

Leitfaden für das Risikomanagement von Dritten

Wie Sie das Risiko durch Drittparteien in Ihrem
Unternehmen erfolgreich mindern können

2025



Überblick

Der Leitfaden zum Risikomanagement von Dritten ist eine umfassende Ressource voller Einblicke, Ratschläge und Beispiele, die Unternehmen dabei helfen, alle Aspekte des Risikos durch Drittparteien zu erkennen und anzugehen.

Ein starkes Programm für das Risikomanagement von Dritten hilft Ihrem Unternehmen, intelligente Entscheidungen zu treffen, wenn es um die Zusammenarbeit mit Geschäftspartnern geht. Es schützt Ihr Unternehmen auch vor Risiken, die durch Drittparteien entstehen können.

Dieser Leitfaden ist in drei Hauptabschnitte unterteilt: PLANEN, UMSETZEN und MESSEN. In diesen Abschnitten finden Sie Informationen und Tools, die Sie benötigen, um eine risikobasierte Strategie zu entwickeln, Drittparteirisiken zu definieren und Bereiche zu identifizieren, in denen Sie die Effektivität Ihres Programms verbessern sollten.

NAVEX® | Navigator Series

Die Navigator Series bietet fundierte Anleitungen zum Aufbau und zur Optimierung von Risiko- und Compliance-Programmen. Unsere Unterlagen stützen sich auf aktuelle Untersuchungen und bieten grundlegende Einblicke und vertiefende Analysen zu bestimmten Themen und Regionen. Sie sollen Ihnen als Grundlage für Ihre Planungen dienen, um die erfolgreiche Umsetzung Ihres Programms zu fördern.

Inhalt

Einleitung	4
Warum ist das Risikomanagement von Dritten wichtig?	4
Vorteile eines starken Programms für das Risikomanagement von Dritten	5
Planen	7
Ziele definieren und eine Strategie erstellen	7
Bedarfsermittlungsrechner	8
Kritische Komponenten für die Planung	9
Identifizieren Sie Ihre Drittparteien	11
Überlegen Sie, welche Arten von Drittrisiken bestehen	12
Definieren Sie einen Prozess für das Risikomanagement von Dritten	13
Identifizieren Sie Elemente, die automatisiert werden können	14
Wer sollte für Ihr Programm für das Risikomanagement von Dritten verantwortlich sein?	15
Umsetzen	16
Verwalten Sie Ihr Programm für das Risikomanagement von Dritten	16
Gewinnen Sie ein tieferes Verständnis der Risiken und wirtschaftlichen Eigentümer	19
Drittparteien kontinuierlich überwachen	19
Bewertung der ESG-Leistung von Drittparteien	19
Alle Risiken mit einer umfassenden Risikobewertung betrachten	20
Informieren Sie sich, wie Drittparteien ihre IT-Risiken schützen	20
Decken Sie die Integrität der Lieferkette auf und planen Sie Unterbrechungen ein	20
Messen	21
Fazit	23

Einleitung

Warum ist das Risikomanagement von Dritten wichtig?

Die Geschäftslandschaft entwickelt sich ständig weiter, insbesondere in Hinblick auf das Management von Drittparteirisiken. Wie erkennt und begegnet Ihr Unternehmen Risiken, die von Ihren Drittparteien ausgehen, wenn sich die Geschäftsanforderungen ändern, globale Vorschriften entwickeln und neue Trends entstehen? Einfach ausgedrückt: Wenn Sie kein robustes Programm haben, ist Ihr Unternehmen einem erheblichen Risiko ausgesetzt.

Die Reduzierung von Risiken durch Drittparteien sollte ein Eckpfeiler Ihres GRC-Programms (Governance, Risiko und Compliance) sein. Nachfolgend sind einige der Faktoren aufgeführt, die bei der Bewältigung von Drittparteirisiken zu berücksichtigen sind.

Zunehmende Abhängigkeit von Drittparteien

Die Anzahl der Anbieter, Lieferanten und anderen Vertreter, mit denen Unternehmen zusammenarbeiten, wächst stetig – und damit auch die Risiken, die damit einhergehen. Unternehmen verlassen sich bei kritischen Vorgängen zunehmend auf Dritte. Die Auslagerung dieser Aufgaben birgt jedoch unzählige Risiken und deren angemessenes Management sollte für die Unternehmensführung oberste Priorität haben.

Verstärkte Globalisierung

Angesichts der Expansion der Märkte und der zunehmenden Konkurrenz ist eine zunehmende Globalisierung unvermeidlich. Für viele Unternehmen bedeutet der Wettbewerb auf neuen Märkten eine enge Zusammenarbeit mit Drittparteien.

