GLOBAL PERSPECTIVES & INSIGHTS

Governance, Risiko und Kontrolle

Teil I: Risikobereitschaft aus einer nichtfinanziellen Risikoperspektive neu denken

Teil II: Nichtfinanzielle Risiken quantifizieren

Teil III: Wie die digitale Transformation GRC transformiert

The Institute of Internal Auditors

Inhalt

Einführung 4

Die Risikobereitschaft 5

Risikoprofile beeinflussen den Appetit 5

Was ist ein nichtfinanzielles Risiko? 5

Herausforderungen im Zusammenhang mit der Berichterstattung über nichtfinanzielle Risiken 6

Die Rolle der Internen Revision 8

Berücksichtigung nichtfinanzieller Risiken bei der Revisionsplanung 8

Der Wert eines zentralen Fokus: die Erfahrung eines Unternehmens 8

Von Anfang an dabei sein 9

Praktische Anleitung aus *Risk in Focus 2023* 11

Fazit ..... Fehler! Textmarke nicht definiert.

Ein umfassendes Verständnis 12

Einführung 14

Nichtfinanzielle Risiken verstehen 15

Lernen, wie man erkennt und misst 15

Die Bühne bereiten 16

Auf die Quantifizierung hinarbeiten 16

Die Rolle der Internen Revision 18

Zukunftsorientiert bleiben und Kontrollen überwachen 18

Zukunftsorientierte Aufgaben 19

Fazit 20

Einführung 22

Die Diskussion zur digitalen Transformation 2023 23

Das Ausmaß der digitalen Transformation 23

Die Auswirkungen der digitalen Transformation auf GRC 24

Die Interne Revision in der GRC-Diskussion 26

Einen Platz am Tisch behalten 26

Das Risiko der Verbreitung von GRC-Tools 26

Strategien zur Führung und Förderung von Diskussionen 27

Fazit ..... Fehler! Textmarke nicht definiert.

Seien Sie ein aktiver Teil der Revisions-Community 28

Teil 1: Risikobereitschaft aus einer nichtfinanziellen Risikoperspektive neu denken

Über den Experten

W. Scott Page, CIA, CCSA, CRMA, CPA, CA

Scott ist Leiter der Internen Revision bei MDA, Ltd. Mit Sitz in Brampton, Ontario, Kanada, bietet MDA Geointelligenz, Robotik sowie Weltraumoperationen und Satellitensysteme an. Scott verfügt über mehr als 20 Jahre Erfahrung in den Bereichen Verteidigungs- und Raumfahrtfertigung, professionelle Dienstleistungen, Gesundheitswesen, Vertriebsdienstleistungen und Fertigungsindustrie.

Einführung

Das Konzept der Risikobereitschaft – Das Ausmaß des Risikos, das eine Organisation bereit ist, einzugehen, um ihre Ziele zu erreichen, ist von grundlegender Bedeutung für eine effektive Governance in allen Organisationen. Historisch gesehen wurden Entscheidungen über die Risikobereitschaft eines Unternehmens hauptsächlich von finanziellen Risikoüberlegungen bestimmt. Dies ändert sich jedoch angesichts der zunehmenden Konzentration auf nichtfinanzielle Risiken, einschließlich Umwelt-, Sozial- und Governance-Risiken (ESG) und damit verbundener regulatorischer und berichtsrelevanter Überlegungen. Den Risiken im Zusammenhang mit der Art und Weise, wie Organisationen in Bezug auf die Welt um sie herum agieren, wird zunehmend mehr Aufmerksamkeit geschenkt.

Die Bewertung dieser Risiken im Rahmen der Risikobereitschaft ist ein Bereich, in dem Interne Revisoren sinnvolle Beiträge leisten können. Dieser Global Knowledge Brief, der erste Teil einer dreiteiligen Reihe zu Governance, Risiko und Kontrolle (GRC) des IIA, untersucht im Detail dieses Thema, die Herausforderungen beim Überdenken der Risikobereitschaft unter Berücksichtigung nichtfinanzieller Risiken und die wichtige Rolle der Internen Revision in diesem Prozess.

Die Risikobereitschaft

Risiken und Chancen in Einklang bringen

Risikoprofile beeinflussen den Appetit

Die Internationalen Grundlagen für die berufliche Praxis (IPPF) des IIA definieren die Risikobereitschaft einfach als „das Ausmaß des Risikos, das eine Organisation bereit ist zu akzeptieren." In der Praxis stellt die Risikobereitschaft, auch Risikotoleranz genannt, ein Gleichgewicht zwischen den potenziellen Vorteilen von Innovationen und den Bedrohungen dar, die Veränderungen unweigerlich mit sich bringen. Daher ist die Risikobereitschaft für jedes Unternehmen einzigartig und hängt von einer Reihe von Faktoren ab, wie zum Beispiel:

Kultur — Aufgrund langjähriger Richtlinien, Einstellungen oder anderer Faktoren kann die Organisation in ihrem Umgang mit Risiken mehr oder weniger offensiv vorgehen.

Branche — Der Umfang der Regulierung oder andere Compliance-Aspekte können beispielsweise einen Einfluss darauf haben, wie risikoscheu das Unternehmen ist.

Markt — Das Ausmaß des Wettbewerbs, dem ein Unternehmen ausgesetzt ist, oder die Stabilität des Marktes sind Faktoren, die die Risikoentscheidung beeinflussen können.

Finanzielle Stärke - Ein Unternehmen, das weniger Vertrauen in seine Finanzlage hat, ist möglicherweise risikoaverser. [1]

Nichtfinanzielle Risiken
(unvollständige Liste)

- Operations
- Compliance
- Strategie
- Dienstleister
- Cybersecurity
- Soziale Verantwortung
- Reputation
- Datenschutz
- Datenintegrität
- Schutz geistigen Eigentums
- Vergütung
- Mitarbeiterverhalten
- Arbeitsmanagement
- Ethische und Unternehmenskultur
- Öffentliche Gesundheit
- Diversity, Gleichbehandlung und Inklusion
- Menschenrechte
- Personal
- Umwelt:
  - Treibhausgasemissionen
  - Abfallmanagement
  - Rohstoffquellen
  - Zugriff auf und Management von natürlichen Ressourcen
  - Klimawandel

Was ist ein nichtfinanzielles Risiko?

Die Einbeziehung nichtfinanzieller Risiken in Diskussionen über die Risikobereitschaft beginnt mit dem Verständnis, was diese umfassen. Tatsächlich erhöht die schiere Anzahl der Risiken, die in diese Kategorie fallen (siehe nebenstehende Liste), die Wahrscheinlichkeit, dass einige übersehen oder missverstanden werden. Dies unterstreicht, wie wichtig es ist, nichtfinanzielle Risiken in jede Diskussion über die Risikobereitschaft einzubeziehen. Über die bloße Einbeziehung hinaus müssen Organisationen jedoch auch darauf vorbereitet sein, auf diese nichtfinanziellen Elemente zu reagieren und die Informationen zu ermitteln, die zur Bewältigung von Risiken in verschiedenen Geschäftsprozessen auf Unternehmensebene erforderlich sind.

[1] Jean-Gregoire Manoukian, "Risk Appetite and Risk Tolerance: What's the Difference?", Wolters Kluwer, September 29, 2016, https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference#:~:text=Risk%20Appetite%20Is%20the%20General%20Level%20of%20Risk%20You%20Accept&text=Because%20determining%20risk%20appetite%20will,risk%20you%20need%20to%20manage.

Herausforderungen im Zusammenhang mit der Berichterstattung über nichtfinanzielle Risiken

Berichterstattung

Mehr als 60 % der CAEs bei börsennotierten Organisationen hielten das Risikoniveau im Bereich Nachhaltigkeit/nichtfinanzielle Berichterstattung für moderat, hoch oder sehr hoch *(2023 North American Pulse of Internal Audit des IIA)*.[2] Tatsächlich arbeiten viele Unternehmen daran, Nachhaltigkeits-/nichtfinanzielle Themen zu messen und darüber zu berichten. Beispielsweise veröffentlichen insgesamt 96 % der im S&P 500 und 81 % im Russell 1000 gelisteten Unternehmen Nachhaltigkeitsberichte.[3]

Eine Herausforderung für Organisationen in diesem Bereich besteht darin, dass viele nichtfinanzielle Risiken schwer zu messen sind. Beispiele hierfür sind Inklusion, ethisches Verhalten, Unternehmenskultur und die Umweltauswirkungen des Handelns des Unternehmens sowie seiner Lieferanten und Geschäftspartner.[4] Ein damit verbundenes Problem besteht in möglichen Folgen, wenn Organisationen sich bei der Aggregation oder Berichterstattung nichtfinanzieller Informationen auf falsche oder irreführende Indikatoren oder Rahmenwerke verlassen.

Derzeit gibt es keine endgültigen, weltweit anerkannten Standards für die nichtfinanzielle Berichterstattung und Offenlegung. Das kann zu einem Mangel an konsistenter und vergleichbarer Berichterstattung führen. Stattdessen haben Organisationen im Allgemeinen die Möglichkeit, je nach Bedarf bestimmte Richtlinien auszuwählen, verschiedene Richtlinien zusammenzustellen oder die Berichterstattung vollständig abzulehnen. Tatsächlich hat das Center for Sustainable Organizations eine Liste von 23 nichtfinanziellen Mess- und Berichterstattungsstandards und -rahmen zusammengestellt, die viele unterschiedlicher Zielgruppen, Leistungskonstrukte und primärer Messformate abdecken.[5]

Es zeichnet sich jedoch eine Reihe allgemein akzeptierter Berichtsstandards ab. Eine wichtige Entwicklung war die Gründung des International Sustainability Standards Board (ISSB) durch die International Financial Reporting Standards Foundation (IFRS). Es konsolidiert die bestehende Value Reporting Foundation und das Climate Disclosure Standards Board und hat die Verantwortung für das Integrated Reporting Framework übernommen. Dies alles ist Teil der Bemühungen, eine umfassende globale Grundlage für die Offenlegung von Nachhaltigkeit für die Kapitalmärkte zu schaffen. Ziel ist es, den Anforderungen an eine qualitativ hochwertige, transparente, verlässliche und vergleichbare Berichterstattung von Unternehmen zu Klima- und anderen ESG-Themen gerecht zu werden. Das ISSB gab bekannt, dass seine ersten Standards zur Klima- und Nachhaltigkeitsberichterstattung gegen Ende des zweiten Quartals 2023 veröffentlicht werden.

