolgen. In bestimmten Fällen kann eine Genehmigung durch das Leitungsorgan oder die Aufsichtsbehörde erforderlich sein.

Im Falle von Mehrfachfunktionen besteht möglicherweise ein erhöhtes Risiko der Unvereinbarkeit, des Interessenkonflikts und der verminderten Klarheit über Rechenschaftspflicht und Verantwortung. Mitigierende Maßnahmen können erforderlich sein, um innerhalb der Risikobereitschaft zu bleiben, ggf. zusammen mit der Berichterstattung an das Leitungsorgan oder eine Aufsichtsbehörde.

Gemeinsame Anstrengung zur Erreichung von Compliance

Selbst wenn es eine bestimmte Compliance-Funktion oder -Abteilung gibt, ist es wichtig zu erkennen, dass nicht alle Compliance-Aktivitäten nur an einer Stelle innerhalb der Struktur eines Unternehmens angesiedelt sind. Mitarbeiter auf allen Ebenen sowie die Geschäftsleitung und Aufsichtsorgane müssen zu den kollektiven Compliance-Bemühungen beitragen. Verantwortung und Rechenschaftspflicht sind über die gesamte Hierarchie, die definierten Rollen und die Weisungsstrukturen einer Organisation verteilt, um Compliance zu erreichen, Compliance-Risiken zu mindern und die Einhaltung von Anforderungen und Erwartungen zu überwachen.

Die Einhaltung externer und interner Anforderungen und Erwartungen wird häufig von Fachabteilungen oder Einzelpersonen außerhalb einer ausgewiesenen Compliance-Abteilung wahrgenommen. Ihre jeweiligen Aufgaben und Zuständigkeiten können durch branchenspezifische Vorschriften oder durch eine bestimmte Person oder eine Reihe von Anforderungen oder Erwartungen enger definiert sein. Beispiele hierfür sind: die Einhaltung von Gesetzen und Vorschriften im Bereich des Personals, die von der Personalabteilung wahrgenommen wird, und die Einhaltung von Finanzberichterstattungs- und Steueranforderungen, die von der Finanzabteilung wahrgenommen wird.

Wie oben angedeutet, können verschiedene Rollen und Abteilungen für die Erreichung von Compliance sowie für die Beaufsichtigung, Überwachung und Kontrolle von Compliance-Aspekten verantwortlich sein. Daher ist es wichtig, die sechs Grundsätze anzuwenden, um die mit Compliance zusammenhängenden Merkmale einer einzelnen Funktion und ihrer Zuständigkeiten zu ermitteln.

Eine wirksame Governance profitiert sowohl von informeller als auch von formeller Kommunikation, Koordination und Zusammenarbeit und fördert die Transparenz. Wenn jedoch informelle Interaktionen in den Governance- und Kontrollstrukturen die angemessene Identifikation, Eskalation und Mitigierung von Compliance-Problemen umgehen, kann dies die Wirksamkeit der formellen Governance- und Kontrollstrukturen untergraben und die Festlegung von Rechenschaftspflicht und Verantwortung verwischen.

Bei der Beurteilung der Wirksamkeit eines Governance-Modells ist es wichtig, nicht nur die formelle Governance-Struktur zu bewerten, die zur Erreichung von Compliance entwickelt wurde, sondern die Organisation auch auf informelle Kommunikations-, Entscheidungs- und Handlungswege zu untersuchen, um festzustellen, ob, wo und wann die informelle Governance-Struktur die formelle untergräbt oder behindert. Starke formelle und informelle Interaktionen zur Stärkung von Kommunikation, Koordination und Zusammenarbeit werden durch das Drei-Linien-Modell gefördert. Eine informelle Governance-Struktur kann jedoch die Compliance blockieren, Kontrollen umgehen und zu einem ineffektiven Risikomanagement führen sowie die Klarheit der Verantwortlichkeiten und der Rechenschaftspflicht verschleiern. Die Anwendung des *Drei-Linien-Modells* zur Identifikation von Rollen, Verantwortlichkeiten und Tätigkeiten ermöglicht es Organisationen, einen effektiven Governance-Rahmen zu entwerfen, einschließlich der Entwicklung von Schutzvorkehrungen, um die Risiken informeller Governance, Entscheidungsfindung und Aktivitäten zu mindern, die zu Compliance-Versäumnissen führen können.

Ein wirksames Compliance-Programm fördert nicht nur die Einführung und Einhaltung einer formalen, dokumentierten Governance- und Kontrollstruktur, sondern ist auch ein Schlüsselelement für die Entwicklung und Aufrechterhaltung einer Compliance- und Kontrollkultur, die die Wirksamkeit des *Drei-Linien-Modells* fördert.

Anwendung der sechs Grundsätze

Das Drei-Linien-Modell fördert einen prinzipienbasierten Ansatz zur Beurteilung und Abstimmung von Rollen und Zuständigkeiten unter Berücksichtigung der Gegebenheiten einer Organisation, einschließlich ihrer spezifischen Compliance-Anforderungen und Erwartungen. Die sechs Grundsätze des Modells können verwendet werden, um Compliance – als Ergebnis, als Risikokategorie, als Rolle oder Abteilung oder als eine Reihe von Tätigkeiten – und ihren Beitrag zu einem erfolgreichen Governance-Rahmen besser zu verstehen. (Den vollständigen Wortlaut der sechs Grundsätze finden Sie im *Drei-Linien-Modell*).

Grundsatz 1: Festlegung von Governance-Anforderungen

Grundsatz 1 beschreibt die Mindestanforderungen, die an die Governance zu stellen sind:

- Verantwortung (des Leitungsorgans gegenüber den Interessengruppen für den Erfolg).
- Tätigkeiten und Einsatz von Ressourcen (durch das Management zur Erreichung der Ziele – einschließlich Risikomanagement und Einhaltung der Vorschriften).
- Prüfungssicherheit und Beratung (durch eine unabhängige Interne Revision zu allen Aspekten, um eine wirksame Beaufsichtigung und Transparenz zu ermöglichen und Vertrauen und kontinuierliche Verbesserung zu fördern).