Verstärkte Durchsetzung

Die globale Landschaft hat sich in den letzten Jahren verändert, und infolgedessen haben die globalen Regulierungsbehörden einen stärkeren Fokus auf Risiken durch Dritte gelegt. Das US-Justizministerium (DOJ) und die Securities and Exchange Commission (SEC) haben die Durchsetzung des Foreign Corrupt Practices Act (FCPA) zu einer obersten Priorität gemacht, und die US-amerikanischen und andere globale Regulierungsbehörden haben die Sanktionsdurchsetzung verstärkt. Darüber hinaus gibt es einen wachsenden Trend zu globalen Vorschriften zum Schutz der Menschenrechte in der Lieferkette, die insbesondere im [deutschen Lieferkettengesetz](#) und in der EU-Lieferkettenrichtlinie festgelegt sind.

Zunahme von Cyberangriffen

Alle Organisationen, von kleinen Betrieben bis hin zu großen Konzernen, sehen sich mit einer Zunahme der Häufigkeit, Raffinesse und Auswirkungen von Cyberangriffen konfrontiert. In diesem Zusammenhang verfeinern und aktualisieren böswillige Akteure kontinuierlich ihre Bemühungen, Systeme, Netzwerke und Informationen zu kompromittieren – insgesamt macht dies die Cybersicherheit zu einem schwierigen Thema.

Da immer neue Technologien auf den Markt kommen und von Unternehmen zur Optimierung ihrer Geschäftsabläufe eingesetzt werden, kann der Umfang, in dem Ihre Daten weitergegeben werden, exponentiell zunehmen. Die zunehmend komplexen Technologien in allen Unternehmensbereichen sowie die Verwendung personenbezogener Daten erfordern ein umfassendes Programm, um zu verstehen, wer Zugriff auf die Daten Ihres Unternehmens hat und wie diese Informationen verarbeitet werden.

Die Risiken sind real

Wie wir in den Nachrichten häufig sehen, haben Führungsfehler im Umgang mit Drittparteien Unternehmen in Form von hohen Bußgeldern und auferlegten Strafen geschadet. Selbst wenn die Geldstrafe verkräftet werden kann, kann der Reputationsverlust weitreichende und langanhaltende Folgen für viele Jahre haben.



Compliance



Informationssicherheit



Recht



Beschaffung

Risikomanagement von Dritten ist ein wichtiges Anliegen für Führungskräfte im gesamten Unternehmen, einschließlich Compliance, Informationssicherheit, Recht, Beschaffung und mehr. Viele Unternehmen sind jedoch noch dabei, sich damit auseinanderzusetzen, wie sie ihre Drittparteien am besten verwalten können, um Risiken zu begrenzen und Programme auf der Grundlage von Bewertungen des operativen Risikos zu entwickeln.

Vorteile eines starken Programms für das Risikomanagement von Dritten

Das Management von Drittparteirisiken kann einen großen Unterschied darin machen, wie gut Ihr Unternehmen die Haftung, die ein Dritter darstellen kann, identifizieren, verwalten und begrenzen kann.

Das Risiko Ihrer Drittpartei ist Ihr Risiko – und Sie sollten darauf vertrauen, dass Ihr Programm das Risiko für Ihr Unternehmen minimieren kann.

Ein starkes Programm für das Risikomanagement von Dritten – das Onboarding, Screening, Testkontrollen, Untersuchungen und Risikominderung von Beziehungen zu Drittparteien im gesamten Unternehmen umfasst – hilft Ihrem Unternehmen auf mehreren Weisen:

Vermeidung von Bußgeldern, Strafverfolgungsmaßnahmen und Rechtskosten

Ein starkes Programm für das Risikomanagement von Dritten hilft Ihrem Unternehmen, rechtliche Schritte und Bußgelder zu vermeiden, und kann auch Strafen reduzieren und regulatorische Maßnahmen im Falle eines Vorfalls mindern.

Förderung der Kultur Ihres Unternehmens

Der [FCPA](#) empfiehlt, dass Unternehmen nachweisen müssen, dass sie eine Kultur des ethischen und verantwortungsvollen Verhaltens, sowohl intern als auch gegenüber Dritten, fördern. Ein klarer Weg dies zu erreichen, besteht darin, von Dritten zu verlangen, Ihren Verhaltenskodex zu

verstehen und einzuhalten, an Ihrer Compliance-Schulung für Drittparteien teilzunehmen und Ihre Richtlinien über eine [Richtlinienmanagement-Lösung](#) zu bestätigen.

Erstellen Sie ein genaueres Risikobild

Ein umfassendes Programm für das Risikomanagement von Dritten liefert ganzheitliche Daten darüber, wo das Unternehmen dem größten Risiko ausgesetzt und wo es gut geschützt ist. Diese Erkenntnisse sind nicht nur hilfreich für Schulungs-, Richtlinien- und Einstellungsentscheidungen, sondern können auch darauf hinweisen, wo sofortige Maßnahmen erforderlich sind und Ressourcen zugewiesen werden sollten.

Kontinuität fördern

Störungen in Beziehungen zu Dritten können sich nachteilig auf die kontinuierliche Fortführung der Geschäftspraktiken auswirken. Versäumnisse von Drittparteien können zu rechtlichen Maßnahmen, Betriebsunterbrechungen oder regulatorischen Maßnahmen führen, deren Lösung erhebliche Ressourcen erfordert. Im schlimmsten Fall können Ausfälle Dritter sogar die Existenzfähigkeit Ihres eigenen Unternehmens gefährden.

