Verhalten in Organisationen

Topical Requirement

User Guide

The Institute of Internal Auditors

DIIR Deutsches Institut für Interne Revision e.V.

Contents

Überblick über die Topical Requirements

Die Topical Requirements sind ein wesentlicher Bestandteil der Internationalen Grundlagen für die berufliche Praxis (International Professional Practices Framework®), zusammen mit den Global Internal Audit Standards™ und Global Guidance. Das Institute of Internal Auditors fordert, dass die Topical Requirements in Verbindung mit den Standards angewendet werden, die die maßgebliche Grundlage für die geforderten Praktiken darstellen. Dieses Dokument enthält Referenzierungen zu den Standards als Quelle für ausführlichere Informationen.

Die Topical Requirements formalisieren die Art und Weise, wie Interne Revisorinnen und Revisoren allgegenwärtige Risikobereiche angehen, um die Qualität und Konsistenz innerhalb des Berufsstandes zu fördern. Das Mandat der Internen Revision definiert klar den Umfang und die Arten der von der Internen Revision erbrachten Leistungen, darunter auch die Berücksichtigung der Topical Requirements (Standard 6.1 „Mandat der Internen Revision“). Topical Requirements bilden eine Grundlage und liefern relevante Kriterien für die Durchführung von Prüfungsleistungen, die sich auf den Gegenstand eines Topical Requirement beziehen (Standard 13.4 „Bewertungskriterien“). Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich und wird für die Bewertung bei Beratungsleistungen empfohlen. Es ist nicht die Absicht der Topical Requirements, alle potenziellen Aspekte abzudecken, die bei der Durchführung von Prüfungsaufträgen zu berücksichtigen sind. Sie sollen vielmehr einen Mindestsatz an Anforderungen bereitstellen, um eine konsistente, zuverlässige Beurteilung des Themas zu ermöglichen.

Die Topical Requirements sind klar mit dem Drei-Linien-Modell des IIA und den Global Internal Audit Standards verlinkt. Governance, Risikomanagement und Kontrollprozesse sind, in Übereinstimmung mit Standard 9.1 „Verstehen von Governance-, Risikomanagement- und Kontrollprozessen“, die Hauptbestandteile der Topical Requirements. In Verbindung mit dem Drei-Linien-Modell beziehen sich Governance auf Leitungs- und Überwachungsorgane, Risikomanagement auf die zweite Linie und Kontrollen oder Kontrollprozesse auf die erste Linie. Das Management ist sowohl in der ersten als auch in der zweiten Linie vertreten. Die Interne Revision stellt als unabhängiger und objektiver Assurance Provider, der den Leitungs- und Überwachungsorganen Bericht erstattet, die dritte Linie dar (Prinzip 8 „Aufsicht durch das Leitungs- und Überwachungsorgan").

Anwendbarkeit, Risiko und professionelles Urteilsvermögen

Topical Requirements müssen befolgt werden, wenn Interne Revisionen Prüfungsaufträge zu Themen durchführen, für die es ein Topical Requirement gibt, oder wenn Aspekte des Topical Requirement in anderen Prüfungsaufträgen identifiziert werden.

Wie in den Standards beschrieben, ist die Risikobeurteilung ein wichtiger Teil der Planung durch die Revisionsleitung. Die Festlegung der in den Revisionsplan aufzunehmenden Prüfungsaufträge erfordert eine mindestens jährliche Beurteilung der Strategien, Ziele und Risiken der Organisation (Standard 9.4 „Revisionsplan“). Bei der Planung einzelner Prüfungsaufträge müssen die

Internen Revisorinnen und Revisoren die für den Auftrag relevanten Risiken beurteilen (Standard 13.2 „Risikobeurteilung zu einem Auftrag“).

Wenn der Gegenstand eines Topical Requirement während des risikobasierten Planungsprozesses der Internen Revision identifiziert und in den Revisionsplan aufgenommen wird, müssen die im Topical Requirement dargelegten Anforderungen zur Beurteilung des Themas im Rahmen der betroffenen Aufträge angewendet werden. Zusätzlich muss das Topical Requirement im Rahmen eines Auftrags auf seine Anwendbarkeit hin beurteilt werden, wenn die Interne Revision einen (im Plan enthaltenen oder nicht im Plan enthaltenen) Auftrag durchführt und Elemente des Topical Requirement identifiziert werden. Außerdem muss das Topical Requirement auf seine Anwendbarkeit hin beurteilt werden, wenn ein Auftrag erteilt wird, der ursprünglich nicht im Plan vorgesehen war und das Thema umfasst.

Bei der Anwendung des Topical Requirement spielt die professionelle Beurteilung eine wichtige Rolle. Risikobeurteilungen sind die Grundlage für Entscheidungen von Revisionsleitungen, welche Aufträge in den Revisionsplan aufgenommen werden sollen (Standard 9.4). Darüber hinaus nutzen Interne Revisorinnen und Revisoren ihre professionelle Beurteilung, um zu entscheiden, welche Aspekte im Rahmen der einzelnen Aufträge abgedeckt werden sollen (Standards 13.3 „Auftragsziele und Auftragsumfang“, 13.4 „Bewertungskriterien“ und 13.6 „Arbeitsprogramm“), und um die Ressourcen zu identifizieren, die notwendig sind, um die Auftragsziele zu erreichen (Standard 13.5 „Auftragsressourcen“).

Es ist nachzuweisen, dass die Anwendbarkeit jeder Anforderung des Topical Requirement beurteilt wurde, einschließlich einer Begründung für den Ausschluss von Anforderungen. Die Einhaltung des Topical Requirement muss unter Nutzung des professionellen Urteils der Prüferinnen und Prüfer, wie in Standard 14.6 „Auftragsdokumentation“ beschrieben, dokumentiert werden.

Das Topical Requirement liefert einen Mindestrahmen für die zu berücksichtigenden Kontrollprozesse, aber Organisationen, die das Risikothema als sehr hoch einschätzen, müssen möglicherweise zusätzliche Aspekte beurteilen.

Wenn die Revisionsleitung feststellt, dass die Interne Revision nicht über die erforderlichen Kenntnisse verfügt, um Revisionsaufträge zu einem Thema der Topical Requirements durchzuführen, kann der Auftrag an einen externen Dienstleister vergeben werden (Standards 3.1 „Kompetenz“, 7.2 „Qualifikation der Revisionsleitung“, 10.2 „Management personeller Ressourcen“). Die Standards gelten für alle Personen oder Funktionen, die Leistungen der Internen Revision erbringen, unabhängig davon, ob eine Organisation interne Revisorinnen oder Revisoren direkt beschäftigt, sie über einen externen Dienstleister beauftragt oder beides. Die Revisionsleitung trägt die letztendliche Verantwortung für die Einhaltung der Standards. Wenn die Revisionsleitung feststellt, dass die Ressourcen für die Interne Revision unzureichend sind, muss sie das Leitungs- und Überwachungsorgan über die Auswirkungen der unzureichenden Ressourcen und darüber informieren, wie Ressourcenengpässe behoben werden sollen (Standard 8.2 „Ressourcen“).

Durchführung, Dokumentation und Berichterstattung

Bei der Anwendung der Topical Requirements müssen Interne Revisorinnen und Revisoren auch die Standards einhalten und ihre Tätigkeiten im Einklang mit Domain V („Erbringung von Revisionsleistungen“) durchführen. Die Standards in Domain V beschreiben die Planung von Aufträgen (Prinzip 13 „Plane Aufträge wirksam“), die Durchführung von Aufträgen (Prinzip 14 „Führe die

Auftragsarbeiten aus“) und die Kommunikation von Auftragsergebnissen (Prinzip 15 „Kommuniziere Auftragsergebnisse und überwache Maßnahmenpläne“).

Topical Requirements sind entwickelt worden, um konsistente und qualitativ hochwertige Revisionspraktiken zu unterstützen. Sie sind in Verbindung mit den geltenden lokalen Gesetzen, Vorschriften, aufsichtsrechtlichen Erwartungen und anderen fachlich anerkannten Rahmenwerken anzuwenden, die zusätzliche oder spezifischere Anforderungen auferlegen können. Interne Revisorinnen und Revisoren haben möglicherweise bereits Arbeitsprogramme und Prüfungsverfahren auf der Grundlage dieser Vorschriften und Rahmenwerke entwickelt. Sie sollten ihre geplanten Prüfungshandlungen zum Verhalten in Organisationen und alle zuverlässigen Prüfungshandlungen anderer interner und externer Assurance Provider (Standard 9.5 „Koordination und Vertrauen“) mit den Topical Requirements abgleichen, um eine angemessene Abdeckung sicherzustellen.

Die Abdeckung des Topical Requirement kann auf Grundlage der professionellen Beurteilung der Prüferinnen und Prüfer entweder im Revisionsplan oder in den Arbeitspapieren des Auftrags dokumentiert werden. Die Anforderungen können von einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Der Nachweis, dass das Topical Requirement auf seine Anwendbarkeit hin geprüft wurde, muss, einschließlich einer Begründung für etwaige Ausschlüsse, aufbewahrt werden.

Qualitätsprüfung

Die Standards verlangen, dass die Revisionsleitung ein Programm zur Qualitätssicherung und Verbesserung entwickelt, umsetzt und aufrechterhält, das alle Aspekte der Internen Revision abdeckt (Standard 8.3 „Qualität“). Die Ergebnisse sind der Geschäftsleitung und dem Überwachungsorgan mitzuteilen. In der Kommunikation muss über die Einhaltung der Standards durch die Interne Revision und die Erreichung der Leistungsziele berichtet werden.

Die Einhaltung der Topical Requirements sollte in der Beaufsichtigung auf Auftragsebene (Standard 12.3 „Überwachung und Verbesserung der Leistung bei der Durchführung von Aufträgen“) berücksichtigt werden und wird im Rahmen von Qualitätsbeurteilungen beurteilt.

Verhalten in Organisationen

Die Neuausrichtung der Prüfung von Kultur

Der Fortschritt von der Prüfung der Kultur als ein abstraktes und vages Thema hin zu einer strukturierten und präzisen Beurteilung des Verhaltens in Organisationen stellt eine notwendige und zeitgemäße Weiterentwicklung innerhalb des Berufsstands der Internen Revision dar. Obwohl allgemein anerkannt ist, dass kulturelle Defizite oft die Ursache für erhebliches Kontrollversagen sind, hat dieser Bereich in der Praxis der Internen Revision noch keine nennenswerte Bedeutung erlangt. Die Neudefinition der Prüfung der „Kultur” als Prüfung des „Verhaltens in Organisationen, das nicht an den Organisationszielen ausgerichtet ist” bietet eine klarere, strukturiertere, präzisere und besser prüfbare Grundlage. Wie bei jedem Risiko können Organisationen dies durch die Entwicklung geeigneter Kontrollen und deren wirksame Umsetzung bewältigen.

> Hinweis
>
> Die Topical Requirements verwenden die allgemeine Terminologie der Internen Revision, so wie sie in den Global Internal Audit Standards definiert ist. Leser sollten die Begriffe und Definitionen im Glossar der Standards konsultieren.

Das Topical Requirement zum Verhalten in Organisationen übernimmt diese Philosophie und legt Mindestanforderungen für die Beurteilung des Verhaltens fest, wenn eine Risikobeurteilung ergibt, dass es in den Umfang der Überprüfung fällt. Diese Anforderungen sind vollständig mit dem traditionellen risikobasierten Prüfungsansatz vereinbar und können mit minimalen Anpassungen auf alle Prüfungsfunktionen angewendet werden. Dieser begleitende User Guide enthält praktische Beispiele dafür, wie dieser Ansatz in Standard-Prüfungsaufträge integriert werden kann, sowie Leitlinien zur Überprüfung des umfassenderen Rahmenwerks für das Verhalten in der Organisation oder einzelner Komponenten. Der erhebliche Einfluss dieses Themas auf die Organisationsziele erfordert eine proaktive Betrachtung und Anwendung.

Die Definitionen der folgenden Schlüsselbegriffe sind für das Verständnis und die Anwendung des Topical Requirements notwendig. Angesichts der Unausgereiftheit des Themas verwenden Organisationen diese Begriffe uneinheitlich. Die bereitgestellten Definitionen sollen den Benutzern helfen, die Terminologie ihrer Organisation an die Terminologie des Topical Requirements und dieses User Guides anzupassen.