Das Leitungsorgan ist letztlich dafür verantwortlich, dass die Organisation sich im Einklang mit anerkannten Standards und gesellschaftlichen Normen verhält. Das Management muss die mit der Einhaltung und Nichteinhaltung von Vorschriften verbundenen Risiken entsprechend der vom Leitungsorgan geäußerten Bereitschaft steuern. Dazu kann es gehören, dass einzelne Funktionen und Teams gebildet werden, die sich speziell mit Aspekten der Compliance befassen, und dass die Entscheidungsbefugnisse zwischen der ersten Linie, die für die Risiken verantwortlich ist, und der zweiten Linie, die die Einhaltung der Risikobereitschaft glaubwürdig hinterfragt und die erste Linie zur Einhaltung anhält, klar definiert werden. Die Interne Revision gibt gegenüber Management und Leitungsorgan Prüfungssicherheit über die Angemessenheit und Wirksamkeit der Kontrollen für Compliance und berät sie im Hinblick auf kontinuierliche Verbesserungen und Innovationen.

Darstellungen aus der Praxis

> **Das Gesundheitswesen ist eine stark regulierte Branche, in der die Erbringung fast jeder Dienstleistung die Einhaltung bestimmter Regeln, Vorschriften oder Normen erfordert. Krankenschwestern, Ärzte und anderes Personal müssen sicherstellen, dass jede erbrachte Leistung ordnungsgemäß genehmigt und dokumentiert wird. Diejenigen, die für die Einhaltung der Vorschriften verantwortlich sind (einzelne Rollen oder eine Abteilung), können die klinischen Abteilungen hinsichtlich der Dokumentations- und Genehmigungsanforderungen für ein bestimmtes Verfahren beraten, aber letztlich sind die Mitarbeiter in der ersten Linie für die Umsetzung der Prozesse und Kontrollen sowie die Einhaltung dieser Anforderungen verantwortlich.**
>
> - Leiter Compliance und Interne Revision, USA

Ein Beispiel aus meiner Branche ist die Einstufung der wichtigsten Compliance-Risiken für das Unternehmen und die gesetzlichen Anforderungen sowie die Ausrichtung von Aktivitäten, Kontrollen, Überwachung und Verantwortlichkeiten auf die Einhaltung der gesetzlichen Anforderungen und im Verhältnis zu diesen Risiken. So kann eine Organisation beispielsweise in Übereinstimmung mit den gesetzlichen Vorschriften einen Beauftragten für die Einhaltung der Geldwäschevorschriften, einen Beauftragten für den Datenschutz, einen Beauftragten für die Bekämpfung von Bestechung und Korruption usw. haben und Zuständigkeiten für die Bereiche Produkte, Offenlegung, Beschäftigung, Beschwerden usw. definieren sowie über bestimmte Ressourcen verfügen, um die Erzielung von Compliance und das Management dieser Hauptrisikobereiche zu unterstützen. Dem Leitungsorgan wird regelmäßig Bericht erstattet, und alle Aktivitäten unterliegen einer unabhängigen Internen Revision.

- Chief Compliance Officer, United Kingdom

Ein gutes Beispiel für die Herausforderungen, mit denen Organisationen heute konfrontiert sind, ist das Bestreben, „Umwelt-, Sozial- und Governance"-Standards (ESG) einzuführen und zu berücksichtigen. Das Leitungsorgan ist dafür verantwortlich, das Management dafür verantwortlich zu machen, dass sich die Organisation im Einklang mit der Strategie, den Standards und den gesellschaftlichen Normen verhält, die das Leitungsorgan festgelegt hat. Daher muss das Leitungsorgan sicherstellen, dass das Management die für das Unternehmen geltenden ESG-Risiken, die externen Gesetze und Vorschriften sowie die internen Richtlinien und Verfahren, die relevanten Leistungskennzahlen und verlässliche, authentische und vergleichbare Daten zum Nachweis der Einhaltung dieser internen Anforderungen und Erwartungen klar darlegt. Darüber hinaus wollen oder müssen sich sowohl das Management als auch das Leitungsorgan vergewissern, dass die ESG-Compliance-Ziele erreicht werden. Eine komplexe Zuordnung von Zuständigkeiten und Verantwortlichkeiten innerhalb der Organisation ist erforderlich, um die jeweiligen Rollen und Abteilungen und deren Aktivitäten zu erfassen, die für die Umsetzung von ESG und den Nachweis der Einhaltung erforderlich sind.

- Chief Compliance Officer, USA

Grundsatz 2: Angemessene Beaufsichtigung der Governance

In Grundsatz 2 werden die Aufgaben des Leitungsorgans definiert:

- Governance.
- Beaufsichtigung des Managements.
- Einrichtung und Beaufsichtigung einer wirksamen Internen Revision.

Das Leitungsorgan ist letztlich für die Governance verantwortlich und stellt sicher, dass geeignete Strukturen und Prozesse vorhanden sind. Dazu gehören Vorkehrungen für die Einhaltung von Vorschriften sowie die Überwachung der Rolle der Internen Revision.

Das Leitungsorgan muss den Grad des Vertrauens bestimmen, den es in Bezug auf die Einhaltung von Anforderungen und Erwartungen in Bezug auf die Höhe des Risikos und die potenziellen Auswirkungen auf die strategischen Ziele hat und benötigt. Bei der Festlegung seiner Compliance-Risikobereitschaft oder -toleranz überwacht das Leitungsorgan die Durchführung der Tätigkeiten des Managements und die Erfüllung der jeweiligen Verantwortlichkeiten der benannten Rollen und Abteilungen, um Compliance-Ergebnisse im Einklang mit der Compliance-Risikobereitschaft und den entsprechenden Toleranzen zu erzielen.

Das Leitungsorgan sollte sicherstellen, dass die Interne Revision angemessen positioniert und ausgestattet ist, um unabhängige und wirksame Prüfungen und Beratungen zur Compliance zu bieten. Der CAE muss dem Leitungsorgan, einem unabhängigen Prüfungsausschuss oder einem gleichwertigen benannten Ausschuss des Leitungsorgans gegenüber rechenschaftspflichtig sein, um seine Autorität und den unabhängigen Status sicherzustellen.