Regulatorisch

Nach Angaben des World Business Council for Sustainable Development (WBCSD) gibt es derzeit mehr als 2.000 obligatorische und freiwillige ESG-Berichtsanforderungen und Ressourcen aus mehr als 70 Ländern. Dies allein stellt eine gewaltige Herausforderung für Organisationen dar, die versuchen, die obligatorische und freiwillige nichtfinanzielle Berichterstattung und die damit verbundenen Risiken zu verstehen.

Die Europäische Union (EU) hat bei der verpflichtenden Offenlegung nichtfinanzieller Risiken eine Vorreiterrolle übernommen. Seit 2014 verpflichtet die Richtlinie zur nichtfinanziellen Berichterstattung (NFRD) große Unternehmen von öffentlichem Interesse mit Sitz in der EU und mehr als 500 Mitarbeitern (ca. 11.700), Informationen zu Umweltbelangen, sozialen Belangen, der Behandlung von Mitarbeitern, der Achtung der Menschenrechte usw. zu veröffentlichen. Anti-Korruption und Bestechung sowie Diversität in Unternehmensvorständen (in Bezug auf Alter, Geschlecht, Bildung und beruflichen Hintergrund) und andere Themen.

Im Januar 2023 trat die Corporate Sustainability Reporting Directive (CSRD) der EU in Kraft. Sie aktualisiert die Regeln für die Sozial- und Umweltberichterstattung im Rahmen der NFRD und erhöht die Zahl der Unternehmen, die Bericht erstatten müssen (ca. 50.000). Unternehmen müssen die neuen Regeln erstmals im Geschäftsjahr 2024 für Berichte anwenden, die im Jahr 2025 veröffentlicht werden. Bis dahin gelten die NFRD-Berichtsregeln.[6]

---

[2] *2023 North American Pulse of Internal Audit* , The IIA, 2023, https://www.theiia.org/globalassets/site/content/research/pulse/2023/2023-Pulse-of-Internal-Audit.pdf .

[3] *2022 S&P 500 and Russell 1000 Sustainability Reporting in Focus*, Governance & Accountability Institute Inc., 2022, https://www.ga-institute.com/research/ga-research-directory/sustainability-reporting-trends/2022-sustainability-reporting-in-focus.html#:~:text=All%2DTime%20High%20of%20Sustainability,and%2081%25%20of%20Russell%201000.

[4] *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA,, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

[5] „Non-Financial Measurement & Reporting Standards & Frameworks", Center for Sustainable Organizations, 2023, https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf .

[6] "Corporate Sustainability Reporting," European Commission, accessed March 2023, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.

In den USA hat die Securities and Exchange Commission (SEC) vorgeschlagen, von den Unternehmen zu verlangen, dass sie in ihren Registrierungserklärungen und regelmäßigen Berichten Offenlegungen im Zusammenhang mit dem Klima und der Cybersicherheit angeben. Es wird erwartet, dass die SEC im Jahr 2023 endgültige Regeln zu beiden Bereichen bekannt gibt. Obwohl private Unternehmen von Anforderungen der SEC ausgenommen sind, könnten sie den Druck von Interessengruppen verspüren, ähnliche Offenlegungen vorzunehmen.

Greenwashing

Neben mangelnder Vergleichbarkeit und Transparenz in der Berichterstattung kann auch die Vertrauenswürdigkeit zum Problem werden, wenn Unternehmen bei der Festlegung von Zielen zu optimistische Annahmen treffen oder Daten falsch darstellen, um ein positiveres Bild zu vermitteln. In Europa fanden nationale Verbraucherschutzeinrichtungen Grund zu der Annahme, dass 42 % der umweltfreundlichen Behauptungen von Unternehmen übertrieben, falsch oder irreführend waren. Diese als Greenwashing bezeichneten Praktiken können dem Ruf von Organisationen schaden. Die daraus resultierenden Auswirkungen auf die Kundenzufriedenheit mit einem Unternehmen und seinen Produkten oder Dienstleistungen können den Gewinn je Aktie und die Kapitalrendite beeinflussen.[7]

Darüber hinaus können laut IIA „ohne eine begründete ESG-Risikomanagementstrategie, die auf einem klaren Verständnis der Probleme aufbaut, schlecht erstellte Nachhaltigkeitsberichte schnell mit der Einhaltung gesetzlicher Vorschriften in Konflikt geraten und die Erwartungen der Anleger verfehlen.“[8]

42

PROZENTSATZ DER UMWELTFREUNDLICHEN ANGABEN VON UNTERNEHMEN, DIE ALS ÜBERTRIEBEN, FALSCH ODER IRREFÜHREND EINGESTUFT WERDEN.

Quelle: Harvard Business Review, *“How Greenwashing Affects the Bottom Line”*

Unternehmen, die sich zum ersten Mal mit nichtfinanziellen Daten auseinandersetzen, müssen neue Leistungs- und andere Kennzahlen sowie geeignete Richtlinien, Prozesse und interne Kontrollmaßnahmen entwickeln, um verlässliche Informationen für die Entscheidungsfindung zu generieren und die Qualität der erzeugten und berichteten Daten sicherzustellen.

[7] Ioannis Ioannou, George Kassinis, and Giorgos Papagiannakis, “How Greenwashing Affects the Bottom Line,” July 21, 2022, Harvard Business Review, https://hbr.org/2022/07/how-greenwashing-affects-the-bottom-line.

[8] *Internal Audit’s Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

Die Rolle der Internen Revision

Prüfungss- und Beratungsdienstleistungen

Berücksichtigung nichtfinanzieller Risiken bei der Revisionsplanung

Interne Revisoren planen ihre Prüfungen auf der Grundlage der Risikobereitschaft der Gesamtorganisation und der geprüften Bereiche. Der Internen Revision wird häufig die Aufgabe übertragen, unabhängig Prüfungssicherheit über die Wirksamkeit des Rahmenwerkes für die Risikobereitschaft einer Organisation zu liefern. Der zunehmende Fokus von Regulierungsbehörden und Stakeholdern auf Nachhaltigkeit und andere nichtfinanzielle Themen erfordert, dass Revisionsleitungen die damit verbundenen Risiken berücksichtigen, die eine Bedrohung für die Organisation darstellen können. Dazu gehört auch, dass sie verstehen, wie sie in die Aktivitäten und Strategien des Unternehmens passen, und wissen, welche Abteilungen die Aufsicht über die damit verbundenen Praktiken haben. Revisionsleitungen sollten auch das Bewusstsein für nichtfinanzielle Risiken beim Überwachungsorgan und der Geschäftsleitung schärfen.

Eine Schlüsselaufgabe der Internen Revision wird darin bestehen, ein geeignetes Kontrollumfeld für nichtfinanzielle Risiken festzustellen, mit dem relevante Maßnahmen überwacht werden können und verhindert wird, dass eine Organisation aufgrund schlecht konzipierter Kontrollen und Systeme ungültige und irreführende Informationen berichtet. Kompetente Interne Revisionen verfügen über die erforderlichen Fähigkeiten und Erfahrungen, um wirksame nichtfinanzielle Kontrollumgebungen zu unterstützen, einschließlich Schulungs- und Beratungsleistungen. Die ilterne Revision kann Ratschläge zu Rahmenwerken oder Standards geben, die die Organisation nutzen kann, um nichtfinanzielle Risiken zu managen, zu mindern und möglicherweise darüber zu berichten. Die Interne Revision kann auch Ratschläge zu den nützlichsten Berichtskennzahlen geben, einschließlich neuer Indikatoren zur Erfassung sowohl quantitativer als auch qualitativer Daten, die nichtfinanzielle Risiken zutreffend darstellen.

Die Daten deuten darauf hin, dass Nachhaltigkeit und nichtfinanzielle Überlegungen langsam Einzug in die Routine der Internen Revision halten. Dem Pulse-Bericht zufolge gaben 22 % der Befragten an, dass sie Nachhaltigkeitsaspekte generell in ihre Prüfungen einbeziehen. Spezifische Prüfungen der Nachhaltigkeits-/nichtfinanziellen Berichterstattung machten jedoch nur knapp 2 % der Aufwände im Revisionsplan aus.[9]

Der Wert eines zentralen Fokus: die Erfahrung eines Unternehmens

Die Schaffung der richtigen Grundlage ist ein wichtiger Faktor bei der Einbeziehung nichtfinanzieller Risiken in die Risikobereitschaft.

Als Scott Page als Leiter der Internen Revision zu MDA, Ltd. kam, hatte jeder Geschäftsbereich seinen eigenen Risikomanagementprozess. Das Unternehmen war aber an einem zentralisierten Ansatz interessiert. Um diese Zentralisierung zu erreichen, war ein ganzheitlicher und integrierter Ansatz von entscheidender Bedeutung. Um Informationen zusammenzuführen, hat das in Kanada ansässige Unternehmen, das Dienstleistungen in den Bereichen Robotik, Satellitensysteme und Geointelligenz anbietet, ein vielseitiges Softwaretool für den Bewertungsprozess eingeführt. Das Tool kann von verschiedenen Teams verwendet werden, einschließlich der Internen Revision bei Kontrolltests und der IT bei der Bewertung von Cyber- und Dienstleisterrisiken.

Risikoinformationen und -kontrollen werden somit unternehmensweit geteilt. Das Tool sammelt Details zu allen Risiken, die sich auf die Strategie oder Ziele auswirken könnten, um zu sehen, wie sie sich auf die Fähigkeit des Unternehmens auswirken könnten, seine kurzfristigen Ziele und seinen langfristigen strategischen Plan zu erreichen. „Wir wollten alle Risikoüberlegungen in einer einzigen Informationsquelle zusammenfassen“, sagte Page. „Es hilft uns zu verstehen, wie das, was wir tun, mit allen anderen zusammenhängt.“

Risiken im Zusammenhang mit internen Kontrollen, Finanzberichten, Operations, IT und Dienstleistern wurden mit aktuellen Ansätzen bereits gut erfasst. Jedoch hat die Organisation auch damit begonnen, ESG- und andere nichtfinanzielle Risiken zu berücksichtigen. Die Verwendung

[9] *2023 North American Pulse of Internal Audit* , The IIA.

desselben Tools zur Konsolidierung dieser zusätzlichen Risiken bedeutet, dass „Sie immer darüber informiert sind, was in anderen Bereichen vor sich geht“, sagte Page.

Auch wenn die Identifizierung, Bilanzierung und Prüfung nichtfinanzieller Risiken kompliziert sein kann, hat MDA durch seinen zentralisierten Fokus einen soliden Ausgangspunkt geschaffen. Unter anderem möchte das Unternehmen ESG nicht als Silo betrachten, da die damit verbundenen nichtfinanziellen Risiken so viele Bereiche betreffen.