- **Kultur** – Entscheidungen, die Mitarbeiterinnen und Mitarbeiter während ihrer Tätigkeit treffen, und die Art und Weise, wie sie mit anderen zusammenarbeiten, sowie die Faktoren, die dieses Verhalten innerhalb der Organisation beeinflussen. Zu diesen Faktoren zählen formelle Mechanismen wie Anreize und Ziele sowie informelle Mechanismen wie kollektive Werte und Überzeugungen.
- **Leistungsbeurteilungen** – Einzel- oder Gruppenbewertungen zur Angemessenheit der eigenen Arbeit.
- **Leitungs- und Überwachungsorgan** – Das höchste Gremium der Organisation, das mit der Governance beauftragt ist.
- **Stakeholder** – Eine Gruppierung mit einem direkten oder indirekten Interesse an den Aktivitäten und Resultaten einer Organisation. Dazu können das Leitungs- und Überwachungsorgan, das Management, Mitarbeiterinnen und Mitarbeiter, Kunden, Lieferanten, Aktionäre, Regulierungsbehörden, Finanzinstitute, externe Prüfer, die Öffentlichkeit und andere gehören.
- **Verhalten** (conduct) – Verhalten in Bezug auf regulatorische Anforderungen und Erwartungen.
- **Verhalten in Organisationen –** Die beobachtbaren Entscheidungen, die Mitarbeiterinnen und Mitarbeiter während ihrer Tätigkeit treffen, und wie sie mit anderen zusammenarbeiten. Dieses Verhalten beeinflusst die Leistung und das Erreichen der Organisationsziele. Einfach ausgedrückt ist das Verhalten in Organisationen „die Art und Weise, wie wir Dinge tun“. Es wird als Teilbereich der Organisationskultur betrachtet.
- **Verhaltensanreize** – Alles, was zur Motivation von Verhalten zur Verfügung gestellt werden kann, einschließlich monetärer Anreize, wie Gehaltserhöhungen, Boni oder Aktienoptionen, oder nicht monetärer Anreize, wie Komplimente, bevorzugte Aufgaben oder freie Tage.
- **Verhaltensbezogene Risikoindikatoren** – Verwertbare Managementinformationen zum Verhalten.

- **Verhaltensmuster** – Muster, bei denen das Verhalten wiederholt auftritt oder häufiger vorkommt. Sie werden im weiteren Sinne als „die Art und Weise, wie Dinge getan werden" definiert, im Gegensatz zu einmaligen Situationen.
- **Verhaltensrisiko** – Risiko, dass das Verhalten nicht zu den Organisationszielen passt.
- **Werte** – Grundsätze, die das erwartete Verhalten von Menschen leiten.

Abschnitte

Die verbindlichen Anforderungen im Topical Requirement Verhalten in Organisationen und die nicht verbindlichen Überlegungen in diesem User Guide sind in drei Abschnitte unterteilt:

- **Governance** – Klar definierte grundlegende Ziele und Strategien für das Verhalten in der Organisation, die die Ziele, Richtlinien und Verfahren der Organisation unterstützen.
- **Risikomanagement** – Prozesse zur Identifizierung, Analyse, Bewältigung und Überwachung von Risiken im Zusammenhang mit dem Verhalten in der Organisation, einschließlich eines Prozesses zur unverzüglichen Eskalation von Vorfällen.
- **Kontrollen** – Vom Management festgelegte, regelmäßig bewertete Kontrollprozesse zur Minderung von Risiken im Zusammenhang mit dem Verhalten in der Organisation.

Zusätzlich zu den Topical Requirements und diesem User Guide können Interne Revisorinnen und Revisoren weitere fachliche Leitlinien zum Verhalten in Organisationen heranziehen, beispielsweise im Global Guidance des IPPF oder andere, branchenspezifische Ressourcen.

Überlegungen

Interne Revisorinnen und Revisoren können die folgenden Überlegungen heranziehen, um die Beurteilung der Anforderungen des Topical Requirements Verhalten in Organisationen zu unterstützen. Die Buchstaben der einzelnen Überlegungen unten verweisen auf die entsprechenden Anforderungen im Topical Requirement. Diese Überlegungen dienen der Veranschaulichung und sind nicht verbindlich. Interne Revisorinnen und Revisoren sollten sich bei der Entscheidung, was sie in ihre Beurteilungen einbeziehen, auf ihr fachliches Urteilsvermögen stützen.

Einschränkungen bei Aufträgen der Internen Revision im öffentlichen Sektor aufgrund von Gesetzgebung, Regierungsstruktur oder politischem Umfeld werden als potenzielle Hindernisse für die Bearbeitung bestimmter Aspekte dieser Arbeit anerkannt. Interne Revisorinnen und Revisoren im öffentlichen Sektor sollten solche Einschränkungen des Umfangs im Rahmen ihres Risikobeurteilungsprozesses dokumentieren und ihr fachliches Urteilsvermögen einsetzen, um den maßgeschneiderten Umfang ihrer Überprüfung klar zu definieren und zu kommunizieren.

Überlegungen zur Governance

Zur Beurteilung, wie die Governanceprozesse auf das Verhalten in der Organisation angewendet werden können, können Interne Revisorinnen und Revisoren das Folgende überprüfen:

A. Strukturierte Aufgaben und Verantwortlichkeiten zur Sicherstellung, dass das Leitungs- und Überwachungsorgan die Sichtbarkeit und den Einfluss auf die Verhaltensdimensionen der Organisation aufrechterhält. Nachweise können Folgendes umfassen:
    - Ein Governance-Komitee:

- Richtet einen eigenen Ausschuss oder Unterausschuss ein, der sich auf das Verhalten in der Organisation konzentriert und klare Aufgabenbereiche hat, die die Überwachung des Verhaltens in der Organisation mit der strategischen Umsetzung verknüpfen.
- Führt regelmäßige Überprüfungen von verhaltensbezogenen Risikoindikatoren durch, die an den langfristigen Geschäftszielen ausgerichtet sind. Verhaltensbezogene Risikoindikatoren sind Kennzahlen, die anzeigen, ob Maßnahmen erforderlich sind, um sicherzustellen, dass das Verhalten weiterhin mit den Organisationszielen, den damit verbundenen Werten und dem Zweck der Organisation in Einklang steht.
- Bezieht verhaltensbezogene Ziele in die Leistungsbewertungen von Führungskräften und deren Vergütung ein.

- Rahmenwerke für die Berichterstattung an das Leitungs- und Überwachungsorgan:
  - Bieten Einblicke in verhaltensbezogene Risikoindikatoren mithilfe strukturierter Dashboards (z. B. Mitarbeiterengagement, Trends in Vorfällen, Kundenzufriedenheit, wertebasierte Anerkennung).
  - Integrieren kulturbezogene Metriken in die Berichterstattung über strategische Leistungsberichterstattung auf Ebene des Leitungs- und Überwachungsorgans.
- Feedbackmechanismen für Stakeholder, wie z. B. Umfragen, ermöglichen:
  - Dass das Leitungs- und Überwachungsorgan direkte Beiträge zur Ausrichtung des Verhaltens an Werten und Strategie durch die Mitarbeiterinnen und Mitarbeiter, Kunden und andere Stakeholder erhält.
  - Feedback zur Gestaltung der strategischen Ausrichtung und zu Verhaltensinterventionen.

B. Eine effektive Steuerung des Verhaltens in der Organisations erfolgt durch klar definierte Verantwortlichkeiten innerhalb der gesamten Organisation. Das Leitungs- und Überwachungsorgan ist letztendlich dafür verantwortlich, dass die Organisation ein Verhalten fördert und aufrechterhält, das mit ihren organisatorischen Zielen in Einklang steht. Dazu gehören die Festlegung klarer Erwartungen an das Verhalten, die Überwachung der Berichterstattung über Verhaltensrisiken und die Konfrontation des Managements, wenn Abweichungen festgestellt werden. Als Nachweis kann Folgendes dienen:

- Das Leitungs- und Überwachungsorgan:
  - Genehmigt die Risikobereitschaft der Organisation für Verhaltensrisiken und wichtige kulturelle Ziele.
  - Fordert regelmäßíge Berichterstattung über Indikatoren für Verhaltensrisiken (z. B. Trends, Vorfallsmuster, Hinweisgeberthemen).
  - Macht die oberste Führungsebene durch Mechanismen wie Anreizstrukturen und „Tone at the Top“ für die kulturelle Performance verantwortlich.
  - Trifft sich mit Funktionen der zweiten und dritten Linie zu Sachverhalten bezogen auf die Eskalation von Verhaltensrisiken, auf Lücken in der Beaufsichtigung und Angemessenheit von Abhilfemaßnahmen.

- Geschäftsbereiche und das operative Management integrieren Verhaltensvorgaben in den täglichen Betrieb und stellen sicher, dass Entscheidungen, Kommunikation und Teamdynamik die erklärten Werte der Organisation widerspiegeln. Dazu kann die Übernahme von Verantwortung für folgende Bereiche gehören:
  - Modellierung gewünschter Verhaltensweisen und Aufrechterhaltung einer psychologisch sicheren Umgebung.
  - Implementierung von Kontrollen, die das Verhalten beeinflussen, wie z. B. Rekrutierung, Belohnung, Kommunikation und Führungsroutinen.
  - Proaktive Identifizierung und Eskalation von Verhaltensrisiken, sobald diese im operativen Umfeld auftreten.
  - Minderung von Verhaltensrisiken, die eine Folge von Fehlverhalten innerhalb ihrer Teams und der Notwendigkeit von formellen und informellen) Kontrollen sind.
- Risiko, Compliance, Personalwesen und damit verbundene Aufsichtsfunktionen entwerfen und pflegen das Verhaltensrisikorahmenwerk der Organisation. Dies umfasst:
  - Definierte Aufgaben und Verantwortlichkeiten für die Verhaltensüberwachung.
  - Eskalationswege und Datenanalyseprozesse.
  - Dashboards, thematische Analysen und regelmäßige Beurteilungen, um einen vorausschauenden Einblick in die Verhaltensbedingungen in der gesamten Organisation zu erhalten.
  - Die Fähigkeit, Praktiken in Frage zu stellen, bei denen Anreize, Kommunikation oder Führungsverhalten von den erklärten Zielen abweichen.
  - Beratung zu allen wesentlichen Änderungen an mitarbeiterbezogenen Kontrollen, Governance-Rahmenwerken oder strategischen Transformationsinitiativen, die sich auf die Kultur auswirken können.
  - Überprüfung neuer Trends aus Vorfallberichten, Prüfungsfeststellungen und anderen Sicherungsmechanismen, die auf verhaltensbezogene Probleme hinweisen.

c. Governanceprozess, der die Beaufsichtigung des Verhaltens, regelmäßige Überwachung, Bewertungen und die Angleichung von Verhaltensmustern an die Organisationsziele sicherstellt. Der Prozess kann Folgendes umfassen:

- Die Nutzung eines Dashboards zur Bereitstellung wichtiger Datenpunkte aus Quellen wie Umfrageergebnissen zur Mitarbeiterzufriedenheit und Integrität, Fluktuations- und Fehlzeitenquoten, Inhalten aus Speak-up-Kanälen, Daten zu Vorfällen sowie Leistungs- und Innovationskennzahlen. Zu den Merkmalen eines wirksamen Dashboards für das Verhalten in der Organisation gehören:
  - Festlegung von Schwellenwerten zur Identifizierung von Möglichkeiten zur Verhaltensverbesserung.
  - Trennung von Verhaltensdaten (z. B. Speak-up-Daten) von Treiberdaten (z. B. Klarheit der Aufgaben und Verantwortlichkeiten) und Ergebnisdaten (z. B. Kundenbeschwerden).

- Kombination von quantitativen Daten, z. B. aus Umfragen, und qualitativen Daten, z. B. aus Fokusgruppen und Speak-up-Kanälen.

- Das Leitungs- und Überwachungsorgan versteht, wie aktuelle Aspekte des Verhaltens in der Organisation angegangen werden können, um die Wirksamkeit und Leistung der Organisation zu verbessern. Diese Aspekte umfassen, wie:
  - Entscheidungen getroffen werden, einschließlich der Suche nach neuen Perspektiven und Herausforderungen.
  - Mitarbeiterinnen und Mitarbeiter untereinander kommunizieren, einschließlich der Äußerung von Bedenken und Erwartungen.
  - Mitarbeiterinnen und Mitarbeiter zusammenarbeiten, z. B. teamübergreifend und bei der Bewältigung von Konflikten.
  - Mitarbeiterinnen und Mitarbeiter auf Versäumnisse reagieren, z. B. durch Lernen aus Fehlern oder durch Schuldzuweisung und Ablehnung.
  - Sich das Führungsverhalten der mittleren und oberen Führungsebene auf die anderen Verhaltenskategorien auswirkt (z. B. wie Führungskräfte auf Fehler reagieren und wie sie Herausforderungen bei der Entscheidungsfindung annehmen).
  - Strategie und Geschäftsmodell Entscheidungsfindung, Verhaltenskodizes und Leistungsmanagement durch Anreize/Abschreckungsmaßnahmen antreiben.