Darstellungen aus der Praxis

Ein effektives Leitungsorgan ist in der Lage, Veränderungen zu bewirken und sich in der gesamten Organisation Gehör zu verschaffen. Manchmal sind Eskalationen und Berichterstattung eine Selbstverständlichkeit, aber es hängt davon ab, wie aktuell das Leitungsorgan ist und wie gut die Informationen sind, um eine wirksame Aufsicht und Lenkung im „Jetzt" und nicht rückwirkend auf der Grundlage historischer Daten zu gewährleisten. Die Interne Revision sollte überprüfen, ob das Leitungsorgan einen klaren Überblick über die zu steuernden Risiken erhält, um diese Risiken vorhersehen, überwachen und steuern zu können. Die Compliance-Abteilung spielt eine wichtige Rolle in der zweiten Linie, indem sie das Management auf Compliance und die Wirksamkeit von Kontrollen hinweist und dem Leitungsorgan Einblicke in die Wirksamkeit des Compliance-Risikomanagements im Rahmen der Risikobereitschaft gewährt.

- Compliance-Beauftragter, Singapur

Im Gesundheitswesen und in vielen anderen Sektoren kann eine Compliance-Abteilung die tägliche Verantwortung für bestimmte Elemente des Compliance-Programms tragen, wie z. B. Schulung und Ausbildung, Überwachung von Hotlines, Bekanntgabe eines Ethikkodex, Durchführung von Hintergrundprüfungen usw. Bei einigen dieser Tätigkeiten geht es um die Einhaltung von Regelungen, bei anderen um die Festlegung von Richtlinien, die Überwachung oder die Berichterstattung über die Wirksamkeit der Compliance an die Geschäftsleitung oder das Leitungsorgan. Die Interne Revision kann keine unabhängige Prüfungssicherheit über die Wirksamkeit des Compliance-Programms geben, wenn die Compliance-Abteilung dem CAE unterstellt ist. In solchen Fällen kann jedoch ein unabhängiger Dritter damit beauftragt werden, dem Leitungsgremium Prüfungssicherheit zu bieten.

- Leiter Compliance und Interne Revision, USA

Das Leitungsgremium sollte sicherstellen, dass die Compliance-Risiken im Prüfungsplan der Internen Revision sorgfältig beurteilt/berücksichtigt werden, dass die Interne Revision die wichtigsten regulatorischen Risiken und Schwerpunktbereiche der Aufsichtsbehörden über mehrere Jahre hinweg abdeckt und dass die Ergebnisse der Compliance-bezogenen Berichte/Tätigkeiten überprüft werden.

- Chief Audit Executive, United Kingdom

Das Leitungsorgan gibt sowohl dem Management als auch der Internen Revision die Richtung für das Compliance-Risikomanagement vor. Damit das Leitungsorgan die Compliance wirksam beaufsichtigen kann, müssen angemessene quantitative und qualitative Informationen über den Status der Compliance, die sowohl vom Management als auch von der Internen Revision bereitgestellt werden, regelmäßig und häufig überprüft werden. Das Leitungsorgan sollte als ständigen Tagesordnungspunkt das Spektrum der Compliance-Risikomanagement-Aktivitäten behandeln, um ein zukunftsorientiertes Compliance-Risikomanagement und nicht nur eine rückwärtsgerichtete, ereignisorientierte Konzentration auf Regelverletzungen, Verstöße und Abhilfemaßnahmen zu ermöglichen.

- Chief Compliance Officer, United Kingdom

Grundsatz 3: Festlegung von Managementrollen in der ersten und zweiten Linie

Grundsatz 3 beschreibt die Rollen des Managements (sowohl in der ersten als auch in der zweiten Linie, die je nach Ressourcen, Zielen, Vorschriften usw. vermischt oder getrennt sein können).

Die Rollen der ersten und zweiten Linie bilden das Management. Sie spiegeln die Verantwortung der ersten Linie für die Bereitstellung von Produkten und Dienstleistungen für die Kunden wider. Die zweite Linie ist für die fachliche Beaufsichtigung, die Risikobeurteilung (insbesondere auf aggregierter oder Portfoliobasis) und die Durchführung von Risikomanagementaktivitäten zuständig und hinterfragt die erste Linie glaubwürdig.

Es können separate Abteilungen, wie z. B. eine Compliance-Abteilung, eingerichtet werden, oder es kann ein Abteilungsleiter oder – in kleineren und weniger komplexen Organisationen – eine Einzelperson ernannt werden, die dem Leitungsorgan entweder direkt oder über einen Ausschuss des Leitungsorgans Bericht erstattet. Der Abteilungsleiter oder die Einzelperson kann auch gemeinsam mit dem CEO oder einem Beauftragten innerhalb des Managements Bericht erstatten. Diese Berichtslinie oder Rechenschaftspflicht gegenüber dem Leitungsorgan mag den Anschein erwecken, dass der Leiter der Compliance-Abteilung oder die Person eine größere Unabhängigkeit genießt. Jedoch ist ein wichtiger Aspekt der Unabhängigkeit das Fehlen von Entscheidungsbefugnissen. In der Regel behält eine Person in einer Compliance-Funktion ein gewisses Maß an Managementverantwortung, von der Kundenakzeptanz über die Gewährung von Ausnahmeregelungen bis hin zur Genehmigung neuer Produkte usw. Dementsprechend schafft eine Berichtslinie an ein Leitungsorgan oder einen Ausschuss des Leitungsorgans für eine solche Abteilung, einen Abteilungsleiter oder eine Einzelperson keine echte Unabhängigkeit. Die Interne Revision und der CAE sind nicht nur hinsichtlich ihrer Berichtslinien vom Management unabhängig, sondern haben auch keine operative Entscheidungsbefugnis, was ein zusätzliches Maß an Unabhängigkeit bedeutet.