Den Ruf des Unternehmens schützen

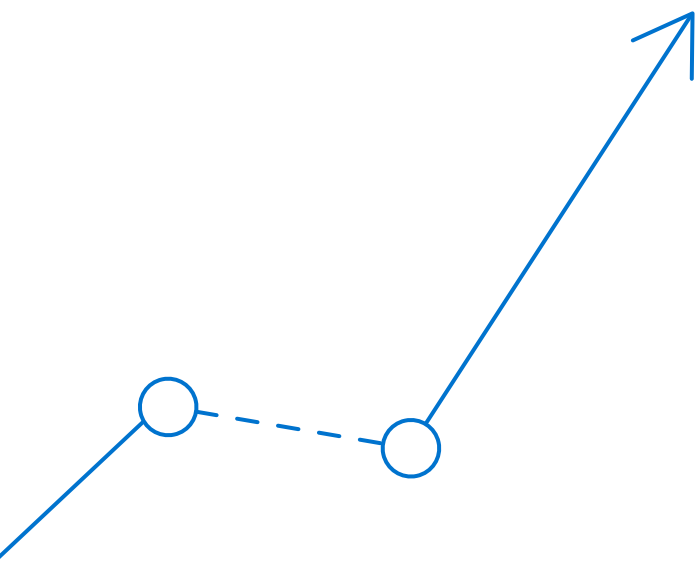
Wie wir in vielen hochkarätigen Fällen sehen, kann ein einzelner Fehler einer Drittpartei die Beziehung des Unternehmens zu seinen Kunden tiefgreifend beeinträchtigen. Sorgen Sie dafür, dass Ihr Unternehmen auch in Zukunft erfolgreich sein wird, indem Sie geprüfte Drittanbieter bevorzugen.

Eine Einheitsgröße passt nicht allen

Viele Programmleiter befürchten, dass sie nicht wissen, wo sie mit einem Programm für das Risikomanagement von Dritten beginnen sollen. Die gute Nachricht ist jedoch, dass Unternehmen keine Massen von Mitarbeitern oder unbegrenzte Budgets benötigen, um die Best Practices des Programms zu erfüllen.

Ein risikobasierter Ansatz für das Risikomanagement von Dritten umfasst die Abstimmung des Risikoprofils von Drittparteien auf Ihr organisatorisches Risikoprofil und den Aufbau eines Programms, das beide optimiert.

Fast jedes Unternehmen verfügt über einige Elemente eines effektiven Programms für das Risikomanagement von Dritten. In den nächsten Abschnitten geben wir Empfehlungen und Vorlagen, um zu ermitteln, was Sie bereits haben und um festzustellen, was Sie benötigen, um Ihre Lücken zu schließen, und die richtige Strategie für Ihr Unternehmen umzusetzen.



Planen

Ziele definieren und eine Strategie erstellen

Ganz gleich, ob Ihr Unternehmen mit einer Handvoll lokaler Beratungsfirmen oder Tausenden von Herstellern auf der ganzen Welt zusammenarbeitet, diese Engagements sind für Ihr Unternehmen relevant – und ihr Versagen würde sich auf die Funktionsfähigkeit Ihres Unternehmens auswirken. Die Landschaft der Drittparteien ist umfangreich und weist oft eine Komplexität auf, die selbst die anspruchsvollsten Unternehmen und Führungskräfte überraschen kann.

In diesem Abschnitt wird erläutert, wie ein Standardprozess für das Risikomanagement von Dritten eingerichtet wird – von der ersten Identifizierung von Drittparteien bis hin zum Onboarding, Risikoscreening, Identifizierung und kontinuierlichem Monitoring.

Erstellung des Business Case für Ihr Programm für das Risikomanagement von Dritten

Beantworten Sie die folgenden Fragen, um festzustellen, welche Auswirkungen ein speziell entwickeltes Programm für das Risikomanagement von Dritten auf Ihr Unternehmen haben würde.