- Das Leitungs- und Überwachungsorgan fordert ein System kontinuierlichen Lernens, das Verbesserungspotenziale identifiziert und diese aktiv und messbar angeht durch:
  - Verwendung evidenzbasierter Erkenntnisse, die auf dem tatsächlichen Verhalten der Mitarbeiterinnen und Mitarbeiter beruhen.
  - Fokus auf das, was innerhalb der Organisation tatsächlich geschieht, anstatt auf das, was beabsichtigt oder gewünscht ist.
  - Beurteilung einer Mischung aus qualitativen und quantitativen Daten, die häufig durch Umfragen, Speak-up-Kanäle, vertrauliche Gespräche und Fokusgruppen gewonnen werden.
  - Anwendung der Erkenntnisse, um Maßnahmen zu bestimmen, die bestimmte Aspekte des Verhaltens in der Organisations stärken und angehen.
  - Einbeziehung eines Maßnahmenplans, um gezielte Interventionen in kritischen Bereichen (z. B. Kommunikationsstrategie, Schulungen, Führungskräfteentwicklung und Diskussionen auf Teamebene) zu kombinieren.

D. Richtlinien und Verfahren zum Vorgehen bei Verhaltensrisiken werden festgelegt, regelmäßig überprüft, wirksam kommuniziert und in die Geschäftsabläufe und Entscheidungsprozesse integriert. Die Richtlinien und Verfahren umfassen die Bereiche Ethik, Personalwesen, Compliance, Risiko, Betrieb und Entscheidungsbefugnisse, um Folgendes sicherzustellen:

- Verhaltenserwartungen werden in relevanten Richtlinien (wie einem Verhaltenskodex und/oder Richtlinien zu Ethik, Personalwesen, Anreizen und der Übertragung von Befugnissen) formell festgelegt. Diese Richtlinien sollten anhand praktischer

Beispiele akzeptables und inakzeptables Verhalten definieren und mit der Risikobereitschaft der Organisation in Einklang stehen.

- Risikomanagementfunktionen ordnen Verhaltenserwartungen den wichtigsten betrieblichen Prozessen zu – wie Einstellung, Leistungsbeurteilung, Einarbeitung und Kundenmanagement – und stellen sicher, dass diese in den täglichen Entscheidungen berücksichtigt werden. Im Rahmen von Prüfungen sollte untersucht werden, wie sich diese Erwartungen auf das tatsächliche Verhalten auswirken, und dem Leitungs- und Überwachungsorgan Bericht erstattet werden.
- Das Leitungs- und Überwachungsorgan bemüht sich darum und erhält Prüfungssicherheit darüber, dass die Richtlinien der Organisation über verschiedene Kanäle (z. B. Intranet, Schulungen, Mitarbeiterversammlungen) zugänglich sind und klar kommuniziert werden. Durch die Einbindung von Fallstudien und Entscheidungsbäumen lassen sich Verhaltenserwartungen besser in einen Kontext setzen. Dashboards können das Verständnis und die Nutzung messen.
- Alle Verhaltensrichtlinien und -verfahren unterliegen einem festgelegten Überprüfungszyklus und werden als Reaktion auf Vorfälle, Umfrageergebnisse oder regulatorische Änderungen aktualisiert. Die Funktionen der zweiten Linie sollten ein Register mit gewonnenen Erkenntnissen führen, um Lücken zwischen dem Verhalten und den Organisationszielen zu identifizieren.
- Das Leitungs- und Überwachungsorgan erhält regelmäßig aktuelle Informationen über den Umfang, die Klarheit und die Wirksamkeit der Richtlinien. Die zweite Linie sollte Verstöße, Auswirkungen der Richtlinien und die Übereinstimmung mit dem gewünschten Verhalten analysieren. Die Wirksamkeit der Richtlinien sollte anhand von qualitativem Feedback und Verhaltensrisikokennzahlen überprüft werden.

Überlegungen zum Risikomanagement

Um zu beurteilen, wie Risikomanagementprozesse auf das Verhalten in der Organisation angewendet werden, können Interne Revisorinnen und Revisoren Folgendes überprüfen:

A. Ein Prozess zum Management von Verhaltensrisiken ist klar definiert und umfasst Verhaltensmerkmale, die für die Erreichung der Organisationsziele kritisch sind. Zu den Merkmalen des Risikomanagements können gehören:
   - Die Rollen und Verantwortlichkeiten stehen in Einklang mit den Rahmenwerken für Unternehmensrisiken und Governance, und die Berichtswege ermöglichen Unabhängigkeit und Einflussnahme.
   - Befugnis, Entscheidungen anzufechten und verhaltensbezogene Risikothemen zu eskalieren, ohne Vergeltungsmaßnahmen oder Verharmlosung befürchten zu müssen.
   - Unabhängigkeit vom operativen Management mit direktem Zugang zur obersten Führungsebene und zum Leitungs- und Überwachungsorgan.
   - Zugriff auf relevante, zeitnahe und aus verschiedenen Quellen triangulierte Verhaltensrisikodaten. Diese Daten umfassen sowohl strukturierte (z. B. Umfrageergebnisse, Verstöße gegen Richtlinien) als auch unstrukturierte Formen (z. B. Meldungen von Missständen, Erkenntnisse aus Fokusgruppen). Zu den Datenquellen gehören

Personalwesen (z. B. Fluktuation, Mitarbeiterbindung und Umfragedaten), Hinweisgeber, Kundenbeschwerden und Prüfungsfeststellungen.

- Nutzung von Datenanalysen zur Identifizierung von Trends, Anomalien und aufkommenden Risiken.
- Nutzung von Dashboards und Risikoindikatoren zur Information des Managements und zur Berichterstattung an das Leitungs- und Überwachungsorgan.
- Nutzung von mit den Organisationszielen verbundenen Verhaltensrisikoindikatoren.
- Durchführung oder Auslagerung von Überprüfungen der Ursachen für Fehlverhalten und kulturelle Diskrepanzen.
- Vertrautheit mit formellen und informellen Verhaltenstreibern (z. B. Anreizsysteme, psychologische Sicherheit und Führungsstil).
- Glaubwürdigkeit und Vertrauen der Führungskräfte gegenüber den operativen Teams, kombiniert mit der Fähigkeit, Entscheidungen in Echtzeit zu beeinflussen.
- Aktive Beteiligung an der Gestaltung und Überprüfung von Kontrollen im Personalwesen (z. B. Anreizsysteme, Einstellung und Schulung).
- Beratende Funktion bei strategischen Veränderungsprogrammen und Transformationsinitiativen.
- Zusammenarbeit mit Führungskräften aus den Geschäftsbereichen, um die Kultur durch Einflussnahme und nicht nur durch Anweisung zu gestalten.
- Laufende Erfassung und Analyse von Daten, darunter möglicherweise:
  - Umfragen zum Engagement und Wohlbefinden der Mitarbeiterinnen und Mitarbeiter.
  - Anerkennungs- und Belohnungsdaten für werteorientiertes Verhalten.
  - Hinweisgebermeldungen und Beschwerden.
  - Kundenfeedback, das sowohl Zufriedenheit als auch Unzufriedenheit hervorhebt.
  - Leistungsbeurteilungen, die Zusammenarbeit, Integrität und Innovation widerspiegeln.
- Einsatz von Datenanalysen zur Identifizierung von Schwachstellen und Erkennung von Trends.
- Ein klar definierter Prozess zur sofortigen Eskalation von Risiken und Verhaltensweisen, die nicht mit den Organisationszielen übereinstimmen.
- Beaufsichtigung der Festlegung und Umsetzung von Maßnahmenplänen des Managements zur Bewältigung von Risiken und zur Stärkung erforderlicher Verhaltensweisen.

B. Zu den zeitnahen Überwachungsprozessen für das Verhalten in der Organisation gehört die Berichterstattung der Ergebnisse an die Stakeholder. Beispiele für Risikoindikatoren in den Kategorien Verhalten, Treiber und Ergebniskategorien sowie meldepflichtige Mängel sind:

- Entscheidungsfindung: Mangelnde wirksame Hinterfragung oder unzureichende Einbeziehung unterschiedlicher Perspektiven.
- Kommunikation: Unzureichende Beachtung der von Einzelpersonen gemeldeten Probleme.
- Zusammenarbeit: Fragmentierte Arbeitsumgebungen, in denen sich die Mitarbeiter nur auf ihre eigene Arbeit konzentrieren.
- Reaktion auf Mängel: Schuldzuweisungen und Bestrafungen für unbeabsichtigte Fehler.
- Formale Treiber: Unklare Aufgaben und Verantwortlichkeiten oder widersprüchliche Ziele.
- Informelle Treiber: Geringe psychologische Sicherheit oder ineffektive Dynamik zwischen den drei Linien.
- Leistungsdaten: Übermäßige Kundenbeschwerden oder stagnierende Innovation oder Digitalisierung.
- Personaldaten: Hohe Fluktuation und Fehlzeiten sowie geringe Zufriedenheit in Umfrageergebnissen.
- Risiko- und Rechtsdaten: Hohe Anzahl von Untersuchungen, Verstößen gegen Richtlinien oder Warnmeldungen und knapp vermiedenen Situationen.

c. Prozesse, die sicherstellen, dass Abweichungen zwischen erwartetem und beobachtetem Verhalten identifiziert und an diejenigen kommuniziert werden, die über die Befugnis und Fähigkeit zum Handeln verfügen. Interne Revisorinnen und Revisoren können Folgendes überprüfen:

- Wirksame Kommunikation ist zeitnah, evidenzbasiert und wird durch die Analyse der zugrunde liegenden Treiber und Ursachen gestützt.
- Gestaltung und operative Wirksamkeit der Kommunikationsmaßnahmen vermeiden oberflächliche Lösungen, Reputationsschäden oder wiederholte Misserfolge.
- Informationen werden aus verschiedenen Quellen gesammelt und zusammengefasst, darunter Mitarbeiterfeedback, Hinweisgeber-Meldungen, Prüfungsfeststellungen und Vorfallüberprüfungen.
- Strukturierte Analysetechniken – wie thematische Überprüfungen, verhaltenswissenschaftliche Modelle und Rahmenwerke zur Ermittlung der Ursachen – gehen über oberflächliche Symptome hinaus und identifizieren die zugrunde liegenden Ursachen für Fehlentwicklungen (z. B. unklare Anreize, geringe psychologische Sicherheit oder ineffektive Führungsstile).
- Lücken werden nicht einfach als Compliance-Verstöße oder isolierte Vorfälle dargestellt, sondern als Ereignisse mit verhaltensbezogenen Ursachen, die kulturelle, systemische und/oder Führungsprobleme widerspiegeln.
- In der Kommunikation wird anhand quantitativer und qualitativer Daten, die die Schlussfolgerungen untermauern, hervorgehoben, was passiert ist und warum.
- Die Organisation trennt Verhaltensmuster, Schwachstellen, die sich aus Verhaltensfaktoren ergeben, und organisatorische Ergebnisse (z. B. Auswirkungen auf die

Leistung, Vertrauen der Stakeholder), sodass das Verhalten und seine Ursachen angegangen werden können. Die Feststellungen werden der richtigen Zielgruppe in der richtigen Detailtiefe mitgeteilt:

- Operative Manager für sofortige Prozesskorrekturen.
- Führungskräfte für die Zuweisung von Ressourcen, die Kommunikation und den Tonfall.
- Leitungs- und Überwachungsorgan oder relevante Ausschüsse für die Beaufsichtigung und strategische Implikationen.

- Visuelle und narrative Tools wie Dashboards, Heatmaps oder Fallzusammenfassungen erläutern die Ergebnisse und unterstützen Empfehlungen und/oder Maßnahmenpläne.
- Auswirkungen auf die Risikoexposition und die Widerstandsfähigkeit des Kontrollumfelds werden in die Prozessüberprüfungen einbezogen.
- Die Kommunikation von Lücken ist an Abhilfemaßnahmen geknüpft und wird auf ihre Erledigung hin überwacht.
- Die Ergebnisse der Interventionen werden beurteilt und weitergegeben, wodurch der Lernzyklus abgeschlossen wird.
- Die Kommunikation ist frei von unzulässiger Einflussnahme und entspricht den festgelegten Eskalationsverfahren, wodurch die Unabhängigkeit und Glaubwürdigkeit der Beurteilungen gewahrt bleibt.