Die Zentralisierung ermöglicht die Verwendung einer gemeinsamen Sprache, die im gesamten Unternehmen und von den Stakeholdern verstanden werden kann, sagte Page. Zusammen mit Führungskräften der Enterprise Risk Management (ERM)-Gruppe definiert er Risiken und wie sie auf einer Skala von 1 bis 5 bewertet werden sollten. Risikoinformationen können einmal gesammelt und im gesamten Unternehmen genutzt werden, wodurch die Effizienz in der Internen Revision und anderswo gesteigert wird. Eine Versionskontrolle wird gewährleistet. Mithilfe dieser gemeinsamen Sprache verstehen Geschäftsleitung und Überwachungsorgan, wenn die Interne Revision oder andere Teams ein Risiko als höchste Priorität (Kategorie 5) und nicht als weniger dringende Priorität (Kategorie 1) einstufen.

Eine ständige Überlegung ist die Prüfbarkeit nichtfinanzieller Informationen, da es, wie bereits erwähnt, keine allgemein anerkannten Berichtsstandards gibt. Bis sich dies ändert, kann die Interne Revision Ratschläge dazu geben, auf welche Kontrollen, Prozesse und Informationen eine Organisation vorbereitet sein muss.

Die Quantifizierung der Zahlen stellt eine weitere Herausforderung dar, da möglicherweise keine Daten verfügbar sind und es möglicherweise schwierig ist, vergleichbare Daten zu erhalten. Bei MDA beispielsweise gibt es kaum Treibhausgasemissionen, ein häufiges ESG-Problem. Es arbeitet jedoch mit vielen externen Anbietern und Beratern zusammen, und diese Partner könnten Emissionen verursachen oder andere Schritte unternehmen, die MDA berücksichtigen muss. Bei der Entwicklung der Säulen seines nichtfinanziellen Risikoprogramms identifiziert MDA diese Partner, überlegt, wie die damit verbundenen Risiken gemessen werden können, entscheidet, wie sie am besten geprüft werden können, und entwickelt dann ein umfassenderes Verständnis darüber, was Dienstleisterrisiken und andere nichtfinanzielle Risiken für das Unternehmen bedeuten.

Laut der Pulse-Umfrage des IIA sind Beziehungen zu Drittparteien der drittgrößte Risikobereich (nach Cybersicherheit und IT), wobei die Prüfungshäufigkeit für Beziehungen zu Drittparteien im Vergleich zum Risikoniveau relativ gering ist.

Auch wenn sich MDA noch in einem frühen Stadium der Identifizierung von Bereichen potenzieller nichtfinanzieller Risiken befindet, hat der bisherige Prozess deutlich gemacht, welche Auswirkungen diese auf die Fähigkeit des Unternehmens, seine Strategien umzusetzen, sowie auf die öffentliche Wahrnehmung des Unternehmens haben könnten. Der Prozess werde der Geschäftsleitung und der Öffentlichkeit auch mehr Informationen für die Entscheidungsfindung liefern, sagte Page. „Wir haben ein umfassenderes Verständnis sowohl der finanziellen als auch der nichtfinanziellen Risiken und wissen, wie wir sie kontrollieren müssen“, erklärte er.

Von Anfang an dabei sein

Interne Revisoren sollten das Management und die Überwachungsorgane darauf aufmerksam machen, wie wichtig es ist, die Interne Revision von Anfang an einzubeziehen, insbesondere wenn es um ein neues Konzept wie das nichtfinanzielle Risiko geht. „Wenn die Interne Revision im Vorfeld einbezogen wird, sind die Erfolgsaussichten später größer“, sagte Page. „Warum sollte ein Unternehmen seine ESG- oder nichtfinanziellen Pläne oder Prozesse einführen und dann später die Interne Revision hinzuziehen und damit verbundene Probleme erst aufzeigen, sobald sie umgesetzt sind?“

Um die Unabhängigkeit zu wahren, kann die Interne Revision nicht Entscheidungen für ein Unternehmen treffen. Sie kann aber Erkenntnisse darüber liefern, wie man am besten mit der Betrachtung nichtfinanzieller Risiken beginnt und welche Ansätze funktionieren könnten und welche nicht. „Wir können ein Geschäftspartner mit Mehrwert sein“, sagte er.

Page hat herausgefunden, dass das Knüpfen von Kontakten im gesamten Unternehmen eine gute Möglichkeit ist, die Bereiche, die sein Team prüfen wird, besser zu verstehen. Page kontaktiert regelmäßig Personen in wichtigen Geschäftsfunktionen und bittet um ein 15-minütiges Treffen bei einem Kaffee – und er ermutigt seine Mitarbeiter, dasselbe zu tun. „Niemand hat jemals Nein gesagt“, sagte er. „Sie sind alle leidenschaftlich dabei und lieben, was sie tun.“

„Was mich als Revisionsleiter beschäftigt, ist: Was weiß ich nicht?“ fügt Page hinzu. „Das kann man nur herausfinden, indem man mit Menschen spricht.“ Zu den Prüfungen seines Teams gehören Gespräche mit Mitarbeitern des geprüften Bereichs. Er hält sich auch über die Arbeit

des ERM-Teams des Unternehmens auf dem Laufenden, obwohl die Interne Revision über einen eigenen unabhängigen Risikobewertungsprozess verfügt.

Die Vernetzung mit seinen Kollegen in Branchen- oder Fachausschüssen hilft auch dabei festzustellen, ob sein Risikomanagementansatz aktuell und so gründlich wie möglich ist. Dieses Hintergrundwissen wird besonders wichtig für nichtfinanzielle oder ESG-Informationen sein, da sich diese Risiken ständig weiterentwickeln.

Page und sein Team gehen aus ihren Gesprächen mit einem besseren Verständnis hervor und sie sind daher besser aufgestellt, wenn es darum geht, einen Bereich zu prüfen. Das wird besonders nützlich sein, um die neuen Grenzen der nichtfinanziellen Daten zu verstehen. MDA umfasst drei separate Geschäftsbereiche, sodass die Interne Revision auch erfolgreiche Praktiken anderer Teams teilen und unnötige Doppelarbeit erkennen kann. „Geschäftssinn führt zu viel größerem Erfolg“, sagte Page. Auch Interne Revisoren können einen Mehrwert schaffen, indem sie den Status Quo hinterfragen, bestehende Praktiken in Frage stellen und Richtlinien entwickeln, die ein besseres Verständnis und eine bessere Identifizierung nichtfinanzieller Informationen ermöglichen.

Praktische Anleitung aus *Risk in Focus 2023*

Risk in Focus 2023, der jüngste jährliche Risikobericht, der von Instituten in der European Confederation of Institutes of Internal Auditing (ECIIA) erstellt wurde, befasst sich mit verschiedenen nichtfinanziellen Risikobereichen, darunter makroökonomische und geopolitische Risiken. Ein Roundtable-Gespräch mit Revisionsleitungen befasste sich mit der Neubewertung globaler Risiken, insbesondere da der Konflikt in der Ukraine Risiken in verschiedenen Bereichen, einschließlich der Stabilität der globalen Energiesysteme, verschärft hat. Ein Teilnehmer am runden Tisch, Ken Marnoch, Executive Vice President für Interne Revision und Investigations bei Shell International, sagte, er und sein Team führten „härtere Gespräche über die Risikobereitschaft".

Aus *„Risk in Focus 2023"* :

> „[Marnoch] sagt, dass es in einem Dilemma am nützlichsten ist, ein klares Verständnis darüber zu haben, wie viel Risiko jedes Unternehmen in bestimmten Bereichen eingehen kann – wenn alle Entscheidungen potenzielle Vor- und Nachteile haben können. Dann kann Klarheit über die Risikobereitschaft, die mit den verschiedenen Entscheidungen verbunden ist, als Orientierungshilfe bei der Bewältigung des Problems dienen.
>
> In der Vergangenheit konzentrierte sich die Interne Revision von Shell auf betriebliche, kulturelle und verhaltensbezogene Risiken. Die Interne Revision hat nun ein spezielles Team zusammengestellt, das sich auf die Risiken und den Kontrollrahmen im Zusammenhang mit der Erreichung strategischer Ziele konzentriert.
>
> „Wenn Sie strategische Ziele auf messbare Ziele, die damit verbundenen Risiken, die expliziten Kontrollen und ein Verständnis dafür herunterbrechen, wie Unternehmensleiter wissen, dass die Kontrollen funktionieren, dann haben Sie Spielraum für eine interne Revision", sagt er. „Zu den Aufgaben des neuen Teams gehört es, den Menschen dabei zu helfen, sich vom starren Denken über die Richtigkeit von Annahmen zu lösen, die sie zu Beginn eines Projekts oder einer Strategie getroffen haben, während sich so vieles in der Welt dramatisch verändert." Um sich in einer ungewissen Zukunft zurechtzufinden, muss man aktiv neugierig sein, Informationen finden, die Überzeugungen auf die Probe stellen, und schnelles Feedback zur aktuellen Realität geben.
>
> „Wenn Sie das Bedürfnis, Recht zu haben, loslassen und anerkennen, dass die Entscheidung zu diesem Zeitpunkt auf der Grundlage der besten Informationen getroffen wurde, sind Sie offener für die Suche nach Informationen, die Ihr Denken herausfordern." Das eröffnet viel mehr Möglichkeiten bei der Bewältigung eines Schlüsselrisikos bei der Umsetzung Ihrer strategischen Ziele."[10]

„Risk in Focus 2023" enthält eine Liste von Fragen, die die Interne Revision bei der Bewertung des Organisationsrisikos verwenden kann:

1. Wie ist die Interne Revision im Hinblick auf den Zeit- und Arbeitsaufwand für ihre Aufgaben auf die strategischen Ziele der Organisation ausgerichtet – einschließlich derjenigen, die geopolitische Risiken und den Klimawandel betreffen?
2. Wie stark ist die Unterstützung für die Aktivitäten der Internen Revision in Bereichen wie Strategie und Krisenmanagement und was kann getan werden, um diese Unterstützung dort zu verbessern, wo sie fehlt?
3. Inwieweit ist die Interne Revision in der Lage, Ressourcen anderer Bereiche zu nutzen, um eine angemessene Abdeckung zu gewährleisten und Doppelarbeit zu minimieren?
4. Woher wissen Sie, ob die Annahmen der Organisation (und der Internen Revision) über die Hauptrisikobereiche heute noch gültig sind und zu den Umständen passen, die im Jahr 2023 voraussichtlich eintreten werden?
5. Verfügt die Organisation über aktuelle Risikobewertungen für das Sanktionsrisiko und über robuste Kontrollen zur Überprüfung von Drittbeteiligungen und Unternehmensaktionären?
6. Inwieweit nutzt die Organisation digitale Tools, um Schlüsselrisiken zu modellieren und „Was-wäre-wenn"-Szenarien durchzuführen?
7. Haben Sie die Beziehung zwischen den Geschäftsfortführungs-, Krisenmanagement- und Risikomanagementteams der Organisation neu bewertet, um sicherzustellen, dass sie ihren Zweck erfüllen?
8. Berücksichtigt die Organisation kritische Stimmen und die externer Experten bei der Risikobewertung ernsthaft?