Bedarfsermittlungsrechner	Ja/Nein
Wie wertvoll ist ein ausgereiftes Programm für das Risikomanagement von Dritten für Ihr Unternehmen?	
Unser Unternehmen würde erhebliche Auswirkungen zu spüren bekommen, wenn wir Risiken nicht rechtzeitig und effektiv identifizieren und analysieren würden	
Ein Ausfall einer Drittpartei würde sich drastisch auf unser Geschäft auswirken und die Fähigkeit zur Bereitstellung von Kernprodukten und -dienstleistungen einschränken	
Unser Unternehmen hat Schwierigkeiten bei der Sicherstellung und/oder Berichterstattung, dass unsere Drittparteien die geltenden Vorschriften und Compliance-Anforderungen erfüllen	
Unsere Branche unterliegt häufig wechselnden Vorschriften und Compliance-Standards, die eine kontinuierliche Überwachung und Kontrollprüfung erfordern	
Wie würden Sie Ihr bestehendes Programm für das Risikomanagement von Dritten heute bewerten?	
Unsere Geschäftseinheiten sind isoliert, was zu unabhängigen Risikobewertungen und einer Unfähigkeit zur Integration in unser GRC-Programm führt	
Wir haben keinen strukturierten Ansatz für das Onboarding von Drittparteien	
Wir haben keinen Standardprozess für die Überprüfung von Drittparteien	
Unser Programm verfügt über keinen zentralen Ort, an dem Risiken aus unserer Drittanbieterlandschaft eingesehen werden können	
Unser Programm verfügt über keine Technologie, um Daten in unserem gesamten Unternehmen zu sammeln, zu verbinden und zu kontextualisieren	
Wir haben begrenzte oder schlecht definierte Arbeitsabläufe zur Verwaltung, Überwachung und Analyse unserer bekannten Risiken und Erkenntnisse	
Wir haben eine begrenzte Sichtbarkeit auf aktuelle und zukünftige Risiken und verlassen uns in erster Linie auf ein reaktionäres Risiko- und Compliance-Verfahren	
Wie würden Sie Ihren Prozess zum Risikomanagement von Dritten bewerten?	
Wir verbringen zu viel Zeit mit administrativen Aufgaben, wie der Sammlung von Informationen für das Onboarding und der Kommunikation von Risiken	
Wir stehen unter dem Druck, Ressourcen aus anderen Geschäftsbereichen abzuziehen, um TPRM-Aktivitäten durchzuführen	
Wir haben keinen automatisierten Prozess zur Erfassung von Risiko- und Compliance-Informationen	
Wir sehen uns häufig geschäftliche Herausforderungen gegenüber, aufgrund nicht identifizierter und nicht eingedämmter Risiken in unserem Unternehmen	
Gesamtzahl der "Ja" Antworten:	

Anzahl der "Ja" Antworten	<5	5 – 7	8 – 10	>10
Bedarfsstufe	Niedrig	Mittelmäßig	Durchschnittlich	Hoch
Handlungsempfehlung	Nicht zu empfehlen	Selektiv handeln	Handeln	Sofort handeln

Kritische Komponenten für die Planung

Ein einheitlicher Ansatz

Es gibt wahrscheinlich mehrere Bereiche Ihres Unternehmens, die sich mit Drittparteibeziehungen beschäftigen und diese verwalten. Aus diesem Grund ist es entscheidend, dass alle wichtigen Stakeholder, einschließlich derjenigen, die an vorderster Front mit Dritten zusammenarbeiten, auf die Verwendung desselben Managementsystems für Dritte ausgerichtet sind. Ein isolierter Ansatz erhöht die Risikoexposition eines Unternehmens erheblich. So kann es beispielsweise sein, dass Ihre Beschaffungsabteilung keine Kenntnis von relevanten Informationen hat, die Ihre Compliance-Abteilung in Bezug auf eine Drittpartei entdeckt hat.

Eine Schlüsselkomponente zur Gewährleistung der Programmkonsistenz ist ein verteiltes, automatisiertes System. Um dies zu unterstützen, ist die volle Zustimmung der Führungskräfte und des Vorstands erforderlich. Die Unternehmensleitung sollte regelmäßig über das Programm für Dritte informieren und allen Mitarbeitern klar machen, dass Beziehungen zu Dritten überprüft werden sollten, um damit verbundene Risiken für das Unternehmen zu erkennen und zu mindern.



Angemessene Ressourcen

Jeder hat mit Kapazitäts-, Ressourcen- und Budgetbeschränkungen zu kämpfen. Neben der Zeit und den Kosten, die für das erste Onboarding von Drittparteien anfallen, müssen Sie bei der Einrichtung Ihres Programms zusätzliche Kosten berücksichtigen. Berücksichtigen Sie die Betriebs- und Geschäftskosten in Bezug auf:

- Die Häufigkeit der laufenden Überwachung, die sich nach Ihrem Risikoprofil und dem Risikoprofil Ihrer Drittparteien richtet
- Die Anzahl der zu überwachenden Drittparteien – und welche Sie häufiger als andere überwachen müssen und warum
- Ihre Notfallpläne für den Fall, dass eine Drittpartei ausfällt – wie Sie sich zurückziehen und Auswirkungen oder Betriebsstörungen begrenzen können
- Bis zu welchem Grad Sie sich zurückziehen müssen. Wäre eine vollständige oder nur eine teilweise Trennung erforderlich? Würde es sich auf alle Geschäftseinheiten oder nur auf die direkt betroffenen auswirken?
- Die spezifischen Zusicherungen, die Sie benötigen, um wieder mit einem gescheiterten Dritten zusammenzuarbeiten, und wie lange der Prozess der Wiederaufnahme der Zusammenarbeit dauern würde
- Ihre voraussichtlichen Kosten in Bezug auf Produktivitätsverluste, Ausfallzeiten, offene Geschäftsbeziehungen und die erneute Zusammenarbeit bzw. Suche nach einem Ersatzanbieter im Falle eines Ausfalls
- Effektive, automatisierte Lösungen, die Ressourcen sparen (auch Vollzeitmitarbeiter), die Produktivität steigern und die Betriebskosten senken

Passende Übersetzungen und Öffentlichkeitsarbeit

Viele Drittparteien mit hohem Risiko sind in Schwellenländern ansässig, in denen Deutsch nicht die Muttersprache ist. In vielen Fällen empfinden Drittparteien die Prüfung des Risikomanagements von Dritten als riskant und verwirrend – insbesondere, wenn die übermittelten Informationen nicht in der Landessprache des Dritten vorliegen.