D. Diskrepanzen zwischen erwartetem und tatsächlichem Verhalten werden auf strukturierte und partizipative Weise behoben, um sicherzustellen, dass Abhilfemaßnahmen auf den Erkenntnissen der Stakeholder basieren, bis zu ihrem Abschluss verfolgt und auf ihre Wirksamkeit hin bewertet werden. Interne Revisorinnen und Revisoren können Folgendes überprüfen:

- Der Lösungsprozess bezieht die am stärksten betroffenen Stakeholder sinnvoll mit ein, darunter operative Manager, Personalabteilung, Geschäftspartner, Arbeitnehmervertreter, Compliance-Berater und betroffene Einzelpersonen oder Teams. Ihre Beiträge stellen sicher, dass die Maßnahmen:
  - Kontextbezogen sind: Sensibel für die betrieblichen Realitäten und informellen Normen, die möglicherweise zu dem Problem beigetragen haben.
  - Glaubwürdig und akzeptiert sind: Höhere Wahrscheinlichkeit, unterstützt und verankert zu werden, wenn die Maßnahmen von den direkt Beteiligten gestaltet werden.
  - Konstruktiv herausfordernd sind: Ermöglichen eine offene Reflexion über beitragendes Führungsverhalten, Schwächen im Kontrollsystem oder Gruppendynamik.
- Die Beiträge der Stakeholder werden eingeholt, zusammengefasst und in Maßnahmenpläne integriert. Zu den Feedback-Mechanismen können Interviews, Fokusgruppen, Umfragediagnostik und andere Methoden gehören.
- Abhilfemaßnahmen werden mit definierten Verantwortlichkeiten, Zeitrahmen und Erfolgskriterien dokumentiert:

- Die Maßnahmen stehen in einem angemessenen Verhältnis zur Bedeutung des Problems.
- Bei Bedarf zielen die Maßnahmen auf formelle Faktoren (z. B. Richtlinien, Anreize) und informelle Faktoren (z. B. psychologische Sicherheit, Teamdynamik) ab.
- Sind mehrere Funktionen beteiligt (z. B. Personalwesen für Schulungen, Risikomanagement für Kontrollen), werden die funktionsübergreifende Umsetzung und Verantwortlichkeiten koordiniert und geklärt.

- Der Fortschritt wird bis zur Fertigstellung verfolgt, um sicherzustellen, dass die Verpflichtungen erfüllt und aufrechterhalten werden. Dazu gehören:
  - Führen eines Verhaltensproblems- oder Verhaltensmaßnahmenregisters oder eines gleichwertigen Tools.
  - Regelmäßige Rücksprache mit den Maßnahmenverantwortlichen, um den Status zu überprüfen.
  - Eskalation von Verzögerungen, Teilfertigstellungen oder Widerständen an die zuständigen Governance-Gremien.
- Die Wirksamkeit der Lösung hinsichtlich der Schließung der Lücke und der Verringerung des Verhaltensrisikos wird beurteilt. Dies kann Folgendes umfassen
  - Neubeurteilung der Verhaltensrisikoindikatoren nach der Umsetzung.
  - Einholung von Feedback von betroffenen Stakeholdern zu beobachteten Veränderungen.
  - Überprüfung von Verhaltensänderungen durch Beobachtung, Umfragen oder Revisionstechniken.
  - Anpassung oder Verstärkung der Maßnahmen, wenn die Ergebnisse schwach oder unklar bleiben.

Überlegungen zu Kontrollprozessen

Um zu beurteilen, wie Kontrollprozesse angewandt werden, um das Risiko zu mindern, dass Verhaltensweisen in der Organisation nicht mit den organisatorischen Zielen übereinstimmen, können Interne Revisorinnen und Revisoren Folgendes überprüfen:

A. Überprüfungen des Verhaltensrisikos, um das Risiko zu verstehen, das durch das derzeitige Verhalten in der Organisation entsteht (d. h. die potenziellen unbeabsichtigten Folgen der Art und Weise, wie Dinge getan werden). Beispiele für solche Überprüfungen sind Beurteilungen von Projekten nach deren Abschluss, Ursachenanalysen und Überprüfungen detaillierter Abläufe in der Praxis.

B. Strukturierte Feedback-Prozesse, um zu verstehen, welche Mechanismen das Management einsetzt, um Erwartungen an das Verhaltens zu kommunizieren (z. B. Town Halls, E-Mail und Treffen zwischen Einzelpersonen und ihren Führungskräften), und um die Wirksamkeit des Management-Tons auf das Verhalten innerhalb einer Organisation zu ermitteln. Dies kann durch die Bewertung der Prozesse geschehen, mit denen die Wahrnehmung und das Verständnis der Mitarbeiterinnen und Mitarbeiter für die Botschaften des Leitungs- und Überwachungsorgans erfasst und analysiert werden. Interne Reviso-

rinnen und Revisoren können Organisationen dabei helfen, ihre Kommunikationsstrategien kontinuierlich zu verfeinern und sicherzustellen, dass der Tone from the Top auf allen Ebenen wirksam ankommt, indem sie Schlüsselkontrollen überprüfen, z. B.:

- Regelmäßige Umfragen, Interviews und Fokusgruppendiskussionen mit Mitarbeiterinnen und Mitarbeitern, in denen Klarheit, Konsistenz und Wirkung der Führungskommunikation erfragt werden und die quantitative und qualitative Daten darüber liefern, wie gut die Botschaften auf den verschiedenen Ebenen der Organisation ankommen und verstanden werden.
- Offene Kanäle für anonyme Rückmeldungen, die es den Mitarbeiterinnen und Mitarbeitern ermöglichen, ihre ehrliche Meinung zu äußern, ohne Repressalien befürchten zu müssen. Diese Kanäle sollten durch digitale Plattformen ermöglicht werden, die Feedback und Vorschläge in Echtzeit erlauben. Die aus diesen Kanälen gewonnenen Daten sollten daraufhin analysiert werden, ob der Tone at the Top von den Mitarbeiterinnen und Mitarbeitern auf allen Ebenen gut verstanden wird.
- Feedback von Sitzungen der Geschäftsleitung, das durch Umfragen, Interviews, Fokusgruppen, Protokolle und anonyme Kanäle gesammelt wird, um sicherzustellen, dass die Geschäftsleitung über unwirksame Kommunikation, Missverständnisse oder verbesserungsbedürftige Bereiche informiert ist. Die Geschäftsleitung zeigt, dass der Beitrag des Personals geschätzt wird, indem sie aktiv auf das Feedback eingeht und darauf reagiert. Wenn dies nicht geschieht, sind die Mitarbeiterinnen und Mitarbeiter möglicherweise weniger geneigt, Feedback zu geben, weil sie das Gefühl haben, dass sich nichts ändern wird.
- Das Feedback zu den Leistungen der Geschäftsleitung ist Bestandteil ihrer Leistungsbeurteilungen, um die Akzeptanz durch die Führung erlassenen Richtlinien kontinuierlich zu überwachen. Dadurch wird die Bedeutung der Führungsbotschaften gestärkt und sichergestellt, dass sie im Tagesgeschäft berücksichtigt werden.

c. Die Eskalation innerhalb einer Organisation wird gefördert, um Risiken frühzeitig zu erkennen und zu mindern und um ein psychologisch sicheres Umfeld zu schaffen, in dem sich die Mitarbeiterinnen und Mitarbeiter wohl fühlen, wenn sie Probleme melden, ohne Vergeltungsmaßnahmen befürchten zu müssen. Interne Revisorinnen und Revisoren können Schlüsselkontrollen überprüfen, um dabei zu helfen, das effektive Risikomanagement zu verbessern, wie z. B.:

- Einfach zu handhabende Feedback-Mechanismen, wie direkte Berichtswege und anonyme Optionen, Hotlines für internen und externen Fraud und Hinweisgeber, Umfragen, Boxen für Vorschläge und digitale Plattformen, um vertrauliche Meldungen zu ermöglichen und Probleme zu erfassen, die Einzelpersonen möglicherweise zögern, offen zu melden.
- Gut definierte und leicht verständliche Prozesse für die Meldung von Problemen, mit mehreren direkten und anonymen internen und externen Kanälen und Bemühungen, das Bewusstsein der Mitarbeiterinnen und Mitarbeiter zu fördern. Zu den Merkmalen der Meldekanäle sollten gehören:
  - Vertraulichkeitsgarantien zum Schutz der Identität von Personen, die Probleme melden.

- Strenge Richtlinien zum Verzicht auf Vergeltungsmaßnahmen, die klar kommuniziert und konsequent eingehalten werden, um Personen, die Probleme melden, zu schützen.
- Rückmeldung an Personen, die Probleme nicht anonym melden, ungeachtet des Grundes oder des Ergebnisses.
- Regelmäßige organisationsweite Zusammenfassungen der in der Vergangenheit gemeldeten Probleme und ihrer Ergebnisse, um zu zeigen, dass Probleme gemeldet und behandelt werden, und um Transparenz über die ergriffenen Maßnahmen zu gewährleisten und Rückmeldungen zu adressieren.

- Regelmäßige Kommunikation seitens des Managements, in der die Bedeutung einer offenen Kommunikation und der Meldung von Problemen hervorgehoben wird und die zeigt, wie das Management selbst ein solches Verhalten vorlebt.
- Regelmäßige Schulungen, in denen die Bedeutung der psychologischen Sicherheit hervorgehoben wird, in denen der Einzelne ermutigt wird, Probleme zu melden, und in denen Hinweise gegeben werden, wie man Probleme angemessen eskalieren kann. Die Schulungen sollten in regelmäßigen Abständen wiederholt werden, um die gewünschten Verhaltensweisen mit der Zeit zu verstärken.
- Informelle Belohnungen, wie z. B. mündliche oder schriftliche Wertschätzung und öffentliche Anerkennung, für Personen, die Probleme melden.
- Regelmäßige Überprüfung des Eskalationsprozesses, um seine Effektivität und Effizienz zu gewährleisten, einschließlich der Einholung von Mitarbeiterfeedback, um Hindernisse für die Meldung von Problemen zu ermitteln und umgehend zu beseitigen.
- Kommunikation über die Lösung von Rückmeldungen.

D. Anreiz- und Abschreckungsprogramme, die mit den gewünschten Verhaltensweisen und Zielen der Organisation übereinstimmen und kommuniziert werden. Interne Revisorinnen und Revisoren können unter anderem folgende Kontrollen überprüfen:

- Sowohl monetäre (z. B. Prämien, Beförderungen) als auch nicht-monetäre (z. B. Anerkennung, Entwicklungsmöglichkeiten) Anreize sind auf die Organisationsziele abgestimmt und an das Zeigen der gewünschten Verhaltensweisen gebunden.
- Ausgewogene Kriterien für die Leistungsbeurteilung umfassen sowohl die Art und Weise, wie die Ziele erreicht werden (z. B. Zusammenarbeit, Integrität und Kundenorientierung), als auch traditionellere Leistungskennzahlen (z. B. finanzielle Ziele)
- Anreizkriterien und Abschreckungsschwellen sind klar definiert, werden einheitlich angewandt und unterliegen der Überprüfung durch das Management oder die Personalabteilung, um Voreingenommenheit und unbeabsichtigte Ergebnisse zu vermeiden.
- Funktionsübergreifende Gruppen validieren die Konsistenz und Fairness von Anreizentscheidungen in allen Geschäftsbereichen.

- Zu den Konsequenzen für Fehlverhalten und Verstöße gegen die Organisationskultur gehören klare, verhältnismäßige Abschreckung (z. B. Bonuskürzungen und Beförderungssperren), wobei die Maßnahmen erläutert und dokumentiert werden, um Transparenz zu gewährleisten.
- Nicht-monetäre Anerkennungsprogramme heben Mitarbeiterinnen und Mitarbeiter hervor, die kulturelle Werte wie ethische Entscheidungsfindung und psychologische Sicherheit vorleben.
- Die Auswirkungen von Anreizprogrammen werden routinemäßig durch Mitarbeiterfeedback und Verhaltenskennzahlen beurteilt, um die Belohnungsmechanismen zu verfeinern oder neu auszutarieren. Anreizprogramme sollten bewertet und angepasst werden, um Folgendes sicherzustellen:
  - Die Ziele sind weder zu eng noch zu weit gefasst.
  - Die Ziele sind erreichbar.
  - Die kurzfristigen Ziele untergraben nicht die langfristigen Ergebnisse.
  - Ein akzeptables Maß an Risikobereitschaft wird formuliert.
  - Sicherheitsvorkehrungen werden getroffen, um ethisches Verhalten bei der Erreichung der Ziele zu gewährleisten (z. B. Führungskräfte als Vorbilder für ethisches Verhalten, Kosten für Betrug sind weitaus höher als der Nutzen, strenge Beaufsichtigung).
  - Die Ziele sind auf die individuellen Fähigkeiten und Umstände zugeschnitten, wobei die Fairness gewahrt bleibt.
  - Die Teamziele stehen nicht im Widerspruch zu den individuellen Zielen.
  - Die intrinsische Motivation wird beurteilt, und das Management erkennt an, dass einige Ziele die intrinsische Motivation einschränken können.
  - Die Endziele der Organisation werden berücksichtigt, und die Art der Ziele (z. B. Leistung oder Lernen) wird auf ihre Angemessenheit hin beurteilt.
- Die Organisation integriert positive Verstärkung und Abhilfemaßnahmen, um ein proaktives Verhalten in der Organisationsverhalten zu kultivieren, das mit den Organisationszielen und den regulatorischen Anforderungen in Einklang steht. Die Schlüsselkontrollen sollten Folgendes umfassen:
  - Regelmäßige Beurteilung der Wirksamkeit von Kommunikations- und Schulungsprogrammen, um sicherzustellen, dass die Mitarbeiterinnen und Mitarbeiter die Bedeutung der Meldung von Problemen und die Konsequenzen von Verstößen verstehen und sich ermutigt fühlen, Probleme zu melden.
  - Überwachungs- und Berichterstattungssysteme verfolgen die Einhaltung der Regelungen und identifizieren potenzielle Meldeversäumnisse.
  - Disziplinarmaßnahmen werden konsequent und fair angewandt und sind weder so hart, dass sie von einer Meldung abhalten, noch so milde, dass sie unethisches Verhalten nicht verhindern.
  - Feedback-Mechanismen, die es den Mitarbeiterinnen und Mitarbeitern ermöglichen, Probleme anonym zu melden, werden regelmäßig überprüft, um sicherzustellen, dass sie wirksam sind und eine ehrliche Berichterstattung fördern.