Dementsprechend können die Merkmale der Rollen über die Linien hinweg wie folgt formuliert werden:

- Rollen der ersten Linie: Einhaltung von Gesetzen, Vorschriften, Verhaltenskodizes, Unternehmensrichtlinien usw. bei der Bereitstellung von Produkten und Dienstleistungen. Compliance bleibt die Verantwortung des Managements.
- Rollen der zweiten Linie: Einzelne Compliance-Funktionen und -Abteilungen legen Rahmenbedingungen fest, beaufsichtigen, bieten Beratung, Überwachung und Kontrolle, führen Tests durch, hinterfragen das Management und verfügen im Allgemeinen über operative Entscheidungsbefugnisse des Managements, können selbst Risiken eingehen (z. B. Akzeptanz von Kunden oder Klienten, Genehmigung neuer Produkte oder Dienstleistungen, Genehmigung von Transaktionen, Genehmigung von Limitüberschreitungen, Ausnahmen von Richtlinien usw.).
- Rollen der dritten Linie: Die Interne Revision bietet unabhängige Prüfungssicherheit in Bezug auf Compliance, die Wirksamkeit der Bemühungen des Managements zur Erreichung von Compliance und die Arbeit der Compliance-Funktion oder -Abteilung zur Überwachung und Lieferung von Compliance-Risikomanagement Beaufsichtigung und Kontrolle, aber nicht umgekehrt. Die Interne Revision hat keine Entscheidungsbefugnisse und berichtet unabhängig an das Leitungsorgan.

Mit Hilfe des *Drei-Linien-Modells* kann eine Organisation die Einhaltung von Anforderungen und Erwartungen erreichen, zu einer wirksamen und nachhaltigen Governance beitragen und illegale Handlungen und Korruption bekämpfen. Compliance muss auf Transparenz beruhen und einen angemessenen Standard innerhalb der Organisation setzen. Darüber hinaus schafft ein wirksames Compliance-Programm, das die Transparenz fördert, auch bei externen Stakeholdern wie Aktionären, staatlichen Stellen, Aufsichtsbehörden, Börsen, Lieferanten und der Lieferkette Vertrauen in eine Organisation.

Darstellungen aus der Praxis

Die erste und die zweite Linie sollten effektiv zusammenarbeiten, um die Compliance-Risiken des Unternehmens zu ermitteln, zu steuern und zu überwachen. Man sollte sich nicht auf die Interne Revision verlassen, um Dinge zu überwachen, zu testen und zu finden. Dies sollte in der Verantwortung der ersten und zweiten Reihe liegen.

- Chief Administrative Officer, USA

Eine Compliance-Funktion sollte das Unternehmen unterstützen und dafür sorgen, dass die Prozesse und Kontrollen klar aufeinander abgestimmt sind. Es gibt verschiedene Fälle, in denen eine Compliance-Funktion als zweite Linie den Geschäftsbereichen beratend zur Seite steht. Leistungs- und Risikoindikatoren helfen den Geschäftsbereichen, Risiken für die Wirksamkeit der Kontrollen zu ermitteln und zu steuern.

- Chief Compliance Officer, Mexiko

Viele Branchen unterliegen einer Unzahl komplexer Vorschriften. Die Compliance-Abteilung bietet ihr Fachwissen und ihre Beratung in Bezug auf die gesetzlichen Anforderungen oder die jüngsten gesetzlichen Änderungen innerhalb einer bestimmten Abteilung an. Im Gesundheitswesen zum Beispiel ist das Management der verschiedenen klinischen Abteilungen für die Gestaltung und Umsetzung der Kontrollen verantwortlich, die zur Einhaltung der Vorschriften erforderlich sind. Aufgrund ihres Fachwissens ist die Compliance-Abteilung in der idealen Position, um die Einhaltung dieser Anforderungen zu beurteilen.

- Chief Compliance Officer, USA

Eine zentrale Herausforderung, die jedoch in größeren Unternehmen gut umgesetzt wird, ist die Verantwortung für Compliance und die Art und Weise, wie diese von den Mitarbeitern in Compliance-Funktionen oder Compliance-Abteilungen umgesetzt wird. Dies erfordert einen sehr klaren Risikomanagement- und Kontrollrahmen mit klaren Verantwortlichkeiten, Rollen und Zuständigkeiten und wirksamen Eskalationswegen durch eine solide Governance. Ohne diesen Rahmen ist die Compliance-Überwachung unklar und schwer umzusetzen.

- Chief Compliance Officer, United Kingdom

Compliance liegt in der Verantwortung eines jeden. In stark regulierten Branchen wie dem Gesundheitswesen umfasst diese Verantwortung jeden Mitarbeiter und kann die Einhaltung der Genehmigungs- und Dokumentationsanforderungen für ein bestimmtes Verfahren umfassen. Wenn die Compliance-Abteilung die Richtlinien, Prozesse und Kontrollen für bestimmte Verfahren entwickelt oder die routinemäßige Verantwortung für das Verfahren trägt, kann sie keine objektive Prüfungssicherheit liefern. Die Beratung und Konsultation zu den mit einem Prozess oder Verfahren verbundenen rechtlichen Anforderungen würde die Objektivität der Compliance-Abteilung jedoch nicht unbedingt beeinträchtigen.

- Leiter Compliance und Interne Revision, USA

Grundsatz 4: Definition der Rolle der dritten Linie

Grundsatz 4 beschreibt die Rolle der Internen Revision als Anbieter unabhängiger Prüfungssicherheit und Beratung.

Das *Drei-Linien-Modell* unterstreicht die kritische Notwendigkeit der Prüfungssicherheit über die Angemessenheit und Wirksamkeit der Risikoreaktionen, einschließlich der Kontrollen, als grundlegende Komponente der Governance. Zu den Risikoreaktionen und -kontrollen gehören die Maßnahmen zur Erreichung, Überwachung und Beaufsichtigung der Compliance und des Compliance-Risikomanagements. Dies wird erreicht durch die kompetente Anwendung von systematischen und zielgerichteten Prozessen, Fachkenntnissen und Einblicken durch die Interne Revision als einziger vom Management unabhängiger Anbieter von Prüfungssicherheit.

Eine wirksame Koordination und Zusammenarbeit zwischen den Funktionen der Compliance und der Internen Revision kann zum Nutzen einer Organisation erreicht werden, ohne die Wirksamkeit der einzelnen Funktionen zu beeinträchtigen.

Aufgrund der verschiedenen Rollen und Verantwortlichkeiten in einer Organisation kann es andere Quellen von Prüfungssicherheit geben, die in ihrer Gesamtheit eine umfassende, zusammengesetzte Perspektive auf eine Organisation bieten können. Es ist jedoch wichtig, spezifische Rollen und ihre Ausrichtung nach dem *Drei-Linien-Modell* zu analysieren und zu bewerten, um die Qualität und Objektivität einer solchen Prüfungssicherheit zu beurteilen.