Die Bereitstellung von Benachrichtigungen, Anweisungen und Interviewfragen in der Landessprache der Drittpartei kann den Dritten mit dem Prozess vertrauter machen und dazu beitragen, wichtige Fragen wie „Warum ist der Prozess wichtig?“ und „Wie werden unsere Informationen verwendet?“ genau zu beantworten.

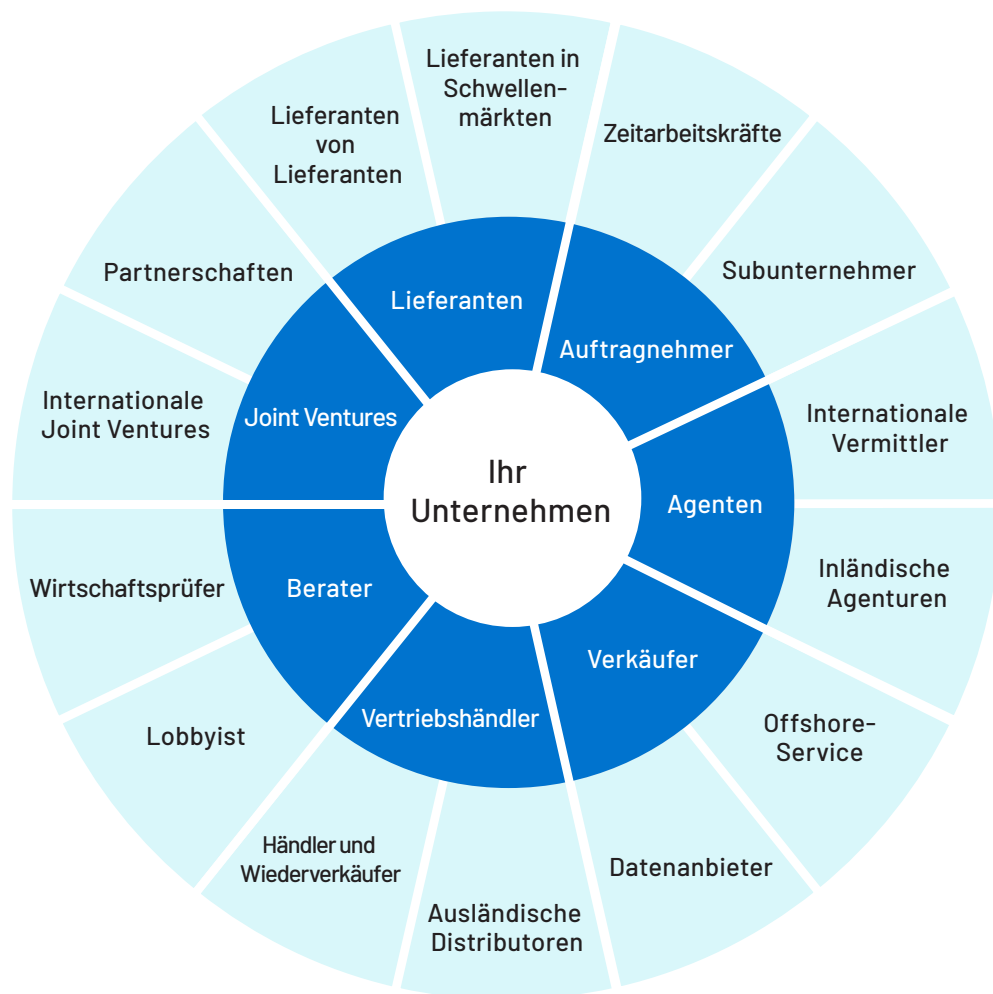
Schulung von Drittparteien

Unternehmen sollten gegebenenfalls die Ausweitung der Compliance-Schulung ihres Unternehmens auf ihre verschiedenen Drittparteien in Betracht ziehen, insbesondere in Bezug auf Verhaltenskodexe und die Bescheinigung von Richtlinien. Entscheidungen darüber, wann und in welcher Form Schulungsunterstützung angeboten wird, sollten das Risikoprofil des Dritten und den Grad des Risikos in der Beziehung widerspiegeln. Ein erstklassiges GRC-Programm bietet anpassbare Schulungen für Drittparteien und kann problemlos zu Ihrer laufenden Compliance-Schulung hinzugefügt werden.