E. Der Problemmanagementprozess der Organisation identifiziert Verhalten, das nicht mit den Organisationszielen übereinstimmt, und eskaliert dies, wenn nötig, um einen Maßnahmenplan für das Management zu erstellen, der das Risiko schlechter Ergebnisse mindert. Interne Revisorinnen und Revisoren können die Schlüsselkontrollen für wirksame Maßnahmen zur Verhaltensänderung überprüfen, wie z. B.:

- Evidenzbasierte Ansätze: Der Maßnahmenplan beinhaltet evidenzbasierte Ansätze zur Verhaltensänderung, die auf Verhaltenswissenschaft, Verhaltensmodellen und Change Management beruhen. Wenn der Ansatz nicht explizit auf einem bestimmten Modell zur Verhaltensänderung beruht, sollte er Interventionsstrategien für folgende Bereiche kombinieren:
  - Kommunikation: Kontinuierliche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter und des Managements für die Notwendigkeit einer Verhaltensänderung sowie für die Akzeptanz und Unterstützung des Wandels.
  - Mitarbeiterschulung und -entwicklung: Investitionen in Schulungsprogramme, die auf die verschiedenen Rollen zugeschnitten sind, und die Vermittlung der erforderlichen Fähigkeiten und Verhaltensweisen an die Mitarbeiterinnen und Mitarbeiter durch Workshops, E-Learning und Möglichkeiten der kontinuierlichen Weiterentwicklung. Dazu gehört auch, dass sie die neuen Fähigkeiten und Verhaltensweisen, die für die von der Organisation gewünschten Veränderungen erforderlich sind, erlernen und wirksam umsetzen können.
  - Entwicklung des Managements: Führungskräfte auf allen Ebenen überlegen, wie sie Verhaltensänderungen in täglichen Situationen ermöglichen und demonstrieren können. Dazu kann es gehören, dass das Management sein eigenes Verhalten anpasst, damit sich das Personal bei der Umsetzung der neuen Verhaltensweisen wohler fühlt, dass es die Mitarbeiterinnen und Mitarbeiter direkt auffordert, die neuen Verhaltensweisen umzusetzen, und dass es zum Lernen ermutigt und Schulungen zu den noch erforderlichen Fähigkeiten und Verhaltensweisen verlangt. Führungsprogramme und Coaching können die Fähigkeiten und das Selbstvertrauen verbessern.
- Konsequente Bestärkung in alltäglichen Situationen: Der Einzelne braucht Unterstützung, Ermutigung und regelmäßige Erinnerungen, um neue Verhaltensweisen zu entwickeln und sie in seine tägliche Arbeitsroutine zu integrieren.
- Kongruente Verstärkung: Ein Interventionsplan sollte in Bezug auf Führungsbotschaften, Prozesse, Systeme, Coaching und informelle Feedback-Mechanismen aufeinander abgestimmt sein, um die gewünschte Veränderung zu verstärken. Diese Abstimmung beseitigt Unsicherheit und Unklarheit und stellt sicher, dass die Mitarbeiterinnen und Mitarbeiter die gewünschten Verhaltensänderungen, deren Umsetzung und deren Bedeutung verstehen.
- Ausrichtung auf die Triebkräfte des Verhaltens: Nachhaltige Verhaltensänderung erfordert, dass man sich mit den zugrunde liegenden Triebkräften der Verhaltensweisen (siehe Risikomanagement, C) befasst und nicht nur mit den Verhaltensweisen selbst.

- Messung: Die Messung des Fortschritts und der Wirksamkeit der Maßnahmen hilft festzustellen, ob sie die gewünschte Wirkung erzielen und ob Anpassungen erforderlich sind. Regelmäßige Aktualisierungen wirken als positive Verstärkung und versorgen die Stakeholder mit Fortschrittsinformationen. Ein wirksamer Messansatz kombiniert qualitative und quantitative Methoden, wie z. B. Umfragen und Interviews, und liefert ein umfassendes Verständnis des Fortschritts.

F. Schulungsprogramme, die das Verhalten beeinflussen sollen, sind ausdrücklich mit definierten Verhaltenserwartungen oder Aussagen zur Risikobereitschaft verknüpft. Beispiele für Schulungsthemen sind Ethik, Compliance, Führung, Inklusion, Risikobewusstsein und Entscheidungsfindung. Interne Revisorinnen und Revisoren können überprüfen, ob die Schulungsprogramme Folgendes erfüllen:

- Spiegeln die gewünschten Verhaltensweisen und Einstellungen wieder und haben klare, dokumentierte Lernziele.
- Beruhen auf Verhaltensnachweisen oder Erkenntnissen aus Vorfällen (z. B. Revisionsfeststellungen, Ursachenanalysen und Feedback-Mechanismen).
- Richten sich an alle relevanten Funktionen mit maßgeschneiderten Modulen für die Geschäftsleitung, Manager und das Personal.
- Sind verpflichtend, wenn relevant (z. B. risikoreiche Prozesse, regulierte Verantwortlichkeiten und Kontrollfunktionen).
- Werden regelmäßig Aktualisierung, wobei der Inhalt mindestens einmal jährlich überprüft wird, um Relevanz und Wirksamkeit sicherzustellen.
- Sind wie folgt konzipiert:
  - Durch Einbindung von realen Szenarien oder Fallstudien Verhaltenserwartungen greifbar machen.
  - Verwendung von Techniken, die die Lernenden ansprechen (z. B. Storytelling und reflektierende Fragen).
  - Aktive Einbeziehung der Geschäftsleitung, um den Tone at the Top anzugeben und die Mitarbeiterinnen und Mitarbeiter zu ermutigen, Verhaltensänderungen vorzunehmen.
- Umfassen Auswirkungen und Kontrollen zur Herstellung von Prüfungssicherheit, die:
  - Den Abschluss von Pflichtschulungen und die Berichterstattung über Ausnahmen verfolgen.
  - Die Auswirkungen auf das Verhalten und die Mitarbeiterbindung durch informelle Umfragen, einfache Tests oder auf Beobachtung basierende Beurteilungen messen.
  - Die Perspektive der Teilnehmer und die Wirksamkeit der Schulungen durch strukturierte Feedbackprozesse erfassen.
  - Sicherstellen, dass die Schulungsinhalte zu den Risikorahmenwerken und Kontrollanforderungen passen und formale Überprüfungs- und Freigabeprozesse umfassen.

G. Die Einstellungsprozesse passen zu den Verhaltenserwartungen der Organisation und beziehen Verhaltenskompetenzen ein. Interne Revisorinnen und Revisoren können z. B. folgende Kontrollmerkmale überprüfen:

- Mithilfe von Instrumenten wie Leitfäden für strukturierte Interviews und szenariobasierten Fragen lässt sich die Übereinstimmung der Bewerber mit den Werten der Organisation beurteilen.
- Verhaltensbasierte Interviews und Feedback von Kollegen werden zur Beurteilung von Eigenschaften wie Empathie, ethisches Urteilsvermögen und Verantwortungsbewusstsein eingesetzt.
- Stellenanzeigen und Employer Branding spiegeln die kulturellen Bestrebungen der Organisation wider, um kulturell passende Bewerber zu interessieren.
- Feedback-Mechanismen ermöglichen es, die kulturelle Integration neu eingestellter Personen zu beurteilen, sodass Abweichungen frühzeitig erkannt werden können.
- Die Dokumentation (z. B. Bewertungsrahmen und Gesprächsprotokolle) zeigt, dass die Einstellungskriterien konsequent angewendet werden.
- Personalabteilung und Geschäftsleitung überprüfen die Einstellungsmuster auf Risiken wie Bevorzugung, Voreingenommenheit oder Nichteinhaltung von Verhaltensstandards.
- Einstellungs- und Beförderungsrichtlinien werden regelmäßig auf ihre Übereinstimmung mit den Werten der Organisation und ihre Wirksamkeit in der Praxis hin überprüft.

Anhang A. Praktische Anwendungsbeispiele

Die folgenden Beispiele beschreiben Szenarien, in denen das Topical Requirement „Verhalten in Organisationen" anwendbar wäre.

Beispiel 1: Einzelüberprüfung des Rahmenwerks zum Verhalten in der Organisation

Die Interne Revision veranlasste eine Einzelüberprüfung des übergreifenden Rahmenwerks zum Verhalten in der Organisation, um dessen Konzeption und operative Wirksamkeit beim Management von Verhaltensrisiken zu bewerten. Der Umfang dieses Auftrags umfasste die Governance-Strukturen, die Risikomanagement-Aktivitäten und die Verhaltenskontrollen, die die Ausrichtung der gesamten Organisation unterstützen.

Die Internen Revisoren haben beurteilt, ob die Zuständigkeiten für die Verhaltensbeaufsichtigung klar definiert und frei von Interessenkonflikten waren. Das Team überprüfte die Aufgabenbeschreibung des Leitungsorgans und vergewisserte sich, dass dieses regelmäßig über Indikatoren für Verhaltensrisiken, wie z. B. Umfrageergebnisse und Trends bei den Speak-up-Kanälen, unterrichtet wurde. Die Überprüfung umfasste auch die Bewertung, ob kulturbezogene Richtlinien, wie z. B. für Hinweisgebersysteme und ethisches Verhalten, routinemäßig aktualisiert und durchgesetzt wurden.

Die Internen Revisoren haben auch Elemente des Risikomanagements beurteilt, beginnend mit dem von der zweiten Linie verantworteten Rahmenwerk für das Management von Verhaltensrisiken, wobei sie sich darauf konzentrierten, ob die wichtigsten verhaltensbedingten Risikofaktoren (wie geringe psychologische Sicherheit oder falsch ausgerichtete Leistungsziele) ermittelt wurden. Die Beurteilung betonte, wie die Organisation die Abweichung zwischen erwartetem und beobachtetem Verhalten verfolgt und behandelt, einschließlich der Frage, ob Verhaltensanomalien systematisch eskaliert und verfolgt wurden

Das Kontrollumfeld wurde untersucht, um festzustellen, ob formale Prozesse die Verhaltenserwartungen unterstützen. Die Prüfer bewerteten Einstellungsprotokolle zur wertebasierten Beurteilung, ob der Inhalt der Einarbeitung mit den Normen der Organisationskultur übereinstimmt und inwieweit (monetäre und nicht-monetäre) Anreize auf unbeabsichtigte Folgen überprüft wurden. Darüber hinaus wurden Schulungsprogramme, Speak-up-Kanäle, Botschaften der Führungskräfte und verwendete Datenanalysen zur Erkennung von Verhaltensauffälligkeiten geprüft.

Dieser Auftrag hat einen umfassenden Überblick darüber geliefert, wie Verhaltensrisiken auf Organisationsebene gehandhabt werden, und bildet die Grundlage für Empfehlungen zur Verbesserung der Verhaltensinfrastruktur der Organisation.

Beispiel 2: Thematische Überprüfung von Anreizpraktiken

Bei diesem Prüfungsauftrag ging es darum, zu beurteilen, wie die Anreizsysteme der Organisation das Verhalten beeinflussen und ob sie mit der Zielsetzung, den Werten und den Erwartungen

der Organisation übereinstimmen. Die Interne Revision wählte dieses Thema aufgrund der zunehmenden Besorgnis über das Risiko von Fehlverhalten und der sich abzeichnenden Anzeichen für auf Druck basierendes Verhalten in den Geschäftseinheiten.