Die Interne Revision ist gegenüber dem Leitungsorgan rechenschaftspflichtig und von den Verantwortlichkeiten des Managements unabhängig. Dies ist entscheidend für das Verständnis der Prüfungsrolle und der besonderen Stellung der Internen Revision innerhalb der Governance. Wenn die Unabhängigkeit der Internen Revision und die Objektivität der Internen Revisoren gefährdet sind, muss der CAE dies dem Leitungsorgan berichten, damit Korrekturmaßnahmen ergriffen werden können.

Interne Revisoren sollten bei der Beurteilung der Wirksamkeit von Compliance-Rollen und -Abteilungen offen für Kommunikation, Koordination und Zusammenarbeit sein, um eine effektive Anwendung des *Drei-Linien-Modells* zu erreichen und eine Kultur der Compliance und Kontrolle zu fördern.

Darstellungen aus der Praxis

> **Bei der Beurteilung des Managements von Compliance-Risiken ist vor allem auf die Wirksamkeit der durchgeführten Maßnahmen zur Eindämmung von Problemen zu achten. Eine solide Risikobeurteilung spezifischer Compliance-Risiken und die Ausrichtung der Aktivitäten auf diese Risiken sind wichtig. Andernfalls könnten viele Tätigkeiten durchgeführt werden, ohne dass die Organisation vor den Risiken der Nichteinhaltung von Regelungen geschützt wird.**
>
> - Chief Audit Executive, Südafrika

> **Eine besondere Herausforderung für Interne Revisoren ist die Einbeziehung der ausdrücklichen Identifikation von Verstößen in ihre Prüfungstätigkeit und Berichterstattung: Verletzungen von Gesetzen und Vorschriften, Verstöße gegen Richtlinien, Standards und Verhaltenskodizes. Um dies zu gewährleisten, müssen qualifizierte Ressourcen zur Verfügung stehen, die eine wirksame Beurteilung und Berichterstattung über das Erreichen des gewünschten Compliance-Ergebnisses ermöglichen.**
>
> - Chief Audit Executive, United Kingdom

Grundsatz 5: Wahrung der Unabhängigkeit der dritten Linie

Grundsatz 5 beschreibt die Bedeutung der Unabhängigkeit der Internen Revision.

Die Interne Revision als dritte Linie weist mehrere Merkmale auf, die ihre Unabhängigkeit ausmachen. Dazu gehören eine unabhängige funktionale Berichterstattung an das Leitungsorgan oder einen Ausschuss des Leitungsorgans und, was besonders wichtig ist, die Unabhängigkeit von der Entscheidungsfindung des Managements.

Risikomanagementfunktionen (einschließlich Funktionen für das Compliance-Risikomanagement) haben zwar häufig eine funktionale Berichtslinie zum Leitungsorgan oder zu einem Ausschuss des Leitungsorgans, sind aber in der Regel in ihrer jeweiligen Funktion auch für Managemententscheidungen zuständig, insbesondere im Hinblick auf die Übernahme, Steuerung, Minderung, Kontrolle und Berichterstattung von Risiken, einschließlich des Compliance-Risikos.

Die zweite Linie kann ihre Verantwortung für ein wirksames und glaubwürdiges Hinterfragen der ersten Linie beibehalten. Jedoch ist die Unabhängigkeit der Internen Revision von der Entscheidungsfindung des Managements ein wesentliches Unterscheidungsmerkmal zwischen der Rolle der dritten Linie und den Rollen der zweiten und ersten Linie, wie oben in Grundsatz 3 ausgeführt.

Darstellungen aus der Praxis

> **Damit die Interne Revision nicht in einen Interessenkonflikt gerät, dürfen Interne Revisoren keine Kontrollen entworfen oder durchgeführt haben oder an der Entscheidungsfindung des Managements beteiligt gewesen sein. Ihr Schwerpunkt liegt auf der Beobachtung, dem Testen und der Beurteilung, um festzustellen, ob Schlüsselrisiken wie beabsichtigt ermittelt und kontrolliert werden. Sie dürfen nicht voreingenommen sein und keine vorgefassten Erwartungen haben.**
>
> - Chief Audit Executive, Australien

> **Der wichtigste Stakeholder der Internen Revision ist das Leitungsorgan, und die organisatorische Unabhängigkeit der Internen Revision ermöglicht es ihr, ungefiltert über Ergebnisse und Empfehlungen zu berichten. Es besteht nicht die Erwartung oder Notwendigkeit sicherzustellen, dass die Kontrollmechanismen und diejenigen, die sie durchführen, in einem positiven Licht dargestellt werden. Die Interne Revision hat letztlich dafür die Verantwortung, die Wahrheit zu berichten.**
>
> - Chief Audit and Compliance Officer, USA

> **Die Aufgaben der zweiten Linie der Compliance-Abteilung umfassen die Festlegung von Richtlinien, die Beratung der Geschäftseinheiten hinsichtlich der Gestaltung von Kontrollen, die Beratung und Überprüfung der Risikobereitschaft der Geschäftseinheiten und die Lieferung von Prüfungssicherheit. Compliance-Mitarbeiter oder -Abteilungen können mit der Ausführung operativer Aufgaben im Auftrag der ersten Linie betraut werden. In solchen Fällen ist die Compliance-Person oder -Abteilung nicht völlig unabhängig von der ersten Linie. Die Interne Revision ist die einzige völlig unabhängige Tätigkeit, da sie von der Entscheidungsfindung des Managements in der ersten und zweiten Linie unabhängig ist.**
>
> - Leiter der Abteilung Unternehmensrisiko und Interne Revision, USA

Grundsatz 6: Durch Zusammenarbeit Werte schaffen und schützen

Grundsatz 6 beschreibt, wie wichtig es ist, die Koordination und Zusammenarbeit zwischen allen Rollen zu gewährleisten.