Identifizieren Sie Ihre Drittparteien

Die Landschaft der Drittparteien wird für die meisten Unternehmen immer umfangreicher und komplexer. Wenn Unternehmen wachsen wollen, gibt es eine Vielzahl von Drittparteien mit tiefgreifendem Fachwissen und breiten Fähigkeiten, die die Erfolgsfähigkeit Ihres Unternehmens erweitern können. Heutzutage erweitern viele Unternehmen aktiv ihre Geschäftsfähigkeiten durch die Zusammenarbeit mit Dritten, mit oder ohne einem risikobasiertem Programm für das Risikomanagement von Dritten.

Ihre unmittelbaren Lieferketten- und Vertriebskanäle stellen direkte Beziehungen zwischen Ihrem Unternehmen und der Drittpartei dar. Dennoch kommt es heutzutage immer häufiger vor, dass Ihre direkte Drittpartei in Ihrem Namen mit externen Fachberatern, Agenten und Auftragnehmern zusammenarbeiten, zu denen Ihr Unternehmen keine direkte Beziehung hat. Wenn Ihre Drittparteien über ein Netzwerk indirekter Drittparteien – manchmal auch als vierte Parteien bezeichnet – verfügen, müssen auch diese berücksichtigt werden



Überlegen Sie, welche Arten von Drittrisiken bestehen

Es gibt verschiedene Arten von potenziellen Risiken, die Dritte für Ihr Unternehmen darstellen können, die in den folgenden Kategorien zusammengefasst sind:

Compliance

Das Risiko, dass ein Unternehmen rechtlichen Sanktionen, finanziellen Einbußen und materiellen Verlusten ausgesetzt ist, weil sie nicht in Übereinstimmung mit Branchengesetzen und -vorschriften, internen Richtlinien oder vorgeschriebenen Best Practices handelt.

Finanzielle Risiken

Das Risiko, Geld bei einer Investition oder einem Geschäftsvorhaben zu verlieren. Zu den häufigeren und ausgeprägteren finanziellen Risiken zählen das Kreditrisiko, das Liquiditätsrisiko und das operationelle Risiko – diese Risiken können für die Beteiligten zu Kapitalverlusten führen.

IT- und Cybersicherheitsrisiken

Das Risiko im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen, Daten oder Informations- (oder Kontroll-)Systemen, das die potenziellen negativen Auswirkungen auf den Geschäftsbetrieb widerspiegelt.

Rechtliches Risiko

Das Risiko, dass eine Drittpartei die Compliance Ihres Unternehmens mit lokalen Gesetzen, Vorschriften oder Vereinbarungen beeinträchtigt.

Operatives Risiko

Das Risiko, dass ein Dritter den Geschäftsbetrieb stört. Dies wird in der Regel durch vertraglich gebundene Service Level Agreements (SLAs) geregelt.

Regulatorische Risiken

Das Risiko, dass sich eine Änderung der Gesetze und Vorschriften wesentlich auf ein Wertpapier, ein Unternehmen, einen Sektor oder einen Markt auswirkt.

Reputationsrisiko

Reputationsschaden ist der Verlust von Finanzkapital, Gesellschaftskapital und/oder Marktanteil, der sich aus der Schädigung des Rufs eines Unternehmens ergibt. Dies wird oft in entgangenen Einnahmen, erhöhten Betriebskosten, Kapital- oder regulatorischen Kosten oder der Zerstörung des Anteilseignerwerts gemessen.

Strategisches Risiko

Das Risiko, dass Ihr Unternehmen seine Geschäftsziele aufgrund eines Versagens Dritter nicht erreichen kann.

Ihr Drittpartei-Risikoprofil

Nachdem Sie Ihr Netzwerk von Drittparteien identifiziert haben, ist es entscheidend, die Auswirkungen dieser Engagements auf den Erfolg Ihres Unternehmens klar zu verstehen. Dies bedeutet nicht nur, Tiefe und Umfang Ihrer Drittparteienbeziehungen zu definieren, sondern auch die Kosten für den Erfolg oder Misserfolg Ihres Programms zu verstehen. Das bedeutet, dass Erfolgskriterien definiert und alle möglichen Einschränkungen des Programms eingeplant werden müssen.

Bewerten Sie Ihre Risiken, indem Sie Folgendes definieren:

- Das regulatorische Umfeld und die Branche, in der Ihr Unternehmen tätig ist
- Die Anzahl der Drittparteien, mit denen Ihr Unternehmen zusammenarbeitet
- Die Arten von Drittparteien, mit denen Sie zusammenarbeiten (Lieferanten, Wiederverkäufer, Vertriebspartner, Hersteller usw.) und wo sie sich befinden
- Die Anzahl der für Ihren Geschäftsbetrieb kritischen Drittparteien

- Die Produkte und Dienstleistungen die von jeder Drittpartei erbracht werden
- Welche Daten jeder Drittpartei zur Verfügung stehen

Berücksichtigen Sie bei der Bewertung Ihrer Position das regulatorische Umfeld, in dem Ihr Unternehmen und Ihre Drittparteien tätig sind. Einige Branchen sind stärker reguliert als andere, und einige Aufträge von Dritten ziehen mehr rechtliche und regulatorische Aufmerksamkeit auf sich. Um Ihr Drittparteiprogramm und Ihr Unternehmen bestmöglich zu schützen, sollten Sie zunächst die Bedrohungen und Chancen kennen, die in dem Umfeld, in dem Sie tätig sind, vorhanden sind.