Die Prüfung begann mit der Bewertung der Governance-Regelungen für die Gestaltung und Genehmigung von Anreizstrukturen. Die Revision beurteilte, ob die für die Umsetzung von Governance-Entscheidungen zuständigen Stellen, wie Personalabteilung oder Vergütungsausschuss, eine formelle Aufsicht über die Gestaltung von Anreizen hatten und ob ihre Arbeit von den Risiko-, Compliance- oder Prüfungsfunktionen unabhängig überprüft wurde.

Es wurde eine Risikomanagementperspektive angewandt, um zu verstehen, ob bei der Entwicklung von Anreizstrukturen auch deren Auswirkungen auf das Verhalten berücksichtigt wurden. Die Prüfer untersuchten, ob die Organisation Szenarien getestet oder Verhaltensrisiken in Bezug auf ihre Vergütungsstrukturen analysiert hat. Sie überprüften auch, ob verhaltensbezogene Leistungsindikatoren, wie z. B. Messung der Zusammenarbeit, verfolgt und zur Bewertung der Ergebnisse herangezogen wurden.

Die Kontrolltests erstreckten sich auf eine Reihe von Mechanismen, mit denen belohnungsbezogenes Verhalten beeinflusst werden sollen. Dazu gehörten Balanced Scorecards mit Leistungskriterien, die die Leistungen und die Art und Weise, wie sie erreicht wurden, messen, die Anwendung von Malus (eine Strafe oder Gehaltskürzung) und/oder Rückforderungsbestimmungen sowie das Vorhandensein von 360-Grad-Feedbackprozessen. Die Prüfer untersuchten auch die Schulungen, die den Führungskräften zur Abgabe von Verhaltensfeedback angeboten wurden, und untersuchten nicht-monetäre Anerkennungsprogramme, die wertebasiertes Verhalten belohnten.

Während des gesamten Auftrags haben die Internen Revisoren versucht herauszufinden, ob Anreizpraktiken unbeabsichtigt zu unerwünschtem Verhalten führen könnten, wie z. B. übermäßige Risikobereitschaft, das Nutzen von Abkürzungen in Prozessen oder das Zögern, Probleme zu eskalieren. Es wurden Empfehlungen ausgesprochen, um die Transparenz zu verbessern, wertebasierte Ziele konsequenter zu verankern und die unabhängige Überprüfung des Managements der zweiten Linie bei der Gestaltung von Belohnungen zu stärken.

Beispiel 3: Integration in eine traditionelle Prüfung – Cyberrisiko-Management

In diesem Beispiel hat die Interne Revision Überlegungen zu Verhaltensrisiken in eine traditionelle Prüfung zum Cyberrisiko-Management integriert. Die Prüfer haben erkannt, dass viele Cyber-Versäumnisse nicht nur auf technische Probleme, sondern auch auf menschliches Verhalten zurückzuführen sind, und haben daher Verhaltensprüfungen in den gesamten Auftrag eingebaut.

Der Auftrag begann damit, zu beurteilen, inwieweit Verhaltensrisiken im Rahmen der Steuerung der Cyber-Resilienz anerkannt wurden. Die Prüfer überprüften die Aufsicht des Leitungs- und Überwachungsorgans über die Cyber-Strategie und suchten nach Belegen dafür, dass die Gremien die Abstimmung des Verhaltens mit den Organisationszielen überwachen und erörtern, z. B. die Einhaltung sicherer Praktiken oder die Vorbildfunktion der Führungskräfte für sicheres Verhalten.

Im Hinblick auf das Risikomanagement bewertete das Team, ob die Cyber-Risikobewertungen der Organisation menschliche Faktoren berücksichtigt haben. Dazu gehörte auch die Beurteilung, ob Verhaltensdaten (z. B. die Häufigkeit von Fehlern bei Phishing-Tests, Verletzungen des Systemzugriffs oder niedrige Abschlussquoten bei Schulungen) zur Überwachung und Eskalation

von Risiken verwendet wurden. Außerdem wurde untersucht, ob die Ursachen früherer Sicherheitsvorfälle ermittelt wurden, um potenzielle verhaltensbedingte Faktoren wie unklare Verantwortlichkeiten oder die Haltung des Managements zu identifizieren.

Die Kontrolltests konzentrierten sich auf die Gestaltung des Verhaltens und den sicheren Betrieb. Die Prüfer überprüften, ob bei der Einstellung von Mitarbeitern mit privilegiertem Zugang ein Verhaltensscreening durchgeführt wurde. Die Anreizstrukturen wurden dahingehend beurteilt, ob sie sichere Online-Praktiken förderten oder unbeabsichtigt riskantem Verhalten Vorrang vor Sicherheit einräumten. Auch die Cybersicherheitsschulungen wurden bewertet, um festzustellen, ob sie ansprechend waren, regelmäßig aufgefrischt wurden und Simulationen enthielten, in denen das Verhalten bei Phishing und Social Engineering getestet wurde.

Schließlich wurde untersucht, wie das Management sicheres Verhalten durch Kommunikation fördert und ob die Mitarbeiter sich wohl fühlen, wenn sie unsicheres Verhalten in Bezug auf Cybersicherheit melden. Eine Organisationskultur, die die Mitarbeiter ermutigt, ihre Meinung zu sagen, wurde als ein entscheidender Faktor für die Widerstandsfähigkeit angesehen

Die Einbeziehung von Verhaltensaspekten in diese Cyber-Prüfung führte zu tieferen Einsichten und nützlichen Empfehlungen und stärkte die Fähigkeit der Organisation, Risiken in einem ihrer wichtigsten Bereiche zu managen.

Anhang B. Fallstudien spezifischer Prüfungen

Fallstudie 1: Ministerium für Wohnungswesen (öffentlicher Sektor)

Die Beispiele in dieser Fallstudie zeigen, wie die Interne Revision einer Behörde das Topical Requirement Verhalten in Organisationen anwenden würde, um zu beurteilen, wie die Behörde ihr Ziel der Bereitstellung gerechter Wohnungsdienstleistungen für die Öffentlichkeit erreicht. Interne Revisoren sollten sich darüber im Klaren sein, dass die Prioritäten von Amtsträgern, politische Empfindlichkeiten, Haushaltsmittelzuweisungen und einige politische Entscheidungen außerhalb ihres Aufgabenbereichs liegen. Die Art und Weise, wie leitende Beamte und Führungskräfte diese Politik auslegen und anwenden, sowie die interne Kultur der Behörde gehören jedoch sicher in den Revisionsumfang.

Governance

A. Aufgaben und Zuständigkeiten – Die Abteilung verfügt über eine klare Organisationsstruktur mit einer Trennung der Zuständigkeit für die Gestaltung der Politik (leitende Beamte) und die Umsetzung der Wohnungspolitik. Ein Ziel der Internen Revision ist festzustellen, ob strukturelle Interessenkonflikte vermieden werden: Ist beispielsweise die Verantwortung für die Einhaltung der Richtlinien von der Aufsicht über die Auftragnehmer getrennt?

B. Rechenschaftspflicht – Der Leiter der Organisation und die oberste Führungsebene sind für organisatorische Ziele verantwortlich, die mit auf die Kultur bezogenen Ergebnissen verbunden sind, wie z. B. Fairness bei der Wohnungsvergabe und Wohlbefinden der Mitarbeiter. Die Interne Revision prüft, ob die Rechenschaftspflicht sichtbar ist und akzeptiert wird.

C. Aufsicht und Überwachung – Ein „Kulturausschuss“ unter dem Vorsitz einer leitenden Führungskraft prüft vierteljährlich Mitarbeiterbefragungen, Hinweisgeber-Daten und Beschwerden von Stakeholdern. Die Prüfer beurteilen, ob diese Prozesse eine Frühwarnung vor Fehlverhalten liefern.

D. Richtlinien und Verfahren – Es gibt angemessen genehmigte Verhaltenskodizes, Richtlinien für die Wohnungsvergabe und Register für Interessenkonflikte, die regelmäßig (z. B. mindestens halbjährlich) überprüft werden. Die Interne Revision prüft, ob die Aktualisierungen die Lehren aus Skandalen im Wohnungswesen und öffentlichen verfügbaren Prüfungsberichten widerspiegeln.

Risikomanagement

A. Rahmenwerk für Verhaltensrisiken – Die Abteilung identifiziert kulturelle Risiken, die sich auf die Erbringung öffentlicher Dienstleistungen auswirken können, wie z. B. Günstlingswirtschaft bei der Wohnungszuweisung, übermäßige Bürokratie oder die Abneigung der Mitarbeiter, behördliche Anordnungen in Frage zu stellen. Die Interne Revision stellt

sicher, dass diese Risiken formell im Risikoregister festgehalten und von der Leitung berücksichtigt werden, und dass bei Bedarf Maßnahmen ergriffen werden.

B. Indikatoren und Analysen – Auf Dashboards werden verhaltensbezogene Daten wie Personalfluktuation, Beschwerden, die Anzahl informeller Beschwerden von Mietern und der Öffentlichkeit sowie die Beantwortung von Anträgen auf Einsicht in öffentliche Unterlagen oder auf Informationsfreiheit erfasst. Die Prüfer beurteilen, ob die Indikatoren und Analysen zuverlässig sind und innerhalb der Behörde diskutiert werden.

C. Abweichungsmanagement – Wenn Abweichungen auftreten (z. B. Hinweisgeberfälle, die eine Abweichung von den Grundsätzen der Fairness zeigen), werden sie an die oberste Führungsebene weitergeleitet. Die Prüfer verifizieren, ob die Abweichungsanalyse zu Abhilfemaßnahmen führt.

D. Einbeziehung von Stakeholdern in die Problemlösung – Die zuständigen Behörden, Wohnungsbaugesellschaften, Gewerkschaften und Bürgergremien werden konsultiert, wenn kulturelle Probleme (z. B. Unhöflichkeit des Personals oder Voreingenommenheit bei der Vergabe) festgestellt werden. Die Prüfer verifizieren, ob das Feedback aus diesen Konsultationen in die Lösungsplanungen einfließt.

Kontrollen

A. Verhaltensrisikoüberprüfungen – Nach dem Scheitern von Wohnungsbauprojekten (z. B. Verzögerungen beim Bau von Sozialwohnungen) werden rückblickende Überprüfungen durchgeführt. Die Prüfer verifizieren, ob verhaltensbedingte Ursachen (wie schlechte Zusammenarbeit, Schuldzuweisungen) beurteilt werden.

B. Festlegung des Tons – Leitende Führungskräfte kommunizieren die Erwartungen in Bezug auf Fairness, Unparteilichkeit und Dienstleistungsqualität durch Town Halls und Intranet-Videos. Interne Revisoren verifizieren, ob diese Erwartungen bekannt sind und umgesetzt werden.

C. Eskalationsmechanismen – Die Abteilung unterhält eine öffentlich zugängliche Hinweisgeber-Hotline und ein Beschwerdeverfahren für Mieter, Mitarbeiter und die allgemeine Öffentlichkeit. Die Prüfer untersuchen die Rechtzeitigkeit, die Vertraulichkeit und den Nachweis, dass Meldungen ohne Vergeltungsmaßnahmen erfolgen.

D. Anreize – Bei der Leistungsbeurteilung werden die Zusammenarbeit der Mitarbeiter, das Engagement der Stakeholder und die Fairness im Umgang mit den Mietern hervorgehoben. Die Prüfer beurteilen, ob diese Verhaltensweisen durch Beförderungen und Auszeichnungen gefördert werden.

E. Überwachung des Verhaltens – Vorgesetzte beurteilen die Mitarbeiter im Rahmen jährlicher Überprüfungen anhand von Verhaltensstandards (Integrität, Empathie gegenüber schutzbedürftigen Mietern). Die Prüfer stellen fest, ob die Ergebnisse konsistent sind und Muster schlechten Verhaltens angegangen werden.

F. Schulungen – Verpflichtende Programme decken unbewusste Voreingenommenheit, Konfliktlösung und ethische Entscheidungsfindung bei der Wohnungsvergabe ab. Die Prüfer verifizieren, ob die Teilnahmequoten hoch sind, und beurteilen die Ergebnisse von Umfragen nach der Schulung.

G. Abhilfemaßnahmen – Wenn kulturelle Verstöße (z. B. Manipulation von Wartelisten) festgestellt werden, werden Ursachenanalysen durchgeführt und Maßnahmenpläne überwacht. Die Prüfer überprüfen, ob die Abhilfemaßnahmen wirksam und nachhaltig sind.