Eine wirksame Governance erfordert nicht nur eine angemessene Zuweisung von Verantwortung, sondern auch eine enge Abstimmung der Aktivitäten durch Koordination, Zusammenarbeit und Kommunikation. Das Leitungsorgan stützt sich auf die Berichte des Managements, der Internen Revision und anderer, um die Aufsicht auszuüben und dem Management die Richtung vorzugeben, damit es seine Ziele erreicht, Risiken steuert und Werte schafft. Die Aufgaben des Leitungsorgans sowie die Aufgaben der ersten, zweiten und dritten Linie tragen gemeinsam zur Wertschöpfung und zum Schutz von Werten bei, wenn sie aufeinander und auf die vorrangigen Interessen der Stakeholder abgestimmt sind. Dementsprechend tragen eine klare Kommunikation der Compliance-Verantwortlichkeiten im gesamten Unternehmen, der Entscheidungsrechte, Berichtspflichten, Risikobereitschaft, gemeinsamen Taxonomien, klar definierten Beurteilungseinheiten, Leistungs- und Risikoberichte im Vergleich zu den Anforderungen und Erwartungen sowie Test- und Prüfungsprogramme zu einer besseren Koordination und Zusammenarbeit bei.

Darstellungen aus der Praxis

Ein Beispiel für die Koordination und Zusammenarbeit ist der Datenschutz. Die Compliance-Abteilung (in bestimmten Unternehmen in Zusammenarbeit mit der Rechtsabteilung) ermittelt die rechtlichen Anforderungen, teilt sie dem Unternehmen mit und sorgt dafür, dass geeignete Verfahren und Kontrollen eingeführt werden. Die Geschäftsteams (Betrieb, IT, Informationssicherheit usw.) setzen die Aktivitäten um, einschließlich der Überwachung, Eskalation und Meldung von Informationen nach Bedarf. Das Informationssicherheitsteam und die Compliance-Teams überwachen die wichtigsten Risikobereiche, um sicherzustellen, dass die Geschäftsteams die Verfahren einhalten und die Überwachung und Berichterstattung angemessen ist. Die Interne Revision beurteilt bei der Prüfung dieser Bereiche den Rahmen für das Management relevanter Risiken, einschließlich des Compliance-Risikos, sowie die damit verbundenen und von den Geschäftsteams durchgeführten Prozesse und Kontrollen.

- Chief Compliance Officer, United Kingdom

ESG ist ein gutes Beispiel für die Koordination und Zusammenarbeit innerhalb der Organisation, um die Anforderungen und Erwartungen zu erfüllen. Die Rollen der ersten, zweiten und dritten Linie müssen im Rahmen ihrer jeweiligen Funktion und unter der Aufsicht des Leitungsorgans zusammenarbeiten, um die gewünschten ESG-Ergebnisse zu erzielen. Diejenigen, die für Compliance verantwortlich sind, werden mit anderen in der Organisation zusammenarbeiten, um die ESG-Ziele der Organisation zu erreichen:

- **Das Leitungsorgan legt die Strategie und die Risikobereitschaft fest und gibt den Ton für Kultur und Verhalten an.**
- **Das Management integriert die ESG-Anforderungen und -Erwartungen in die Governance und den Betrieb der Organisation.**
  - **Bietet Beratung, Rahmenbedingungen und Anforderungen zu Inhalt, Gestaltung und Umsetzung geeigneter Strukturen, Systeme und Prozesse für die strategische und operative Planung, Zielsetzung, Datenerfassung, Entscheidungsfindung und Berichterstattung im Zusammenhang mit ESG.**

- **Beurteilt die mit der Einhaltung der externen ESG-Anforderungen und -Standards und der internen Richtlinien und Ziele verbundenen Risiken.**
- **Entwickelt Standards, Rahmenwerke, Grundsätze oder Modellen, die für die Messung, Überwachung und Berichterstattung der Auswirkungen auf die Erreichung von ESG-Ergebnissen angewendet werden sollten.**
- **Bewertet die Genauigkeit und Konsistenz von Daten und Methoden, die zur Erhebung von Daten für die Nachhaltigkeits- und ESG-Berichterstattung verwendet werden.**
- **Führt von Mess- und Bewertungsverfahren ein, definiert Wesentlichkeit und listet relevante Indikatoren (KPIs) auf, führt interne und externe Berichterstattungsmethoden, -richtlinien und -instrumente ein.**

- **Die Interne Revision bietet dem Leitungsorgan unabhängige Prüfungssicherheit hinsichtlich der oben genannten Aktivitäten und der Erreichung der ESG-Ziele durch das Management sowie dem Management Berichterstattung über die Einhaltung von Anforderungen und Erwartungen.**

- Chief Compliance Officer, United Kingdom

Wichtige Fakten über Compliance

Zehn wichtige Punkte, die es zu beachten gilt

1. Möglicherweise gibt es keine speziellen Ressourcen, Abteilungen, Manager usw. für Compliance. Nicht alle Organisationen sind in der Lage oder müssen Ressourcen auf diese Weise zuweisen. In dem Maße, in dem Organisationen komplexer werden, in hohem Maße oder spezifisch reguliert sind, größer werden, einer stärkeren Kontrolle unterliegen, in einem sich schnell verändernden Umfeld (regulatorisch, wirtschaftlich usw.) tätig oder und sich mit ähnlichen Faktoren auseinandersetzen müssen, entscheiden sie häufig, dass als arbeitsteilige und formale Komponente der Organisationsgestaltung Einzelpersonen, Teams, Systeme und/oder andere Ressourcen für Aspekte der Compliance eingesetzt werden müssen. Solche Ressourcen können extern sein, z. B. durch die Auslagerung bestimmter Compliance-Überwachungen oder fachlicher Kompetenzen.

2. Bei der Anwendung der sechs Grundsätze des *Drei-Linien-Modells* zur Bewertung von Funktionen im Zusammenhang mit Compliance ist es sinnvoll, die Ergebnisse zu betrachten, für die die Funktion verantwortlich ist:

- Einhaltung von Gesetzen, Vorschriften, Verträgen, Richtlinien, Verfahren, Verhaltenskodizes oder anderen Anforderungen bei der Bereitstellung von Produkten und Dienstleistungen.
- Fachaufsicht, Risikobeurteilung (insbesondere auf aggregierter oder Portfoliobasis) und Durchführung von Risikomanagementaktivitäten sowie glaubwürdiges Hinterfragen der ersten Linie, um die Einhaltung der geltenden Verhaltenskodizes oder Standards, Anforderungen und Erwartungen in der gesamten Organisation zu fördern und zu erreichen.
- Beurteilung der Angemessenheit und Wirksamkeit des Compliance-Programms.
- Bereitstellung von Expertenmeinungen zur Wirksamkeit des Compliance-Programms und seiner Komponenten in der gesamten Organisation.