Die Anzahl der Drittparteien, mit denen Ihr Unternehmen zusammenarbeitet, ist ein Indikator für Ihr Risikoniveau. Es kann Ihnen dabei helfen, Ihre Herausforderungen zu definieren – viel mehr als die Größe Ihres Unternehmens in Bezug auf Mitarbeiter oder Umsatz. Tatsächlich ist der Anteil der Drittparteien im Verhältnis zu der Größe Ihres Unternehmens ein klarerer Hinweis auf Ihr Risikoniveau als absolute Zahlen. Beispielsweise gibt es globale Fertigungsunternehmen, die die Fertigung über große Drittanbieternetzwerke ermöglichen und dabei nur sehr wenige Mitarbeiter direkt beschäftigen. Umgekehrt gibt es riesige multinationale Unternehmen, die mit sehr wenigen Drittparteien zusammenarbeiten.

Ein Teil Ihres Risikoprofils wird dadurch definiert, wie tief Ihre Drittparteien in Ihr Unternehmen integriert sind. Wenn Sie darüber nachdenken, wie viele Ihrer Drittparteien für Ihre Geschäftsleistung entscheidend sind, überlegen Sie, wie groß die Auswirkungen wären, wenn Sie Ihre Zusammenarbeit mit einer Drittpartei oder einer Reihe von Drittparteien schnell reduzieren oder erhöhen, oder wenn Sie sich vollständig von ihnen trennen müssten. Während Sie das interne GRC-Programm Ihres Unternehmens direkt verwalten können, haben Sie weniger Einblick in die Programme Ihres Drittanbieters. Daher ist die Möglichkeit, dass ein Ausfall Dritter die Betriebsfähigkeit beeinträchtigt, ein Maß für das Risiko.

Berücksichtigen Sie bei der Überprüfung der potenziellen finanziellen, betrieblichen und Reputationsrisiken für Ihr Unternehmen die Fähigkeit Ihres Unternehmens, das Risiko Dritter angemessen zu verwalten und zu mindern. In einigen Fällen überwiegen die Risiken einer Geschäftsbeziehung mit einem Dritten die potenziellen Vorteile. Legen Sie die Kriterien für diese Entscheidung rechtzeitig im Voraus fest oder bestimmen Sie einen Beauftragten, der die Befugnis hat, Grenzfälle zu genehmigen oder abzulehnen.

Das Sprichwort **Vertrauen ist gut, Kontrolle ist besser** trifft in Bezug auf Risiken durch Dritte zu. Nutzen Sie Daten, Tools und ein aktives Programm für das Risikomanagement von Dritten, um Ihr tatsächliches Risiko zu definieren.

Definieren Sie einen Prozess für das Risikomanagement von Dritten

Entwickeln Sie einen konsistenten, strukturierten Prozess zur Bewertung und Zuweisung von Risiken an jede Drittpartei. Während kontinuierliche Prozesse für Effizienz sorgen, erfordert ein effektives Risikomanagement von Dritten die Bewertung jeder Drittpartei auf der Grundlage ihres spezifischen Risikokontexts und einzigartigen Risikoprofils. Stellen Sie folgende Fragen:

- Welche Abteilungen im Unternehmen erledigen welche Aufgaben?
- Generieren wir doppelte Arbeitsbelastung?
- Welche Komponenten benötigen Input von externen Drittparteien?
- Welche Freigaben sind von wem und an welcher Stelle im Prozess erforderlich?

Identifizieren Sie Elemente, die automatisiert werden können

Technologie zur Prozessoptimierung einsetzen

Die Vereinfachung von Prozessen kann zu einer erheblichen Reduzierung der Komplexität, des Zeitaufwands und der damit verbundenen Kosten führen. Noch wichtiger ist, dass die Automatisierung Sie dazu zwingt, klar definierte Standards zu setzen. Die Einhaltung dieser Standards wiederum hilft Unternehmen, Vorurteile und Fehler zu vermeiden. Gängige Prozesse, deren Automatisierung für ein starkes Programm für das Risikomanagement von Dritten in Betracht gezogen werden sollten:

Onboarding und Überprüfung von Drittparteien

Optimieren Sie das Onboarding mit einem konsistenten Prozess, um alle erforderlichen Daten von Drittparteien zu sammeln und führe Sie erste Überprüfungen durch, um die damit verbundenen Risiken während der Erwägungsphase Ihrer Geschäftsbeziehung zu verstehen.