[10] *Risk in Focus 2023: More Risky, Uncertain, and Volatile Times Ahead,* European Confederation of Institutes of Internal Auditing, 2022, https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/.

Fazit

Ein umfassendes Verständnis

Es ist wichtig zu verstehen, dass nichtfinanzielle Risiken erhebliche finanzielle Auswirkungen auf ein Unternehmen haben können, einschließlich seiner ERM-Bemühungen. Um der Unternehmensführung zu helfen, nichtfinanzielle Risiken zu verstehen und zu bewältigen, können Revisionsleitungen ihr umfassendes Verständnis der vielen Facetten – und Bedrohungen – des Unternehmens nutzen. Die Unternehmensleitung kann so wertvolle Einblicke in diese Risiken gewinnen und wird bei der Festlegung der Risikobereitschaft der Organisation unterstützt, um dies Risiken angemessen zu berücksichtigen und anzugehen.

Teil 2 : Quantifizierung nichtfinanzieller Risiken

Über den Experten

Anishka Collie, CIA, CPA

Anishka Collie, CIA, CPA, ist CEO und Principal Consultant bei ATC Financial Advisors & Consultants in Nassau, Bahamas. Sie verfügt über mehr als 20 Jahre Erfahrung in den Bereichen externe Prüfung, Interne Revision und Corporate Governance, Unternehmensrisikomanagement und interne Kontrollen sowie in den Bereichen Finanzplanung, Beratung, Sanierung von Finanzprozessen und Überprüfung von Geschäftsprozessen. Sie konzentriert sich auf Kunden in der Finanzdienstleistungsbranche und hat bei zahlreichen Schulungen zur Buchhaltung und Wirtschaftsprüfung Vorträge gehalten.

Hassan NK Khayal, CIA, MBA, CRMA, CFE

Hassan NK Khayal, CIA, MBA, CRMA, CFE, ist Manager der Internen Revision bei Scope Investment in Dubai. Im Internal Auditor, einer weltweiten Publikation des IIA, wurde er als einer der Top 15 unter 30 aufstrebenden Führungskräften weltweit und als aufgehender Stern der Internen Revisions vorgestellt. Er promoviert derzeit in Betriebswirtschaftslehre an der Katholischen Universität in Murcia, Spanien. Zusätzlich zu seinen Abschlüssen verfügt er auch über Berufszertifizierungen in den Bereichen Robotics Process Automation, Qualitätsmanagement, Health and Safety, Umweltmanagement und Risikomanagement.

Jason Minard, CIA, CISA, CPA (inaktiv)

Jason Minard, CIA, CISA, CPA (inaktiv), ist Senior Vice President und Senior Manager für Supervisory Controls and Analytics bei Wells Fargo Advisors in St. Louis, Missouri, USA. Mit über 25 Jahren Erfahrung in der Wertpapierbranche und Wirtschaftsprüfung hat er Prüfungen in Bereichen wie Investmentverkäufe, Einhaltung gesetzlicher Vorschriften, Wertpapiergeschäfte, Investmentbanking, Vermögensverwaltung, Treuhandverwaltung und Finanzen durchgeführt und geleitet. Er hat einen Bachelor-Abschluss in Betriebswirtschaft von der St. Louis University und verfügt über die Lizenzen als General Securities Representative und General Sales Supervisor.

Einführung

Management-Guru Peter Drucker wird oft mit den Worten zitiert: „Was du nicht messen kannst, kannst du nicht lenken.“ Tatsächlich haben Unternehmen schon lange erkannt, wie wichtig es ist, finanzielle Risiken zu quantifizieren und zu messen. Der neue Trend der letzten Jahre war das zunehmende Interesse an nichtfinanziellen Risiken, einschließlich Umwelt-, Sozial- und Governance-Risiken (ESG), und damit verbundenen regulatorischen und berichtsrelevanten Überlegungen. Die Herausforderung bestand darin, etwas zu messen, das oft keinen leicht erkennbaren monetären Wert hat. Dies ist eine Herausforderung, die Unternehmen überwinden müssen, da nichtfinanzielle Risiken durchaus finanzielle Auswirkungen haben können.

Dieser Global Knowledge Brief, der zweite Teil einer dreiteiligen Reihe zu Governance, Risiko und Kontrolle (GRC), untersucht die Herausforderungen bei der Quantifizierung nichtfinanzieller Risiken, wie Unternehmen diese angehen und die wichtige Rolle, die die Interne Revision spielt, um dazu beizutragen, das Verständnis in diesem Bereich voranzutreiben.

Nichtfinanzielle Risiken verstehen

Unzählige potenzielle Bedrohungen

Lernen, wie man erkennt und misst

Generell gelten nichtfinanzielle Risiken als solche, die sich aus den Auswirkungen einer Organisation auf die Welt und umgekehrt aus den Auswirkungen der Welt auf die Organisation ergeben. Die unvollständige Liste (siehe Kasten) spiegelt viele, aber nicht alle, des breiten Spektrums nichtfinanzieller Risiken wider, denen Organisationen ausgesetzt sein können. Die Definitionen dieser Risiken sind oft inkonsistent oder unklar, was die Erkennung und Messung schwierig macht.

Allerdings bestehen auch nichtfinanzielle Risiken bei reinen Finanztransaktionen. Betrachtet man beispielsweise das Kreditrisiko bei einem Kredit über 50.000 US-Dollar, sind der Kreditwert und der potenzielle Anfangsverlust klar. Andererseits umfasst das nichtfinanzielle Risiko für diese Transaktion Überlegungen wie den Zeit- und Arbeitsaufwand für die Bewältigung eines möglichen Kreditausfalls, bemerkte Anishka Collie, CIA, CPA, CEO und Hauptberaterin bei ATC Financial Advisors & Consultants, Nassau Bahamas, wo sie ausgelagerte Risiko- und Revisionsdienste anbietet. Wenn es sich um einen erheblichen Kredit handelt oder dieser Teil eines Musters notleidender Kredite ist, muss die Organisation möglicherweise auch tiefer graben, um zu verstehen, ob die Unternehmenskultur, die verfügbare Dokumentation und die internen Kontrollen oder das aktuelle Schulungsniveau geeignet sind, das Kreditrisiko zu mindern und gute Kreditentscheidungen zu gewährleisten.

Da nichtfinanzielle Risiken schwer zu quantifizieren sein können, besteht ein damit verbundenes Risiko darin, dass die Berichterstattung und Offenlegung nichtfinanzieller Risiken einer Organisation unzuverlässig ist. Beispielsweise kann die Erreichung bestimmter Nachhaltigkeitsziele als absichtlich überhöht angesehen werden oder Probleme beim Erreichen dieser Ziele werden unterschätzt, eine Praxis, die im Zusammenhang mit ESG-Themen als „Greenwashing“ bezeichnet wird. „Greenwashing kann beabsichtigt sein oder einfach aufgrund des relativ geringen Reifegrads der derzeit verfügbaren Standards für die nichtfinanzielle Berichterstattung erfolgen“, bemerkte ein Prüfungsleiter bei einem Roundtable-Gespräch der European Confederation of Institutes of Internal Auditing (ECIIA).[11] Derzeit ist die Berichterstattung möglicherweise inkonsistent oder schwierig zu vergleichen, da es keine weltweit anerkannten Standards für die Berichterstattung und Offenlegung nichtfinanzieller Informationen gibt. Darüber hinaus stehen verschiedene Rahmenwerke oder Standards zur Verfügung, was es für Unternehmen möglicherweise schwierig macht, zu bestimmen, welche Richtlinien sie befolgen und wie sie diese anwenden sollen, insbesondere weil sie oft teilweise oder in Kombination mit Regeln aus einem anderen Standard oder Rahmenwerk verwendet werden. Das Center for Sustainable Organizations hat eine Liste von 23 nichtfinanziellen Mess- und Berichterstattungsstandards und -rahmen zusammengestellt, die auf zahlreichen unterschiedlichen Leistungskennzahlen basieren und auf unterschiedliche Arten von Organisationen abzielen.[12]

Nichtfinanzielle Risiken (unvollständige Liste)

- Operations
- Compliance
- Strategie
- Dienstleister
- Cybersecurity
- Soziale Verantwortung
- Reputation
- Datenschutz
- Datenintegrität
- Schutz geistigen Eigentums
- Vergütung
- Mitarbeiterverhalten
- Arbeitsmanagement
- Ethische und Unternehmenskultur
- Öffentliche Gesundheit
- Diversity, Gleichbehandlung und Inklusion
- Menschenrechte
- Personal
- Umwelt:
  - Treibhausgasemissionen
  - Abfallmanagement
  - Rohstoffquellen
  - Zugriff auf und Management von natürlichen Ressourcen
  - Klimawandel

[11] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.
[12] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf.

Die Bühne bereiten

Organisationen sollten proaktiv darüber nachdenken, wie sie nichtfinanzielle Risiken quantifizieren können. Viele tun dies jedoch nicht. Der Umgang mit finanziellen Risiken korreliert mit dem Hauptziel einer Organisation – der Maximierung des Aktionärsvermögens und der Steigerung der Einnahmen. Bei der Bewältigung nichtfinanzieller Risiken werden Unternehmen aufgefordert, Geld für Maßnahmen auszugeben, deren Wert schwer zu verstehen ist und die nicht sofort zum Umsatz beitragen. „Solange Sie die Auswirkungen des Risikos nicht quantifizieren und finanziell beziffern können, ist es unwahrscheinlich, dass Sie die erforderliche Zustimmung des Managements zur Bewältigung des Risikos erhalten", so PwC.[13]

Eine weitere Hürde besteht darin, dass Kontrollfunktionen für nichtfinanzielle Risiken im gesamten Unternehmen silohaft sein können. Da diese Risiken so vielfältig sind, unterliegen sie häufig der Aufsicht einer Vielzahl unterschiedlicher Teams. Jedes Team verfügt möglicherweise über einen eigenen Risikoidentifizierungsprozess, eine eigene Berichtsstruktur und sogar über unterschiedliche IT-Systeme im Zusammenhang mit nichtfinanziellen Risiken. „Die gleichen Personen, sei es die Interne Revision, Compliance oder ein anderer Bereich, werden aufgefordert, dasselbe Verfahren immer und immer wieder durchzuführen", sagte Hassan NK Khayal, CIA, MBA, CRMA, CFE, Revisionsmanager bei Scope Investment in Dubai. Der zusätzliche Aufwand dieser Doppelarbeit macht es wahrscheinlicher, dass das Management Investitionen in Informationsbeschaffung und Quantifizierungsbemühungen zurücknimmt.