3. Eine einzige Compliance-Rolle oder -Abteilung innerhalb einer Organisation deckt möglicherweise nicht alle Compliance-relevanten Angelegenheiten für diese Organisation ab.[8] In solchen Fällen sollte die Organisation den Umfang der Compliance-Rolle(n) oder -Abteilung(en) sowie die Zuständigkeit von Rollen für andere Anforderungen und Erwartungen klar dokumentieren. Dies ist für kleinere Organisationen – in denen einer Person mehrere Aufgaben und Rollen zugewiesen und einige Aufgaben ausgelagert werden können – ebenso wichtig wie für größere Organisationen, in denen es mehrere Rollen oder Abteilungen geben kann, die mit verschiedenen Compliance-Aktivitäten betraut sind.

4. Eine Compliance-Funktion oder der Leiter einer Compliance-Abteilung kann in der Praxis und vorbehaltlich rechtlicher und aufsichtsrechtlicher Anforderungen einer der folgenden Rollen in einer Organisation unterstellt sein: der obersten Führungsebene (z. B. dem CEO, dem Chief Risk Officer, dem Chief Operating Officer, dem Chefsyndikus oder anderen) und/oder dem Leitungsorgan oder einem Ausschuss dessen. In einigen Fällen kann die Compliance-Abteilung, obwohl sie Teil des Managements ist, an den CAE berichten. Die Angemessenheit dieser Berichtslinie kann zum Teil durch die Beurteilung der Verantwortlichkeiten gemäß dem *Drei-Linien-Modell* und den jeweiligen rechtlichen und regulatorischen Anforderungen bestimmt werden.

[8] Für die Bereiche Ethik, Nachhaltigkeit, Finanzberichterstattung, Datenschutz, Personalwesen und rechtliche Verpflichtungen kann es beispielsweise eigene interne und/oder externe Ressourcen geben, die für Compliance oder zusätzliche Beaufsichtigung und Risikomanagement für bestimmte Compliance-Komponenten bieten. Im Zuge der Entwicklung von Umwelt-, Sozial- und Governanceaspekten (ESG) gibt es beispielsweise eine Reihe neuer Rollen, Verantwortlichkeiten, Aktivitäten und Abteilungen in verschiedenen Organisationen, die sich auf die Compliance der weitreichenden Aspekte von ESG konzentrieren.

5. Eine Compliance-Funktion oder der Leiter einer Compliance-Abteilung kann einem oder mehreren Board-Komitees oder deren Vorsitzenden unterstellt sein oder Rechenschaft ablegen. Dies ist jedoch nicht gleichbedeutend mit Unabhängigkeit vom Management und ersetzt nicht die Notwendigkeit einer unabhängigen Prüfung durch die Interne Revision.

6. Einzelne Compliance-Rollen und Compliance-Abteilungen können unter anderem für folgende Aufgaben zuständig sein: umfassendes Compliance-Risikomanagement, Überwachung, Test, Analyse, Beurteilung, Beratung, Prüfungssicherheit, Festlegung von Richtlinien, Entwicklung und Umsetzung von Systemen und Kontrollen, Managemententscheidungen, Beaufsichtigung und Schulung.

7. Compliance-Rollen und -Abteilungen können auch Aufgaben umfassen, die eng oder direkt mit der Bereitstellung von Produkten und Dienstleistungen verbunden sind. Dies würde eine klare Dokumentation der Zuständigkeiten, Befugnisse und Verantwortlichkeiten in der Rolle erfordern (z. B. die Fähigkeit, die Nichteinhaltung von Vorschriften bei der Bereitstellung eines Produkts oder einer Dienstleistung zu verhindern, indem eine Transaktion untersagt oder ein Veto gegen eine Managemententscheidung eingelegt wird).

8. Die Rollen der ersten und zweiten Linie sollten getrennt werden. Die Mitglieder der ersten Linie sollten die Risiken, die sie eingehen, selbst tragen. Die Mitglieder der zweiten Linie sollten die Rahmenbedingungen und Standards festlegen und überwachen, um die erste Linie bei der Bewältigung ihrer Risiken zu unterstützen, und gleichzeitig die Entscheidungen und Aktivitäten der ersten Linie glaubwürdig hinterfragen. In der Praxis kann es je nach den Anforderungen der Rechtsordnung oder der Branche sowie der Größe und Komplexität der Organisation und anderer Faktoren zu einer Vermischung der Rollen kommen. In diesem Fall müssen die Kompatibilität dieser Rollen beurteilt und die damit verbundenen Risiken gemindert werden. Dies kann Anpassungen der Rollenzusammensetzung erfordern, um die Risiken, die sich aus miteinander unvereinbaren Tätigkeiten innerhalb einer Rolle ergeben, wirksam zu mindern. Die Verantwortung für das Risikomanagement verbleibt bei den Rollen der ersten Ebene und im Umfang des Managements.

9. Unabhängig davon, wie Organisationen ihre Ressourcen für Compliance-Verpflichtungen strukturieren, trägt das Management die Verantwortung dafür, dass die Organisation ihre Anforderungen und Erwartungen innerhalb der vom Leitungsorgan festgelegten Risikobereitschaft erfüllt.

10. Eine wesentliche Aufgabe der Compliance-Funktion in der zweiten Linie ist die Beurteilung der Wirksamkeit des Compliance-Programms der Organisation und der Anstrengungen, die erforderlich sind, um die Compliance-Anforderungen und Erwartungen der Organisation zu erfüllen.

ANHANG:
Anpassung der Zuständigkeiten für Compliance-Rollen und -Aktivitäten

Compliance-Aktivitäten sind ein wesentlicher Bestandteil der Governance, des Risikomanagements und der internen Kontrolle einer Organisation. Die Verantwortung für die Maßnahmen, die zur Erreichung, Unterstützung, Überprüfung und Bestätigung der Compliance erforderlich sind, sowie die Ausführung dieser Verantwortung kann verschiedenen Teilen der Organisation zugewiesen werden. Die für die Compliance-Aktivitäten Verantwortlichen müssen die erwarteten Ergebnisse definieren, die die Compliance ausmachen, und geeignete Maßnahmen festlegen, um das Erreichen dieser Ergebnisse nachzuweisen.