Wichtige Erkenntnis

Die öffentlichen und offiziellen Anweisungen und die Gestaltung der Politik auf hoher Ebene liegen außerhalb des Aufgabenbereichs und der Kontrolle der Internen Revision liegen, aber die Governance-, Risiko- und Kontrollstrukturen der Abteilung in Bezug auf das Verhalten sind prüfbar. Die Anwendung aller 15 Anforderungen im Topical Requirement Verhalten in Organisationen stellt sicher, dass die Internen Revisoren beurteilen können, ob sich das Verhalten in der Organisation auf die Art und Weise auswirkt, wie Wohnungsdienstleistungen erbracht werden, z. B. in einer fairen, transparenten und werteorientierten Weise, ungeachtet des politischen Kontextes.

Fallstudie 2: Kleines Bauunternehmen (mit kleiner Interner Revision)

Die Interne Revision eines fiktiven Bauunternehmens mit 50 Mitarbeitern sieht sich mit der Befürchtung konfrontiert, dass das Topical Requirement Verhalten in Organisationen für große, komplexe Organisationen konzipiert ist. Es gelten jedoch dieselben Grundsätze – nur eben in angepasster Form. Auch ohne einen Unterausschuss des Leitungsorgans oder ausgefeilte Dashboards kann das Unternehmen nachweisen, dass es alle 15 Anforderungen des Topical Requirements erfüllt

Governance

A. Aufgaben und Zuständigkeiten – Die leitende Führungskraft des Unternehmens delegiert die Verantwortung für das Personalwesen formell an den Büroleiter und die Projektaufsicht an die Standortleiter. Interne Revisoren beurteilen, ob die Aufgaben klar sind und Konflikte vermieden werden (z. B. Genehmigung und Überwachung von Ausgaben für Auftragnehmer durch beide).
B. Rechenschaftspflicht – Jeder Manager unterzeichnet vierteljährliche Erklärungen, in denen er die Verantwortung für das Verhalten des Teams, einschließlich der Einhaltung der Sicherheitsvorschriften und der Behandlung von Subunternehmern, bestätigt. Die Prüfer beurteilen, ob diese Erklärungen angemessen sind und überwacht werden.
C. Aufsicht und Überwachung – Das Management trifft sich monatlich, um die Personalfluktuation, Kundenbeschwerden und Sicherheitsberichte für Projekte zu überprüfen. Die Revisoren überprüfen, ob kulturbezogene Probleme angesprochen und verfolgt werden.
D. Richtlinien und Verfahren – Die Prüfer verifizieren, dass schriftliche Verhaltenskodizes, Sicherheitsprotokolle und Richtlinien gegen Mobbing jährlich überprüft und an die Mitarbeiter kommuniziert werden.

Risikomanagement

A. Rahmenwerk für Verhaltensrisiken – Das Unternehmen identifiziert Risiken wie überstürztes Handeln oder Nichteinhaltung der erforderlichen Sicherheitsverfahren zur Einhaltung von Fristen, Günstlingswirtschaft bei der Zuteilung von Überstunden und Belästigung auf Baustellen. Die Revisoren verifizieren, dass diese Risiken in das Risikoregister aufgenommen wurden.

B. Indikatoren und Analysen - Anstelle von Dashboards verwendet das Unternehmen einfache Tabellenkalkulationen zur Überwachung von Abwesenheiten, Beschwerden und Sicherheitsvorfällen. Die Prüfer beurteilen, ob sich daraus Bereiche ergeben, die überprüft werden sollten.

C. Abweichungsmanagement – Wenn Mitarbeiterbefragungen eine Diskrepanz zwischen „erwartetem Respekt“ und „tatsächlicher Erfahrung“ aufzeigen, müssen die Führungskräfte bei der nächsten Sitzung korrigierende Maßnahmen vorstellen. Die Prüfer stellen fest, ob die Maßnahmen umgesetzt und abgeschlossen wurden.

D. Einbeziehung von Stakeholdern in die Problemlösung – Zuständige Behörden, Arbeitnehmervertreter und manchmal auch wichtige Kunden werden aufgefordert, Stellung zu nehmen, wenn kulturelle Probleme auftauchen. Die Prüfer stellen fest, ob die Antwort das erhaltene Feedback widerspiegelt.

Kontrollen

A. Verhaltensrisikoüberprüfungen – Nach jedem Projektmisserfolg (z. B. Kostenüberschreitung aufgrund schlechter Zusammenarbeit) führt die leitende Führungskraft eine „Lessons Learned“-Sitzung durch. Die Prüfer verifizieren, ob die kulturellen Ursachen (Schuldzuweisungen, schlechte Kommunikation) festgehalten und Kontrollen eingeführt wurden, um Handlungen in der Zukunft zu korrigieren.

B. Festlegen des Tons – Die leitende Führungskraft hält vierteljährliche Mitarbeiterbesprechungen ab, um die Werte Fairness, Qualität und Respekt zu stärken. Interne Revisoren holen das Feedback der Mitarbeiter ein, um zu prüfen, ob der Ton angemessen ist.

C. Eskalationsmechanismen – Da es keine formelle Hotline gibt, bieten ein verschlossener Kummerkasten und ein direkter Zugang zur leitenden Führungskraft die Möglichkeit der Meldung. Die Prüfer verifizieren, ob die Mitarbeiter sie nutzen und ob es Richtlinien gegen Vergeltungsmaßnahmen gibt.

D. Anreize – Die Bonuszahlungen sind bescheiden, hängen aber von der Teamarbeit und dem Kundenfeedback ab und nicht nur von der Einhaltung von Projektterminen. Die Revisoren überprüfen, ob die Verteilung der Prämien konsistent und angemessen ist.

E. Überwachung des Verhaltens – Vorgesetzte geben in Leistungsgesprächen informelles Feedback zum Verhalten der Mitarbeiter. Die Prüfer beurteilen, ob das Feedback teamübergreifend einheitlich angewendet wird.

F. Schulung – Jährlich werden kurze Workshops zu den Themen Respekt am Arbeitsplatz und Sicherheit auf der Baustelle durchgeführt. Die Revisoren verifizieren die Teilnahme und die Wirksamkeit durch stichprobenartige Befragungen.

G. Abhilfemaßnahmen – Kommt es zu Mobbing oder Fehlverhalten, untersucht die leitende Führungskraft (oder bei Bedarf eine höhere Instanz) den Fall, dokumentiert ihn und setzt die Ergebnisse durch. Die Revisoren überprüfen, ob die Sanktionen oder korrigierenden Maßnahmen zeitnah und verhältnismäßig sind.

Wichtige Erkenntnis

Auch ohne eine zweite Linie oder einen Unterausschuss des Leitungsorgans kann ein kleines Unternehmen alle 15 Anforderungen des Topical Requirements Verhalten in Organisationen durch reduzierte Mechanismen umsetzen – einfache Register, direkte Aufsicht durch die leitende Füh-

rungskraft, informelle Überprüfungen und angemessene Schulungen. Dies zeigt, dass das Topical Requirement praktikabel und relevant für alle Organisationen ist, unabhängig von ihrer Größe.

Anhang C. Optionales Dokumentationstool

Von Internen Revisorinnen und Revisoren wird erwartet, dass sie mithilfe ihres fachlichen Urteils die Anwendbarkeit der Anforderungen auf der Grundlage der Risikobeurteilung bestimmen und die Ausnahmen von bestimmten Anforderungen angemessen dokumentieren. Das Topical Requirement kann auf der Grundlage des professionellen Urteils der Prüfer im Revisionsplan oder in den Arbeitspapieren zum Auftrag dokumentiert werden. Die Anforderungen können in einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Das nachstehende druckbare Formular bietet eine Möglichkeit, die Einhaltung des Topical Requirements Verhalten in Organisationen zu dokumentieren, seine Verwendung ist aber nicht verbindlich

Verhalten in Organisationen – Governance

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A. Das Leitungs- und Überwachungsorgan beaufsichtigt und die Geschäftsleitung strukturiert die Aufgaben und Verantwortlichkeiten, um unbeabsichtigte Folgen eines falsch ausgerichteten Verhaltens in der Organisation zu vermeiden. Unbeabsichtigte Folgen umfassen Interessenkonflikte oder unklare Entscheidungsprozesse.		
B. Das Leitungs- und Überwachungsorgan beaufsichtigt und die Geschäftsleitung etabliert und unterhält die individuelle und gruppenweite Verantwortlichkeit für Verhaltenserwartungen. Sie stellen sicher, dass die Aufgaben und Verantwortlichkeiten akzeptiert und verstanden werden und konsistent an den strategischen Zielen der Organisation ausgerichtet sind.		
C. Es gibt Governanceprozesse, die eine regelmäßige Überwachung, Bewertung und Überprüfung der Übereinstimmung zwischen Erkenntnissen über das Verhalten und den Zielen der Organisation sowie Maßnahmen bei Fehlentwicklungen gewährleisten.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
D. Richtlinien und Verfahren für den Umgang mit Verhaltensrisiken werden erstellt und regelmäßig auf Relevanz und Richtigkeit überprüft. Diese Richtlinien und Verfahren werden wirksam kommuniziert und in die Abläufe und Entscheidungsprozesse der Organisation integriert.		

Verhalten in Organisationen – Risikomanagement

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A. Die Organisation hat einen Ansatz zum Management von Verhaltensrisiken angemessen definiert, einschließlich der Verhaltensmerkmale, die für die Erreichung der Organisationsziele entscheidend sind.		
B. Die Überwachung des Verhaltens in der Organisation erfolgt angemessen und zeitnah. Die Ergebnisse werden den Stakeholdern kommuniziert.		
C. Lücken zwischen den Verhaltenserwartungen und den tatsächlichen Verhaltensweisen sowie die damit verbundenen Ursachenanalysen werden den Stakeholdern wirksam und konsistent kommuniziert.		
D. Lücken zwischen den Verhaltenserwartungen und den aktuellen Praktiken werden unter Einbeziehung der Stakeholder geschlossen. Diese Lösungen werden bis zu ihrem Abschluss verfolgt und wirksam gemessen, um sicherzustellen, dass ausreichende Maßnahmen ergriffen werden.		

Verhalten in Organisationen - Kontrollen

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A. Die Organisation hat einen Ansatz entwickelt, um Verhaltensmuster zu identifizieren und zu mindern, die innerhalb der Organisation Risiken für die Erreichung der Organisationsziele darstellen können. Beispiele hierfür sind Leistungsüberprüfungen und Überprüfungen der operationellen Risiken mit Schwerpunkt auf dem Verhalten.		
B. Die Organisation gibt einen klaren und einheitlichen Ton bezüglich der erwarteten Verhaltensweisen vor und kommuniziert diese Erwartungen über vertrauenswürdige und zugängliche Kanäle. Es wird ein strukturierter Feedback-Mechanismus unterhalten, um das Verständnis und die Unterstützung der Mitarbeiterinnen und Mitarbeiter zu beurteilen und gegebenenfalls Veränderungen zu ermöglichen.		
C. Es werden Verfahren eingeführt, um die Meldung von Verhalten in der Organisation zu fördern, das dem Erreichen der Organisationsziele entgegensteht. Die Abläufe umfassen Verfahren für Schutz und Lösungen.		
D. Anreizprogramme, einschließlich Vergütung und nicht-monetärer Belohnungen, sind vorhanden, werden kommuniziert und sind mit den Organisationszielen und den regulatorischen Anforderungen abgestimmt. Dazu gehören auch Nachteile und Konsequenzen für unangemessenes Verhalten in der Organisation.		
E. Es gibt ein Verfahren zur Bewältigung von Problemen, einschließlich der Identifizierung und Korrektur von Verhaltensmustern, die nicht mit den Organisationszielen übereinstimmen, und der Eskalation, falls erforderlich.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
F. Es gibt regelmäßige und wirksame Schulungs- und Sensibilisierungsprogramme, die darauf abzielen, die Übereinstimmung zwischen dem Verhalten in der Organisation und den Organisationszielen zu gewährleisten.		
G. Talentakquise und Onboarding-Prozesse richten sich an den Erwartungen für das Verhalten in der Organisation aus und berücksichtigen Verhaltenskompetenzen.		

Anhang D. Abbildung auf das COSO-Rahmenwerk

Die nachstehende Tabelle stellt die Anforderungen an die Governance-, Risikomanagement- und Kontrollprozesse des Topical Requirements Verhalten in Organisationen dem *COSO Internal Control - Integrated Framework (2013)* und dem *COSO Enterprise Risk Management Framework (2017)* gegenüber. Dieser Querverweis ermöglicht es Internen Revisorinnen und Revisoren, ihre COSO-basierten Prüfungshandlungen mit der Abdeckung des Topical Requirements Verhalten in Organisationen abzustimmen.