Allerdings senken vorbeugende Maßnahmen die Sanierungskosten und schützen die Marke und die Geschäftsbeziehungen des Unternehmens. In den meisten Organisationen seien die Risikoberichtsmethoden noch nicht ausgereift oder präzise genug, um dem Management überzeugende Argumente zu liefern, sagte Khayal. Bei richtiger Auswahl können die richtigen Indikatoren jedoch nichtfinanzielle Risiken erfassen und genau quantifizieren und dem Management den richtigen Kontext bieten, um ihre potenziellen Auswirkungen zu erfassen.

Durch die proaktive Identifizierung potenzieller nichtfinanzieller Bedrohungen vor ihrem Eintritt ist es einfacher, sie zu verstehen und zu quantifizieren. In der Lebensmittel- und Getränkeindustrie lässt sich beispielsweise das finanzielle Risiko leicht quantifizieren, wenn eine bestimmte Menge an Lebensmitteln verdorben ist. Allerdings sei es schwieriger, die damit verbundenen Gesundheits- und Sicherheitskosten und -risiken zu berechnen, bemerkte Khayal. Durch die Berücksichtigung dieser Risiken kann ein Unternehmen proaktive, vorbereitende Maßnahmen ergreifen, wie z. B. die Verbesserung der Sauberkeit, um ein Restaurant attraktiver zu machen und die Wahrscheinlichkeit zu verringern, dass Kunden krank werden. Auch in der Baubranche sinkt die Zahl der Unfälle typischerweise, wenn Sicherheitsingenieure die Gesundheits- und Sicherheitsvorschriften strenger überwachen und durchsetzen.

„Jeder Vorfall bringt seine eigenen Kosten mit sich", sagte Khayal, seien es die direkten Kosten für die Bewältigung des Ereignisses und etwaiger damit verbundener Verletzungen oder die Kosten für damit verbundene Verzögerungen. „In dem Moment, in dem das Risiko eingetreten ist, ist es bereits zu spät", stellte er fest, und der Ruf und die Beziehungen der Organisation sind bereits geschädigt, möglicherweise mit dauerhaften oder erheblichen Auswirkungen. Wenn Unternehmen jedoch die Kosten potenzieller Risikoereignisse bewerten, ist es wahrscheinlicher, dass sie den Wert vorbeugender Maßnahmen erkennen.

Khayal glaubt, dass nichtfinanzielle Risiken größere Auswirkungen haben können als finanzielle. Ihre Auswirkungen können dazu führen, dass Stakeholder wie Aktionäre, Mitarbeiter und Kunden das Geschäftsmodell oder die Praktiken eines Unternehmens in Frage stellen, wenn es zu Reputationsschäden kommt. „All dies setzt Unternehmen erheblich unter Druck, nichtfinanzielle Risiken zu bewältigen", sagte er.

Auf die Quantifizierung hinarbeiten

Obwohl nichtfinanzielle Risiken keinen direkten monetären Wert haben, ist es möglich, ihnen numerische Werte zuzuordnen. Der Schlüssel besteht darin, die Risiken und deren Umfang zu definieren und dann konkrete Überlegungen zur Messung zu finden. Bei der Bewältigung des Kundenrisikos ist es beispielsweise möglich, Faktoren wie die Anzahl der Kundenbeschwerden, die damit verbundenen Standorte oder Situationen, damit verbundene Kundenverluste, Rückgänge bei Neukunden und die Trends zu ermitteln, die diese Daten im Laufe der Zeit offenbaren.

Wenn es keine konkreten Kriterien zur Messung gibt, besteht eine Möglichkeit darin, die Risiken so zu kategorisieren, dass sie möglichst beschreibend und aussagekräftig sind, beispielsweise ob sie auf hohem, mittlerem oder niedrigem Niveau liegen. Wenn beispielsweise ein

[13] "Taking Control: How to Get on top of Non-Financial Risks," Christopher Eaton and David O'Brien, PwC Channel Islands, March 9, 2021.

Compliance- und Regulierungsrisiko besteht, könnten Unternehmen versuchen, das Risiko zu quantifizieren, indem sie die Bandbreite potenzieller Erkenntnisse einer Aufsichtsbehörde in jeder Risikokategorie ermitteln. Durch die Kategorisierung der Ergebnisse erhalten Unternehmen einen Rahmen für die weitere Bewertung jedes Risikos und die Festlegung von Prioritäten.

Ein organisierter Ratingrahmen ist eine weitere Option, die es ermöglicht, Erkenntnisse zu einer Reihe nichtfinanzieller Risiken zu erfassen. Interne Revisionen verwenden möglicherweise ein Bewertungsrahmenwerk, das Beobachtungen bewertet, die von der Internen Revision und anderen Teams gemacht wurden, z. B. Compliance, Risiko, Informationssicherheit oder Recht, die ungeminderte Risiken identifizieren und diese verfolgen, melden oder beheben. Das Rahmenwerk kann verwendet werden, um die Auswirkungen nichtfinanzieller Risiken zu bewerten und deren Quantifizierung zu unterstützen. Ein Beispiel für die Art von Rahmenwerken, die Unternehmen nutzen könnten, um die finanziellen Auswirkungen ihrer Nachhaltigkeitsmaßnahmen besser zu verstehen und zu kommunizieren, ist der United Nations Global Compact and Principles for Responsible Investment Value Driver Model.

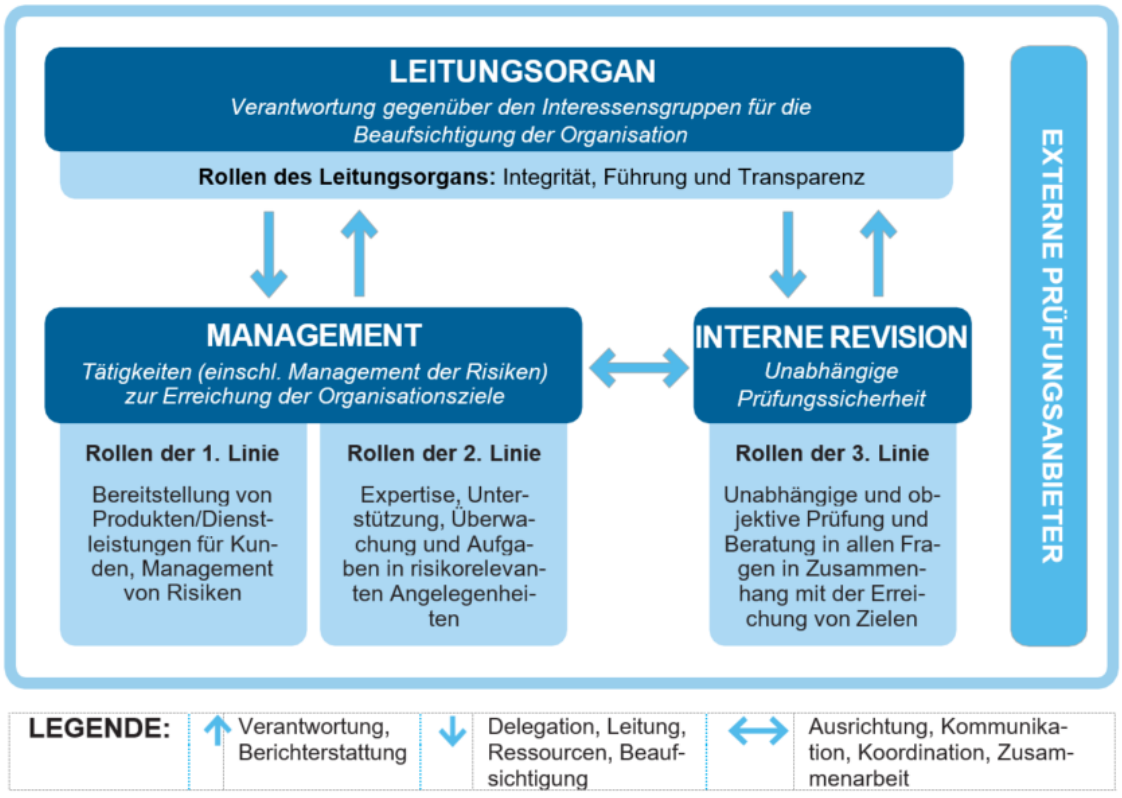
Die Rolle der Internen Revision

„Pioniere“ des nichtfinanziellen Risikos

Zukunftsorientiert bleiben und Kontrollen überwachen

Während Unternehmen an der Quantifizierung arbeiten, besteht die Rolle der Internen Revision darin, strategisch vorzugehen und sich auf die besten Möglichkeiten zur Wertschöpfung zu konzentrieren, so wie im Drei-Linien-Modell des IIA beschrieben (siehe Abbildung 1). Um dieses Ziel zu erreichen, sollten sich Interne Revisoren nicht auf die Analyse von Aussagen und finanziellen Risiken beschränken, sondern vielmehr Vorreiter bei der Bewältigung nichtfinanzieller Risiken sein, indem sie einen risikobasierten Ansatz verfolgen und stets die Zukunft im Blick haben, sagte Khayal. „Idealerweise sollten wir eine der zukunftsorientierteren Abteilungen der Organisation sein“, sagte er. „Wir sollten uns auf zukünftige Risiken konzentrieren, bevor das Management, das die täglichen Auswirkungen im Auge hat, sich ihrer überhaupt bewusst wird.“ Um die Unabhängigkeit zu wahren, definiert die Interne Revision nicht die Risikokategorien oder -definitionen, die die Organisation verwendet, sondern hinterfragt nichtfinanzielle Risikorichtlinien und deren Umsetzung im Einklang mit dem gesamten Risikobewertungsprozess.

Abbildung 1: Das Drei-Linien-Modell



Als Berater ähnelt Collies Rolle stark der eines Internen Revisors und sie kann von Prüfern übernommen werden, wenn es um nichtfinanzielle Risiken geht. Zu Beginn spricht sie mit den Führungskräften der Organisation, darunter nicht nur dem CEO und CFO, sondern auch den Leitern der Bereiche Compliance, Risiko und Interne Revision. Das Ziel besteht darin, ihre Risikodefinitionen für die Organisation zu verstehen, wie

sie Risiken identifizieren und auf welchem Detaillierungsgrad und welche Kontrollen vorhanden sind. Während dieser Diskussionen gelangten die Teilnehmer häufig zu einem neuen Verständnis des Risikos und seiner Auswirkungen, sagte Collie.