Zu den Tätigkeiten, die Compliance umfassen, gehören unter anderem die folgenden:

- Identifikation relevanter externer Gesetze, Regeln und Vorschriften sowie interner Richtlinien, Standards, Verfahren und Verhaltenskodizes sowie akzeptabler Verhaltensweisen im Einklang mit den Organisationszielen.
- Festlegung angemessener Risikomessung für die Einhaltung und Nichteinhaltung relevanter externer Gesetze, Regeln und Vorschriften sowie interner Richtlinien, Standards, Verfahren und Verhaltenskodizes und akzeptablen Verhaltens im Einklang mit den Organisationszielen.
- Durchführung von Risikobeurteilungen im Hinblick auf die Einhaltung einschlägiger externer Gesetze, Regeln, Vorschriften und interner Richtlinien, Standards und Verfahren, einschließlich künftiger und neu auftretender Risiken, sowie auf Verhaltenskodizes und akzeptablem Verhalten im Einklang mit den Organisationszielen.
- Entwurf, Entwicklung und Implementierung von Prozessen und Kontrollen, um die Einhaltung einschlägiger externer Gesetze, Regeln und Vorschriften sowie interner Richtlinien, Standards, Verfahren und Verhaltenskodizes und akzeptablen Verhaltens im Einklang mit den Organisationssielen zu erreichen.
- Durchführen, Aufrechterhalten und Steuern von Prozessen und Kontrollen, um die Einhaltung von externen Gesetzen, Regeln und Vorschriften sowie von internen Richtlinien, Standards, Verfahren und Verhaltenskodizes und akzeptables Verhalten im Einklang mit den Organisationszielen zu erreichen.
- Bewertung, Test und Überwachung der Einhaltung einschlägiger externer Gesetze, Regeln und Vorschriften sowie interner Richtlinien, Normen, Verfahren und Verhaltenskodizes sowie akzeptablen Verhaltens im Einklang mit den Unternehmenszielen.
- Glaubwürdiges Hinterfragen des Managements in Bezug auf das Compliance-Risiko.
- Steuerung und Minderung von Compliance-Risiken.
- Ermittlung von Fällen der Einhaltung oder Nichteinhaltung von Regeln.
- Bericht und Eskalation von Fällen der Nichteinhaltung von Regeln.
- Meldung der Einhaltung oder Nichteinhaltung von Regelungen externen und internen Anforderungen.
- Förderung einer Kultur, die Compliance unterstützt.

- Sensibilisierung durch Kommunikation, Schulung, Werbung und Ausbildung.
- Konsultation und Beratung zu Compliance-Aspekten.
- Einrichtung und Aufrechterhaltung eines Ethik- oder Whistleblowing-Programms.
- Entwicklung und Durchführung von Compliance-Schulungen, -Ausbildung und -Sensibilisierung.
- Wahrnehmung von Aufgaben als Bindeglied zwischen den Aufsichtsbehörden und der Organisation.
- Aufbau und Pflege von Beziehungen zu Fachorganisationen und Branchenverbänden, um relevante Standards, Kodizes oder Richtlinien zu ermitteln, an die sich die Organisation und ihre jeweiligen Tätigkeiten halten sollten oder können, und um das Erfassen und Berichten von Benchmark-Informationen zu erleichtern.
- Aufbau und Pflege von Kontakten zu Infrastrukturorganisationen der Branche, die die Einhaltung von Anforderungen oder Erwartungen an die Nutzer der Infrastruktur und die Gegenparteien festlegen und verlangen können.

Es ist wichtig, dass die Zuständigkeiten und die gewünschten Ergebnisse der einzelnen Rollen klar sind. Einige dieser Aufgaben und Tätigkeiten sind mit anderen Aufgaben unvereinbar, wie z. B. innerhalb der dritten Linie die Genehmigung von Transaktionen, die Akzeptanz von Kunden oder andere Entscheidungen über Geschäftsrisiken, wie im *Drei-Linien-Modell* beschrieben. Wenn die Interne Revision gebeten wird, solche Aufgaben zu übernehmen, sind wichtige Sicherheitsvorkehrungen erforderlich, einschließlich der Zustimmung des Leitungsorgans oder des Audit Committees, des Einsatzes eines Dienstleisters zur Lieferung unabhängiger Prüfungssicherheit in den betroffenen Bereichen und gegebenenfalls der aufsichtsrechtlichen Genehmigung.

Ebenso muss eine Organisation, selbst wenn sie die besten Absichten hat, das Ergebnis der Bereitstellung von Produkten und Dienstleistungen für Kunden in Übereinstimmung mit den Regelungen zu erreichen, wachsam sein, um Rollen zu identifizieren, deren Verantwortlichkeiten sowohl auf die Einhaltung der Regelungen bei der Bereitstellung des Produkts oder der Dienstleistung als auch auf die Überwachung und das umfassendere Compliance-Risikomanagement ausgerichtet sind. Es gelten die Grundprinzipien der Funktionstrennung und der Unabhängigkeit sowie die Erwartung, die entstehenden Risiken zu mindern, wenn miteinander unvereinbare Tätigkeiten in den Rollen festgestellt werden.

In ähnlicher Weise besteht bei denjenigen, die eine Aufsichtsfunktion innehaben, zuweilen die Versuchung, bei der Feststellung von Lücken oder Mängeln im Risikomanagement und in den Kontrolltätigkeiten, die der Bereitstellung von Produkten oder Dienstleistungen zugrunde liegen, ihren eigenen Aufgabenbereich über die Beaufsichtigung hinaus auf die Ausführung auszudehnen. Auch der umgekehrte Fall kann eintreten, wenn sich die erste Linie zu sehr auf die Rollen verlässt, die für die Beaufsichtigung oder das Risikomanagement zuständig sind. Dies untergräbt die Vorteile einer objektiven Beaufsichtigung. In solchen Fällen obliegt es der Beaufsichtigungsfunktion, die Lücke oder den Mangel sowie die Abhilfemaßnahmen des Managements zu identifizieren, zu eskalieren und zu überwachen. Diese Elemente sollten in Übereinstimmung mit den festgelegten Governance-Rollen und -Verantwortlichkeiten abgestimmt und dokumentiert werden.