Anforderungen zur Governance

Anforderung	COSO Internal Control (2013) Referenz	COSO ERM (2017) Referenz
A. Das Leitungs- und Überwachungsorgan beaufsichtigt und die Geschäftsleitung strukturiert die Aufgaben und Verantwortlichkeiten, um unbeabsichtigte Folgen eines falsch ausgerichteten Verhaltens in der Organisation zu vermeiden. Unbeabsichtigte Folgen umfassen Interessenkonflikte oder unklare Entscheidungsprozesse.	Control Environment — Principles 2 (board independence and oversight of escalation channels), 3 (structure, authority, and responsibility).	Governance & Culture — Principles 1 (exercises board risk oversight), 2 (establishes operating structures).
B. Das Leitungs- und Überwachungsorgan beaufsichtigt und die Geschäftsleitung etabliert und unterhält die individuelle und gruppenweite Verantwortlichkeit für Verhaltenserwartungen. Sie stellen sicher, dass die Aufgaben und Verantwortlichkeiten akzeptiert und verstanden werden und konsistent an den strategischen Zielen der Organisation ausgerichtet sind.	Control Environment — Principles 1 (integrity and ethical values), 5 (accountability and performance measures).	Governance & Culture — Principles 4–5 (demonstrates commitment to core values; attracts, develops, and retains capable individuals).
C. Es gibt Governanceprozesse, die eine regelmäßige Überwachung, Bewertung und Überprüfung der Übereinstimmung zwischen Erkenntnissen über das Verhalten und den Zielen der Organisation sowie Maßnahmen bei Fehlentwicklungen gewährleisten.	Monitoring — Principles 16 (ongoing/separate evaluations), 17 (evaluates and communicates deficiencies); Information & Communication — Principles 13 (uses relevant information), 14 (communicates internally), 15 (communicates externally, where relevant).	Governance & Culture — Principle 1 (exercises board risk oversight); Performance — Principles 10–14 (identifies risk, assesses severity, prioritizes risks, implements risk responses); Information, Communication & Reporting — Principles 18–20 (training/awareness reporting).

Anforderung	COSO Internal Control (2013) Referenz	COSO ERM (2017) Referenz
D. Richtlinien und Verfahren für den Umgang mit Verhaltensrisiken werden erstellt und regelmäßig auf Relevanz und Richtigkeit überprüft. Diese Richtlinien und Verfahren werden wirksam kommuniziert und in die Abläufe und Entscheidungsprozesse der Organisation integriert.	Control Activities — Principles 10 (selects and develops control activities), 12 (deploys through policies and procedures).	Review & Revision — Principles 15–17 (assesses change; reviews performance; pursues improvement).

Anforderungen zum Risikomanagement

Anforderung	COSO Internal Control (2013) Referenz	COSO ERM (2017) Referenz
A. Die Organisation hat einen Ansatz zum Management von Verhaltensrisiken angemessen definiert, einschließlich der Verhaltensmerkmale, die für die Erreichung der Organisationsziele entscheidend sind.	Risk Assessment — Principles 6 (specifies suitable objectives), 7 (identifies and analyzes risk), 8 (assesses fraud risk), 9 (identifies and analyzes significant change).	Governance & Culture — Principles 3–5 (demonstrates commitment to core values; attracts, develops, and retains capable individuals); Strategy & Objective-Setting — Principles 6–9 (defines risk appetite, evaluates alternative strategies, considers risk in objectives).
B. Die Überwachung des Verhaltens in der Organisation erfolgt angemessen und zeitnah. Die Ergebnisse werden den Stakeholdern kommuniziert.	Information & Communication — Principles 13 (uses relevant information), 14 (communicates internally); Monitoring — Principles 16 (ongoing/separate evaluations), 17 (evaluates and communicates deficiencies).	Performance — Principles 10–14 (identifies risk, assesses severity, prioritizes risks, implements risk responses); Information, Communication & Reporting — Principles 18–20 (training/awareness reporting).
C. Lücken zwischen den Verhaltenserwartungen und den tatsächlichen Verhaltensweisen sowie die damit verbundenen Ursachenanalysen werden den Stakeholdern wirksam und konsistent kommuniziert.	Information & Communication — Principles 14 (communicates internally), 15 (communicates externally, where relevant).	Information, Communication & Reporting — Principles 19–20 (communicates risk information; reports on risk, culture, and performance).
D. Lücken zwischen den Verhaltenserwartungen und den aktuellen Praktiken werden unter Einbeziehung der Stakeholder geschlossen. Diese Lösungen werden bis zu ihrem Abschluss verfolgt und wirksam gemessen, um sicherzustellen, dass ausreichende Maßnahmen ergriffen werden.	Control Activities — Principles 10 (selects and develops control activities), 12 (deploys through policies and procedures); Monitoring — Principles 16 (ongoing/separate evaluations), 17 (evaluates and communicates deficiencies).	Review & Revision — Principles 15–17 (assesses change; reviews performance; pursues improvement).

Anforderungen zu Kontrollen

Anforderung	COSO Internal Control (2013) Referenz	COSO ERM (2017) Referenz
A. Die Organisation hat einen Ansatz entwickelt, um Verhaltensmuster zu identifizieren und zu mindern, die innerhalb der Organisation Risiken für die Erreichung der Organisationsziele darstellen können. Beispiele hierfür sind Leistungsüberprüfungen und Überprüfungen der operationellen Risiken mit Schwerpunkt auf dem Verhalten.	Risk Assessment — Principles 7 (identifies and analyzes risk), 8 (assesses fraud risk), 9 (identifies and analyzes significant change); Monitoring — Principles 16 (ongoing/separate evaluations), 17 (evaluates and communicates deficiencies).	Performance — Principles 10–14 (identifies risk, assesses severity, prioritizes risks, implements risk responses); Review & Revision — Principles 15–17 (assesses change; reviews performance; pursues improvement).
B. Die Organisation gibt einen klaren und einheitlichen Ton bezüglich der erwarteten Verhaltensweisen vor und kommuniziert diese Erwartungen über vertrauenswürdige und zugängliche Kanäle. Es wird ein strukturierter Feedback-Mechanismus unterhalten, um das Verständnis und die Unterstützung der Mitarbeiterinnen und Mitarbeiter zu beurteilen und gegebenenfalls Veränderungen zu ermöglichen.	Control Environment — Principles 1 (integrity and ethical values), 5 (accountability and performance measures); Information & Communication — Principles 13 (uses relevant information), 14 (communicates internally), 15 (communicates externally, where relevant).	Governance & Culture — Principles 1 (exercises board risk oversight), 4 (demonstrates commitment to core values), 5 (attracts, develops, and retains capable individuals); Information, Communication & Reporting — Principles 18–20 (training/awareness reporting).
C. Es werden Verfahren eingeführt, um die Meldung von Verhalten in der Organisation zu fördern, das dem Erreichen der Organisationsziele entgegensteht. Die Abläufe umfassen Verfahren für Schutz und Lösungen.	Information & Communication — Principle 14 (internal communication channels); Control Environment — Principle 2 (board independence and oversight of escalation channels).	Governance & Culture — Principles 1 (exercises board risk oversight), 4 (demonstrates commitment to core values), 5 (attracts, develops, and retains capable individuals); Information, Communication & Reporting — Principles 19–20 (communicates risk information; reports on risk, culture, and performance).
D. Anreizprogramme, einschließlich Vergütung und nicht-monetärer Belohnungen, sind vorhanden, werden kommuniziert und sind mit den Organisationszielen und den regulatorischen Anforderungen abgestimmt. Dazu gehören auch Nachteile und Konsequenzen für unangemessenes Verhalten in der Organisation.	Control Environment — Principles 1 (integrity and ethical values integrity and ethical values), 5 (accountability and performance measures).	Governance & Culture — Principles 4 (demonstrates commitment to core values), 5 (attracts, develops, and retains capable individuals); Performance — Principles 10–14 (identifies risk, assesses severity, prioritizes risks, implements risk responses).

Anforderung	COSO Internal Control (2013) Referenz	COSO ERM (2017) Referenz
E. Es gibt ein Verfahren zur Bewältigung von Problemen, einschließlich der Identifizierung und Korrektur von Verhaltensmustern, die nicht mit den Organisationszielen übereinstimmen, und der Eskalation, falls erforderlich.	Monitoring — Principles 16 (ongoing/separate evaluations), 17 (evaluates and communicates deficiencies); Information & Communication — Principle 13 (uses relevant information).	Review & Revision — Principles 15–17 (assesses change; reviews performance; pursues improvement); Performance — Principles 10–14 (identifies risk, assesses severity, prioritizes risks, implements risk responses).
F. Es gibt regelmäßige und wirksame Schulungs- und Sensibilisierungsprogramme, die darauf abzielen, die Übereinstimmung zwischen dem Verhalten in der Organisation und den Organisationszielen zu gewährleisten.	Control Environment — Principle 4 (commitment to competence); Information & Communication — Principle 13 (uses relevant information).	Governance & Culture — Principle 5 (attracts, develops, retains capable individuals); Information, Communication & Reporting — Principles 18–20 (training/awareness reporting).
G. Talentakquise und Onboarding-Prozesse richten sich an den Erwartungen für das Verhalten in der Organisation aus und berücksichtigen Verhaltenskompetenzen.	Control Environment — Principles 1 (integrity and ethical values), 4 (commitment to competence).	Governance & Culture — Principle 5 (attracts, develops, retains capable individuals).

Anhang E. Prüfungsaktivitäten, die sich mit dem Verhalten befassen

Interne Revisorinnen und Revisoren können feststellen, dass ihre bereits geleistete Arbeit ihnen bei der Anwendung des Topical Requirements Verhalten in Organisationen hilft. In dieser Tabelle sind einige gezielte Prüfungen und allgemeine Prüfungselemente aufgeführt, die sich mit den Anforderungen in Verbindung bringen lassen und gegebenenfalls zur Feststellung der Einhaltung verwendet werden können. Diese Beispiele sind nicht als verbindliche Prüfungen zu betrachten, sondern sollen vielmehr zeigen, wie allgemein durchgeführte Revisionsaktivitäten eine potenzielle Abdeckung des Topical Requirements ermöglichen können.

Beispiele für Prüfungen und Assurance-Tätigkeiten, die sich direkt/indirekt auf das Verhalten beziehen können, sind:

Bereich	Fokussierte Prüfungen	Allgemeine Elemente von Prüfungshandlungen
Governance	• Risikokultur • Corporate Governance • Überprüfung der Wirksamkeit von Leitungs- und Überwachungsorgan • Regulatorische Reaktion • Anreizvergütung • Leistungsmessung • Unternehmensstrategie und Planung • Planung von Transformationen • Mergers and Acquisitions	• Unternehmensrichtlinien und Verfahren • Kontrollen auf Ebene der Organisations/Management Reviews • Behebung von organisationsweiten regulatorischen Angelegenheiten (z. B. Plan zur Geschäftsverbesserung) • Delegation von Befugnissen
Risikomanagement	• Rechts- und Compliancefunktion • Risikomanagement-Rahmenwerk • Ethik- und Compliance-Programm • Umwelt, Soziales und Governance • Fraud-Überprüfungen und Hinweisgeber-Hotline	• Führung von Risiko- und Kontrollregistern • Selbstbeurteilungen des Managements • Reaktion auf Kontrollversagen und Revisions- oder anderen Feststellungen
Kontrollen	• Personalabteilung (einschließlich Einstellung und Bindung von Personal) • Verkaufsprozesse (einschließlich Verkaufsverhalten und Compliance) • Beschaffung (z. B. Unabhängigkeit der Lieferanten, Einladungen) • Niederlassung/Organisationseinheit (z. B. Management und Überprüfung) • Fraud-/Hinweisgeber-Hotline	• Funktionstrennung • Managementüberprüfung und Überwachung von Kontrollen • Individuelle Fraudrisiken • Kompetenzen, Fähigkeiten und Risikobewusstsein • Abhilfemaßnahmen für Prozesse und Kontrollen

Über das Institute of Internal Auditors

Das IIA ist ein internationaler Berufsverband, der weltweit mehr als 265.000 Mitglieder betreut und mehr als 200.000 Zertifizierungen zum Certified Internal Auditor® (CIA®) vergeben hat. Das IIA wurde 1941 gegründet und ist weltweit als führend für Standards, Zertifizierungen, Ausbildung, Forschung und fachlichen Leitlinien für den Berufsstand der Internen Revision anerkannt. Weitere Informationen finden Sie unter theiia.org.

Haftungsausschluss

Das IIA veröffentlicht dieses Dokument zu Informations- und Bildungszwecken. Dieses Material soll keine endgültigen Antworten auf spezifische individuelle Umstände geben und ist daher nur als Leitlinie gedacht. Das IIA empfiehlt, für jede spezifische Situation unabhängigen Expertenrat einzuholen. Das IIA übernimmt keine Verantwortung, falls sich jemand ausschließlich auf dieses Material verlässt.

Copyright

Dezember 2025, Übersetzung durch DIIR – Deutsches Institut für Interne Revision e.V.

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101