Diese ersten Gespräche sind auf hohem Niveau, um zu verstehen, was für den effektiven Betrieb der Organisation erforderlich ist. Der nächste Schritt besteht darin, mit Managern oder Abteilungsleitern zu sprechen, um mehr über den Tagesablauf und mögliche Risiken zu erfahren. Mit diesem Verständnis kann der Prüfer mit Mitarbeitern auf dieser Ebene ein Brainstorming durchführen, um herauszufinden, welche Risikomanagementschritte bereits erfolgreich waren oder fehlgeschlagen sind und wo Schwachstellen im Risikomanagement bestehen. So wie Berater Erfahrungen mit einer Vielzahl von Organisationen vorweisen können, verfügen Interne Revisoren über ganzheitliche Kenntnisse in vielen Bereichen der Organisation. „Sie können Dinge an die Oberfläche bringen, an die diese Teams vielleicht nicht gedacht haben“, sagte Collie.

Prüfer benötigen neue Fähigkeiten, um den Prozess zu moderieren. Bei herkömmlichen Revisionsansätzen geht es darum, Risiken in Bezug auf Kontrollen, Daten und Dokumente zu identifizieren. Die Zusammenarbeit mit Kunden zur Identifizierung und zum Verständnis nichtfinanzieller Risiken erfordert zusätzliche Fähigkeiten und fortlaufende Schulungen im Zusammenhang mit Interviews oder der Moderation einer Brainstorming-Sitzung, sagte Collie. „Eigentlich ist es eine völlig andere Aufgabe, Kunden dabei zu helfen, Risiken zu erkennen“, sagte sie. Die Führung muss in diese Ausbildung investieren, um sicherzustellen, dass die Organisation effektiv und effizient arbeitet.

Die Interne Revision kann auch den Wert und die Zuverlässigkeit bestehender wichtiger Leistungsindikatoren und -metriken bewerten, wenn sie auf nichtfinanzielle Risiken angewendet werden, sowie neue Maßnahmen, die speziell für nichtfinanzielle Risiken und damit verbundene Kontrollen und Risikomanagementprozesse entwickelt wurden. Um dem Vorwurf des Greenwashing vorzubeugen, kann sie laut ECIIA sicherstellen, dass die mit den Interessengruppen geteilten Daten ein faires und genaues Bild der Unternehmensanstrengungen zeichnen.[14]

Khayal baut seinen Prüfungsplan und seine Risikobewertung auf den vielen Risikoelementen auf, die sich auf die Fähigkeit einer Organisation auswirken können, sowohl finanzielle als auch nichtfinanzielle Strategien umzusetzen. Wenn beispielsweise die Unternehmensstrategie und die Wertschöpfung von strengen Lieferkettenpraktiken abhängen, dann sei die Beschaffung immer ein zentrales Anliegen, sagte er. Durch die Kartierung von Risiken und insbesondere nichtfinanziellen Risiken können Bedrohungen wie Bonitätsprobleme von Kunden, Probleme in der Lieferkette und Herausforderungen im Bereich der Cybersicherheit aufgedeckt werden.

Während Organisationen ihre Rahmenwerke ausbauen und die von ihnen verwendeten Definitionen verfeinern, schaffen sie eine gemeinsame Sprache über nichtfinanzielle Risiken. Dies verbessert die Kommunikation über Risiken zwischen der ersten, zweiten und dritten Linie, klärt die Verantwortlichkeiten jeder Linie und ermöglicht jedem, seine eigenen Verfeinerungen zu den gemeinsam genutzten Definitionen hinzuzufügen.

Zukunftsorientierte Aufgaben

In Khayals Organisation muss jeder, der an Kontrollen und Risiko-Selbstbeurteilungen beteiligt ist einen detaillierten Risikoschulungskurs absolvieren, der auch nichtfinanzielle Risiken einschließt. Er ermutigt seine Mitarbeiter außerdem, sich auf drei Hauptaufgaben zu konzentrieren:

- **Bleiben Sie auf dem Laufenden** . Interne Revisoren müssen über die neuesten weltweiten und lokalen Ereignisse auf dem Laufenden bleiben, um Vorfälle besser zu verstehen, die sich jetzt, kurz- oder langfristig auf das Risiko auswirken könnten.
- **Bleiben Sie über neue Technologien auf dem Laufenden.** Khayal ist davon überzeugt, dass die Revisoren der Zukunft und die Organisationen, für die sie arbeiten, über IT-Kenntnisse verfügen müssen. Prüfer können sich nicht mehr ausschließlich auf traditionelle Methoden verlassen, sondern müssen Technologietools integrieren. „Die Welt verändert sich immer schneller“, sagte er. Ohne robuste Technologie „werden Unternehmen nicht in der Lage sein, mitzuhalten, insbesondere da immer mehr makroökonomische Faktoren, mit denen wir konfrontiert sind, nichtfinanzieller Natur sind.“
- **Bleiben Sie im Einklang mit der Strategie, Mission und Vision der Organisation.** Bei Prüfungsplänen muss berücksichtigt werden, welche Risiken am wichtigsten sind und wie diese am besten quantifiziert werden können. Da Unternehmen im Allgemeinen nicht alle Arten von Risiken berücksichtigen können, denen sie ausgesetzt sind, müssen Prüfer verschiedene Faktoren berücksichtigen, um die Risiken zu identifizieren und zu quantifizieren, die wahrscheinlich die größte Bedeutung und Auswirkung haben.

[14] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

Fazit

Als vertrauenswürdige Berater der Organisation sind Interne Revisoren in der einzigartigen Position, ein besseres Verständnis von und bessere Erkenntnisse über nichtfinanzielle Risiken zu fördern. Sie können dies tun, indem sie ihr vorhandenes umfassendes Wissen über das Unternehmen nutzen, neue Kompetenzen erwerben und sich für eine Änderung der organisatorischen Perspektive einsetzen, die bestimmt, wie nichtfinanzielle Risiken am besten quantifiziert werden können.

Teil 3 : Wie die digitale Transformation GRC verändert

Über die Experten

Sarah Kuhn, CIA, CCSA, CRMA

Sarah Kuhn ist eine sehr erfahrene Expertin im Bereich der Internen Revision. Mit über 20 Jahren Mitgliedschaft im Institute of Internal Auditors (IIA) und einer früheren Präsidentschaft des Tulsa Chapters hat sie ihr Engagement für die Branche durch Erfahrung in Abteilungsschulungen, Berichterstattung und Einhaltung von Standards sowie in der Leitung von Prüfungen unter Beweis gestellt Das Team konzentrierte sich auf Datenanalysen und Automation. Sarah ist aktuell auch im IIA Houston Chapter aktiv.

Audra Nariunaite, CIA, CISA, CFE, CHC, CHPC

Audra Nariunaite ist eine Compliance- und Audit-Expertin mit branchenübergreifender Erfahrung und einer nachgewiesenen Fähigkeit, Wachstum und Exzellenz durch strategische Initiativen und Prozessumgestaltung voranzutreiben. Derzeit ist sie Vorstandsmitglied des IIA Northeast Florida Chapter und Mitglied des IIA Litauen. Audra ist derzeit Director of Compliance bei der globalen Beschäftigungsplattform Oyster HR.

Einführung

Kein Trend wirkt sich wohl stärker auf die Governance-, Risiko- und Compliance-Landschaft (GRC) aus als der Anstieg der Nutzung von Technologien im täglichen Geschäftsbetrieb – und es ist leicht zu verstehen, warum. Die Vorteile der digitalen Transformation sind nicht zu unterschätzen, da Tools, die aus diesem Trend hervorgehen, mittlerweile in nahezu allen großen Branchen zur Automatisierung und Beschleunigung von Prozessen eingesetzt werden, sodass GRC- und Sicherheitsabläufe potenzielle Risiken und Probleme schnell erkennen und darauf reagieren können.

Beispielsweise kann die KI-gestützte Verarbeitung natürlicher Sprache mit ihrer Fähigkeit, unstrukturierte Datenquellen von E-Mails bis hin zu Social-Media-Feeds zu analysieren, mit den Fähigkeiten und Erfahrungen menschlicher GRC-Teams kombiniert werden. Die KI stellt Ressourcen für das Risiko- und Compliance-Management auf einem so hohen Niveau von Perfektion und Komplexität bereit, wie es noch vor einer Generation nicht vorstellbar war.

Während die Notwendigkeit, sich einer derart radikalen digitalen Transformation zu unterziehen, früher möglicherweise als Luxus galt, bietet die heutige Risikolandschaft Unternehmen kaum Spielraum für eine Verzögerung der Einführung. Cyberbedrohungen nehmen von Tag zu Tag an Umfang und Komplexität zu. Das Rohvolumen der produzierten, gesammelten und verarbeiteten Daten wächst weiterhin mit atemberaubender Geschwindigkeit, was zu immer größeren Datenschutzrisiken führt. Und die Regulierungslandschaft entwickelt sich weiterhin rasant weiter, um mit der Geschwindigkeit der heutigen Risiken Schritt zu halten. Ohne die Vorteile, die die digitale Transformation bietet, könnten GRC-Funktionen in der heutigen Welt durchaus auf verlorenem Posten stehen.

Als Teil 3 der Global Knowledge Brief-Reihe des IIA zu GRC befasst sich dieser letzte Teil damit, wie sich GRC-Systeme durch die Integration neuer Technologien weiterentwickeln und welche inhärenten Risiken mit der digitalen Transformation verbunden sind. In diesem Brief wird auch darauf eingegangen, welchen Platz die Interne Revision in diesen Diskussionen einnimmt und wie sie Organisationen am besten auf diesem wichtigen Weg unterstützen kann.

Die Diskussion zur digitalen Transformation 2023

Ein belastetes Risiko verstehen

Das Ausmaß der digitalen Transformation

Die Explosion der digitalen Transformation, die während der COVID-19-Pandemie beobachtet werden konnte, wütet weiterhin, und ihre Entwicklung nimmt in gewisser Weise an Geschwindigkeit zu. Dies geschah nicht nur aufgrund des grundsätzlichen Wunsches, Gewinne und Effizienz zu steigern, um sich einen Wettbewerbsvorteil auf dem Markt zu verschaffen, sondern auch aufgrund des Bestrebens, mit der umfangreichen Liste aufkommender Risiken, die in den letzten Jahren entstanden sind, Schritt zu halten (oder ihnen im Idealfall einen Schritt voraus zu sein). Inflation, geopolitische Spannungen wie der Ukraine-Konflikt, der Streit zwischen China und Taiwan, weit verbreitete wirtschaftliche Unsicherheit aufgrund von Ereignissen wie der plötzlichen Schließung großer Bankinstitute, laufende Diskussionen über ESG-Risiken und damit verbundene Änderungen in der Regulierungslandschaft, Unterbrechung von oder Engpässe bei Lieferketten – das sind nur einige der Formen, die das Risiko im Jahr 2023 angenommen hat. Aus der Sicht von Organisationen, deren Aufgabe darin besteht, eine gewisse Prüfungssicherheit anzubieten, wird eine umfassende Einführung der digitalen Transformation als wirksame Lösung angesehen. Tatsächlich sagen laut einem aktuellen Bericht von Gartner 89 % der Vorstandsmitglieder, dass das digitale Geschäft mittlerweile in allen Unternehmenswachstumsstrategien verankert ist, auch wenn nur 35 % sagen, dass sie die Ziele der digitalen Transformation erreicht haben oder auf dem richtigen Weg sind.

„Geschäftsleitungen und Überwachungsorgane haben einen Punkt erreicht, an dem die digitale Geschäftsstrategie und die allgemeine Geschäftsstrategie ein und dasselbe sind“, sagte Jorge Lopez, Vizepräsident und angesehener Analyst bei Gartner, in dem Bericht. „Obwohl CIOs bei der Nutzung von Technologie für operative Exzellenz erhebliche Fortschritte gemacht haben, reicht dies nicht aus, um die strategischen Geschäftsvorteile zu realisieren, die Geschäftsleitungen und Überwachungsorgane von digitalen Investitionen erwarten.“[15]

Wie die digitale Transformation aussieht, ist von Standort zu Standort, von Branche zu Branche und von Organisation zu Organisation unterschiedlich. Was für eine Organisation effektiv oder sogar erreichbar ist, ist für eine andere möglicherweise nicht ideal. Dennoch gibt es einige grundlegende Ähnlichkeiten zwischen Organisationen, die irgendeine Form der digitalen Transformation anstreben. „[Bei der digitalen Transformation] geht es um mehr als nur Technologie“, sagte Chintan Shah, CEO und Gründer von Brainvire , in einem Artikel für *Forbes* . „Es geht um den Wandel in der Denkweise, der es Unternehmen ermöglicht, ihre Geschäftsmodelle und Prozesse neu zu überdenken, um die Chancen zu nutzen, die neue Technologien bieten.“[16]

Lopez äußerte eine ähnliche Meinung. „Da Unternehmen zunehmend in einer Welt ständiger Störungen agieren, denken die zukunftsfähigsten Geschäftsleitungen und Überwachungsorgane darüber nach, wie Umbrüche und Risiken als Quelle von Chancen dienen können. CEOs und CIOs müssen diese Denkweise übernehmen, da Technologie eine immer wichtigere Rolle für den Geschäftserfolg spielt.“

Eine solche Neuinterpretation kann viele Formen annehmen, unter anderem:

- Künstliche Intelligenz (KI), maschinelles Lernen und die Einführung natürlicher Sprachverarbeitung.
- Robotic Process Automation (RPA).
- Fokus auf Cybersicherheit und Datenschutz.
- Cloud-Migration.

15. “Gartner Says 89% of Board Directors Say Digital Is Embedded in All Business Growth Strategies,” press release, Gartner, Oct. 29, 2022, https://www.gartner.com/en/newsroom/press-releases/2022-10-19-gartner-says-89-percent-of-board-directors-say-digital-is-embedded-in-all-business-growth-strategies.

16. Chintan Shah, “Businesses Need to Watch these Digital Transformation Trends in 2023,” Forbes, Jan. 27, 2023, https://www.forbes.com/sites/forbestech-council/2023/01/27/businesses-need-to-watch-these-digital-transformation-trends-in-2023/?sh=7147b04a185d.

- Datenanalyse.
- 5G-Einführung und digitale Optimierung.
- Blockchain.
- Virtuelle geschäftliche Zusammenarbeit.
- Konsumentendatenplattformen.

Die Auswirkungen der digitalen Transformation auf GRC

Bei so vielen Konnotationen und Anwendungen hat die digitale Transformation eindeutig tiefgreifende Auswirkungen auf die GRC-Funktionen gehabt. In vielen Fällen hatten Unternehmen Schwierigkeiten, ein angemessenes Maß an GRC-Abdeckung aufrechtzuerhalten, während die Veränderungen in der Technologielandschaft weiterhin rasant voranschreiten. Eine aktuelle Umfrage von Risk.net in Zusammenarbeit mit IBM unter GRC-Experten im Finanzdienstleistungssektor ergab einige alarmierende Trends, darunter:

- 62 % glauben, dass ihre digitale Transformation Lücken in bestehenden GRC-Prozessen aufgedeckt hat, und fast die Hälfte der Befragten (45 %) ist der Meinung, dass ihre Organisationen jetzt „aufholen". Nur 37 % gaben an, vor der Umstellung Zeit und Ressourcen in ihre digitale Transformation investiert zu haben.
- 77 % glauben, dass die Risiken ihrer Unternehmen gestiegen sind, da sie stärker auf digitale Kanäle angewiesen sind.[17]

Darüber hinaus nannten 56 % in derselben Studie auf die Frage, welche Risiken aufgrund der Trends der digitalen Transformation in ihrem Unternehmen eine größere Bedeutung erlangten, Informations-/Datensicherheit, 48 % gaben Verstöße gegen die Cybersicherheit an, 32 % nannten Risiken Dritter/Lieferkette und 31 % nannten das Compliancerisiko.

Um effektiv zu bleiben, mussten die GRC-Funktionen modernisiert werden, indem sie entscheidende Schritte zur Bewältigung der digitalen Transformation unternehmen, sonst riskierten sie, ihre Organisationen erheblichen Risiken auszusetzen. Zu diesen Schritten gehören:

- Zuweisung oder Rekrutierung neuer Ressourcen.
- Einführung einer Art Hybrid-Cloud-Datenspeichermodell für erweiterte Datenanalyseanwendungen.
- Aktualisierung aktueller GRC-Tools und -Funktionen.
- Einsatz fortschrittlicher Technologie, einschließlich KI-bezogener Tools und Automatisierungssysteme.

Während einige dieser Maßnahmen einigermaßen offensichtlich erscheinen mögen, sind sie aufgrund der Geschwindigkeit, mit der sich die aktuelle Risikolandschaft entwickelt, alles andere als offensichtlich. Beispielsweise verließen sich Organisationen in der Vergangenheit auf die Einhaltung bestimmter Leitlinien oder eines Rahmenwerks aus Standards, Zertifizierungen und/oder Vorschriften, um eine Grundlage bewährter Kontrollen und Prozesse zu schaffen, die eine GRC-Funktion auf Erfolg ausrichten.

Heutzutage kann ein solcher Ansatz jedoch schnell komplex werden. Dies kann folgende Ursachen haben:

- Die schnelle Entwicklung neuer oder aktualisierter Rahmenwerke, die eine schnelle Konformität erfordern. Beispiele hierfür sind die rasche Schaffung verschiedener vorgeschlagener Regulierungsinitiativen in der EU im Zusammenhang mit der digitalen Strategie, darunter der Data Conformance Act, der Digital Markets Act, der Digital Services Act, der Data Act und der AI Act, die alle bis Ende des Jahres 2023 beschlossen werden sollen.
- Ein Mangel an Klarheit oder Anleitung durch die aktuellen Rahmenwerke, der dazu führt, dass Organisationen – zumindest zeitweise – auf sich allein gestellt sind.

„Da Systeme wie ChatGPT und Bing Chat auf den Markt kommen und CoPilot sich derzeit auf die Veröffentlichung vorbereitet, müssen viele Unternehmen schnell handeln, da Mitarbeiter bereits einige dieser Technologien nutzen, um Aufgaben zu erledigen", sagte Sarah Kuhn, eine bekannte Leiterin einer Internen Revision mit mehr als zwei Jahrzehnten Berufserfahrung. „Es gibt einige Organisationen, die sie vollständig

[17] "Digital Transformation and the Future of GRC," Risk.net, IBM, Feb. 2022, https://www.ibm.com/downloads/cas/WWQXRPLG.

blockieren, während andere mit Teams, die besser in der Lage sind, die Technologien zu verstehen, intern detailliertere Richtlinien darüber erstellen, wie und wann sie eingesetzt werden sollten."

Teams, die mit der Entwicklung von Strategien zur Erstellung solcher Richtlinien beauftragt sind, variieren je nach Organisation in ihrer Zusammensetzung, können aber Parteien wie den Chief Digital and Information Officer, IT- und Risikomanagementteams sowie Rechts- und Finanzgruppen umfassen. Sobald sie jedoch erstellt sind, sind Strategien zur Kommunikation und Durchsetzung der Richtlinien ebenso wichtig. „Unternehmen können bis zu einem gewissen Grad nach einem Ehrenkodex arbeiten", sagte Kuhn, „aber es sind auch formellere Maßnahmen zur Kommunikation sich entwickelnder Richtlinien erforderlich." Wenn ein Mitarbeiter beispielsweise eine bestimmte Adresse eingibt, kann ein Programm implementiert werden, das in seinem Browser ein Banner anzeigt, das ihn an die Unternehmensrichtlinien erinnert."

Um eine solche Leistung so reibungslos zu vollbringen, müsste laut Kuhn eine agile, anpassungsfähige GRC-Funktion vorhanden sein, bevor neue Technologien wie ChatGPT in die Risikolandschaft des Unternehmens eindringen. Nicht jede Organisation wird den Segen einer solchen Weitsicht haben, sei es aufgrund begrenzter Ressourcen, begrenzter oder schlechter Qualität verfügbarer Daten, der Priorisierung anderer Probleme oder einfacher Fahrlässigkeit. Unabhängig von den Gründen muss die interne Revision bereit sein, die Initiative zu ergreifen, um die GRC-Funktionen schnell in eine geeignete Position zu bringen, um in dieser neuen Ära erfolgreich zu sein.

Die Interne Revision in der GRC-Diskussion

Verbesserung von GRC im Kontext der digitalen Transformation

Einen Platz am Tisch behalten

Die Interne Revision kann effektives GRC auf verschiedene Weise unterstützen , insbesondere in Organisationen, die bei der Aktualisierung ihrer GRC-Funktionen im Rückstand sind.

Erstens können nur wenige Veränderungen, die es wert sind, angestrebt zu werden, ohne ein gewisses Maß an Investitionen erreicht werden. Solche Investitionen können jedoch schwierig sein, wenn nicht alle Ebenen mit einbezogen werden – von der Spitze der Organisation bis hin zu jedem einzelnen Stakeholder in der GRC-Funktion. Wenn die digitale Transformation nicht akzeptiert wird, besteht die Möglichkeit, dass ihre Vorteile nicht richtig kommuniziert werden. In dieser Hinsicht ist die Interne Revision in der einzigartigen Lage, solche Informationen weiterzugeben, indem sie einfach einen Platz am Tisch behält.

„Von unserem Platz am Tisch aus können wir bei jedem aufkommenden Trend sicherstellen, dass Management und Überwachungsorgan fundierte Entscheidungen treffen“, sagte Kuhn.

Tatsächlich sollte ein Platz am Tisch für einen Internen Revisor immer von entscheidender Bedeutung sein, um seine Pflichten im Einklang mit seinem Mandat erfüllen zu können. Durch regelmäßige und fundierte Kommunikation mit den Stakeholdern spielt die Interne Revision eine unschätzbare Rolle bei der Förderung einer starken Organisationskultur rund um Risikoabsicherung und Compliance. Wenn die Kommunikationskanäle der Internen Revision ihr volles Potenzial ausschöpfen, sollte GRC immer im Vordergrund stehen.

Das Risiko der Verbreitung von GRC-Tools

Nicht alle zur Implementierung verfügbaren Kontrollen sind einer erfolgreichen GRC-fokussierten Kultur förderlich. Beispielsweise stehen im Zuge der Digitalisierung organisatorischer Prozesse mittlerweile viele Datenanalysetools zur Verfügung, die GRC-Module als Add-Ons enthalten. Die Interne Revision könnte erheblich daran gehindert werden, den Stakeholdern eine umfassende Sicht auf GRC zu vermitteln, wenn sich alle einzelnen GRC-Funktionen dazu entscheiden, separate Tools zu ihrer Unterstützung einzusetzen.

„Ich liebe Datenanalysetools und die 100-prozentige Testabdeckung, die sie bieten. Aaber mittlerweile gibt es so viele andere Tools, die GRC als Mehrwertangebot hinzufügen“, sagt Audra Nariunaite , Compliance-Direktorin beim automatisierten Beschäftigungsplattformanbieter Oyster. „Ein Tool, das ich mir kürzlich angesehen habe, fasst andere SaaS-Tools zusammen, um hervorzuheben, welche Verträge kurz vor der Erneuerung stehen und welche potenziellen Steuereinsparungen es gibt. Es bietet aber auch eine Version eines Risiko-Dashboards, das auf den Informationen basiert, die SaaS-Tools verarbeiten. Wenn es die Absicht war, ein solches Tool für etwas anderes als GRC zu kaufen, wüsste ich nicht einmal davon.“

„Plötzlich könnte ich in einer Situation sein, in der ich ein Dutzend zufälliger SaaS-Tools mit Komponenten hätte, die alle ein hohes Risiko darstellen, weil Anbieter unsere privaten Daten verarbeiten“, fuhr Nariunaite fort . „Derzeit gibt es in unserem Ökosystem über 100 SaaS-Tools. Selbst wenn ein kleiner Prozentsatz dieser Tools eine GRC-Version für sehr spezifische Prozesse anbietet, wird es schwierig, diese zu verwalten. Es entstehen individuelle Bereiche, in denen die Leute denken, sie würden Risikobewertungen durchführen, diese aber nicht auf eine Weise durchführen, die ganzheitlich und berichtspflichtig ist.“

Um einem solchen Risiko entgegenzuwirken, besteht eine Strategie darin, dass GRC-Stakeholder einzelne Prozessverantwortliche ernennen, um den GRC-Ansatz zu rationalisieren und einen klaren Kommunikationsweg für die Interne Revision zu erstellen. „Jeder möchte das Richtige tun“, sagte Nariunaite . „Es gibt jetzt einen Drang, das Gesamtrisiko zu managen, und das ist großartig. Es muss jedoch über die Aufteilung der Aufgaben und die Art und Weise, wie diese erfolgen sollte, diskutiert werden, um Prioritäten und Bereiche aufeinander abzustimmen.“

Kuhn äußerte eine ähnliche Meinung, indem er die Balance betonte, die Organisationen zwischen gemeinsamer Verantwortung und Top-Down-Kontrolle haben sollten. „Die Interne Revision sollte versuchen, die Stakeholder so weit wie möglich die GRC-Ziele und -Prozesse vorantreiben zu lassen und sie dann unter dem Gesichtspunkt der Förderung von Zusammenarbeit und Transparenz anzugehen. Die Interne Revision muss Teil dieses Gesprächs sein, damit wir da sein können, um Alarm zu schlagen, wenn wir etwas sehen. Die meisten Menschen verstehen Risiko und Kontrolle im Zusammenhang mit ihren eigenen Rollen. Sie brauchen unsere Einmischung nicht unbedingt, aber wir müssen die umfassenderen Ziele verstehen und wissen, wo die Verantwortlichkeiten liegen, um eine angemessene Beaufsichtigung durchführen zu können."

Strategien zur Führung und Förderung von Diskussionen

Wo möglich, sollte die Interne Revision mit gutem Beispiel vorangehen, indem sie die Vorteile der digitalen Transformation durch die Wirksamkeit ihrer Funktion projiziert und fördert. Während einige Aspekte der digitalen Transformation innerhalb der Internen Revision offensichtlich einen erheblichen Budgetspielraum erfordern, können andere Aspekte, wie etwa die grundlegende Automatisierung, durch Programme wie Excel, Power BI und andere Microsoft-Produktivitätstools durchgeführt werden, die wahrscheinlich bereits intern vorhanden oder zumindest zu minimalen Kosten käuflich zu erwerben sind.

Mit gutem Beispiel voranzugehen gilt auch für den Wissensaustausch, einschließlich der Hervorhebung kritischer Kompetenzen und fehlender GRC-Funktionen. Sowohl innerhalb der Internen Revision als auch in anderen Abteilungen kann die Interne Revision eine konstruktive Rolle bei der Aufdeckung von Wissens-, Schulungs- oder Erfahrungslücken der Belegschaft im Zusammenhang mit der Arbeit mit neuen Technologien spielen und gleichzeitig geeignete Korrekturmaßnahmen fördern. Zu diesen Maßnahmen könnten gemeinschaftliche Schulungen auf Konferenzen, die Beauftragung externer Parteien für Schulungen und Weiterqualifizierungen oder einfach die Einbindung kompetenzbasierter Schulungen in die Arbeitsplätze über kostenlose oder kostengünstige Online-Ressourcen gehören.

In einigen Fällen können Organisationen daran arbeiten, die interne Weiterqualifizierung durch Interaktionen und Kooperationen mit anderen Abteilungen zu fördern. „Eine Strategie, die ich gesehen habe, besteht darin, eine Website zu erstellen, auf der jeder in der Organisation seine eigenen Innovationsideen einbringen und dann darüber abstimmen oder kommentieren kann, was er im Unternehmen sehen möchte", sagte Kuhn. „Das wäre eine Möglichkeit, Wissen und Ideen auf kontrollierte Weise auszutauschen, sodass nicht jeder einfach rausgeht und tausend verschiedene Dinge tut, um Kompetenzen aufzubauen."

Eine solche Diskussion muss nicht immer formell sein. Selbst etwas so Einfaches wie ein Team Chat kann zu einem ähnlichen Ergebnis führen. „In unserer Organisation gibt es mehrere Slack-Kanäle, an denen jeder teilnehmen kann", sagte Nariunaite. „In letzter Zeit hänge ich zum Beispiel im Engineering-Humor-Kanal ab. Sie verstehen, dass ich der Leiter der Compliance bin, behandeln mich aber wie einen Partner. Ich finde es toll, dass wir alle informelle Kontakte zu Teams haben können, die tatsächlich an der Spitze der digitalen Transformationsbewegung stehen."

Um jedoch einen Beitrag zur Diskussion zu leisten, sollte die Interne Revision zusätzlich dazu angeregt werden, sich mit diesen Technologien vertraut zu machen.

Tatsächlich kann der Erwerb dieses Wissens eine wertvolle Gelegenheit für die Interne Revision sein, den organisatorischen Wert, den sie bietet, zu steigern. „Ich glaube nicht, dass wir uns sinnvoll an der Diskussion mit Stakeholdern beteiligen können, wenn wir sie um ein Treffen beispielsweise über KI oder Datenanalyse bitten, wenn wir nicht selbst über ein erhebliches Maß an Wissen verfügen", sagte Nariunaite. „Bei so vielen Aspekten der digitalen Transformation in GRC ist die Frage, wer die Verantwortung dafür übernehmen wird, noch offen. Warum nicht die Interne Revision? Wir sind neugierig, wir sind aufgeschlossen und wir lernen ständig gemeinsam mit unseren Kunden, damit wir in die Diskussionen eingreifen können. Was wäre, wenn wir diejenigen wären, die bei so etwas wie der KI-Implementierung in Compliance beraten würden?"

Fazit

Seien Sie ein aktiver Teil der Revisions-Community

Es gibt kein Zurück von einer digitalen Transformation und die Wahl für ein Unternehmen ist einfach: annehmen oder zurückbleiben. Eine solche Stimmung durchdringt tatsächlich jedes Element der Organisation, von der Führungsebene und dem Sitzungssaal bis hin zu GRC, Betrieb und Interner Revision.

Darüber hinaus sollte es, insbesondere in einer zunehmend vernetzten, globalisierten Welt, über Branchen und geografische Grenzen hinweg fließen. Dabei geht es nicht nur darum, Aufgaben innerhalb der Grenzen einer Organisation wahrzunehmen, sondern auch darüber hinaus aktiv an globalen Revisions-Diskussionen teilzunehmen. Das Engagement in lokalen IIA-Instituten kann eine großartige Gelegenheit sein, um solche Kontakte zu knüpfen, ebenso wie die regelmäßige Teilnahme an IIA-Webinaren und -Konferenzen.

„Die beste Revisions-Lernerfahrung besteht darin, die Erfahrungen anderer Funktionen aus erster Hand zu hören“, sagte Nariunaite. „Ich lerne so viel, indem ich mich mit anderen Fachleuten auf Twitter über aktuelle Prüfungsthemen und Technologietrends austausche. Der Beruf hat sich seit meinem Einstieg so sehr verändert. Es ist so wichtig, diese Branchenverbindungen aufrechtzuerhalten und auf dem Laufenden zu bleiben und zu sehen, wie andere die Herausforderungen, denen Sie gegenüberstehen, erfolgreich meistern.“

Auch wenn die Technologie so weit fortgeschritten ist und sich weiter weiterentwickeln wird, gibt es ein gewisses Maß an Trost, wenn man weiß, dass es beim Lernen und Wachsen in einer beruflichen Rolle immer noch keinen Ersatz für echte menschliche Beziehungen gibt. Angesichts des stetigen Wandels wird es wichtig sein, sich daran zu erinnern.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

Copyright

June 2023

Deutsche Übersetzung durch das DIIR – Deutsches Institut für Interne Revision e.V., Juli 2023

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