Gewinnen Sie ein tieferes Verständnis der Risiken und wirtschaftlichen Eigentümer

Ermitteln Sie den wirtschaftlichen Eigentümer (Ultimate Beneficial Owner, UBO), um die Eigentumsverhältnisse Dritter festzustellen, und führen Sie eine verstärkte Sorgfaltsprüfung durch, um risikoreiche Dritte genauer zu untersuchen und fundierte Entscheidungen zu treffen.

Drittparteien kontinuierlich überwachen

Überwachen Sie Dritte während des gesamten Geschäftsverlaufs, um Echtzeitwarnungen zu erhalten, wenn sich der Risikostatus ändert, die Auswirkungen von Risiken zu verstehen und fundierte Entscheidungen zu treffen.

Bewertung der ESG-Leistung von Drittparteien

Finden Sie heraus, wie sich Dritte für Umwelt-, Sozial- und Governance-Praktiken (ESG) einsetzen, um sicherzustellen, dass Ihre Partner mit den Werten und Standards Ihres Unternehmens übereinstimmen.

Alle Risiken mit einer umfassenden Risikobewertung betrachten

Verknüpfen Sie Dritte mit Richtlinien, Risiken, Kontrollen, um die mit ihnen verbundenen Risiken für Ihr Unternehmen vollständig im Blick zu haben.

Informieren Sie sich, wie Drittparteien ihre IT-Risiken schützen

Stellen Sie sicher, dass Dritte die richtigen Sicherheitsmaßnahmen ergreifen und Ihre Erwartungen beim Umgang mit Ihren Daten erfüllen.

Decken Sie die Integrität der Lieferkette auf und planen Sie Unterbrechungen ein

Verfolgen Sie die Arbeitsweise von Drittparteien und richten Sie Prozesse zur Aufrechterhaltung des Geschäftsbetriebs ein, um sich auf mögliche Betriebsausfälle von Drittparteien vorzubereiten.

Wer sollte für Ihr Programm für das Risikomanagement von Dritten verantwortlich sein?

Die Planung und Implementierung Ihres Programms für das Risikomanagement von Dritten sollte ein kollaborativer und integrativer Prozess sein, an dem Vertreter verschiedener Abteilungen beteiligt sind, darunter Compliance, Recht, Personalwesen, interne Revision, Sicherheit, Risikomanagement, Beschaffung und IT. Die Stakeholder müssen Partnerschaften eingehen, um sicherzustellen, dass das Programm reibungslos umgesetzt wird und dass alle Abteilungen effektiv das erhalten, was sie benötigen.



Umsetzen

Verwalten Sie Ihr Programm für das Risikomanagement von Dritten

Die Implementierung des Programms für das Risikomanagement von Dritten Ihres Unternehmens sollte einem kontinuierlichen Prozess von Onboarding, Screening, kontinuierlicher Überwachung und Lebenszyklusmanagement folgen. Neben diesen Aktivitäten sollten Sie auch eine laufende Kommunikation mit dem Management und anderen wichtigen Stakeholdern über Programmprozesse, Erfolg, Leistung und erwartete Änderungen einbeziehen.

Kommunizieren Sie bei der Umsetzung Ihres Plans transparent die Erwartungen an Ihr Programm gegenüber aktuellen und potenziellen Drittparteien. Arbeiten Sie eng mit Ihren Drittparteien zusammen, um sie über Ihre Erwartungen aufzuklären, einschließlich Ihres Verhaltenskodexes, Ihrer Richtlinien und Prozesse sowie Ihrer Verhaltensanforderungen. Wenn Sie dies frühzeitig tun, schützen Sie sich und den Dritten vor Verhaltensverstößen und unnötigen Risiken während der gesamten Laufzeit des Auftrags.

Kommunikation der Richtlinie

Einer der wichtigsten Aspekte bei der Verwaltung Ihres Programms ist die Kommunikation einer klaren, schriftlichen Richtlinie zum Risikomanagement von Dritten. Stellen Sie sicher, dass die Richtlinien für Dritte, Beschaffung und Lieferketten Ihre aktuelle Richtlinie für Dritte klar und deutlich festlegen. Richtlinien sollten regelmäßig überprüft, bei Bedarf aktualisiert und in regelmäßige Compliance-Schulungen aufgenommen werden.

Risiken mindern

Viele Elemente der Programminitiation können intern durchgeführt werden, bevor Dritte hinzugezogen werden. Zu diesen ersten Schritten können unter anderem die Definition und Weitergabe von Zielen, die Strukturierung von Programmparametern, die Identifizierung von Stakeholdern und Programm-Champions sowie die Einholung eines Budgets gehören. Die Einrichtung dieses ersten Programms kann Monate dauern, bevor das erste Onboarding und die erste Überprüfung einer Drittpartei erfolgen kann.

Insbesondere wenn Unternehmen in einer komplexen Drittanbieterlandschaft arbeiten und die Sicherstellung der Programmwirksamkeit von entscheidender Bedeutung ist, kann ein Stresstest Ihrer Prozesse und Fähigkeiten durch ein begrenztes Early-Adopter-Programm dazu beitragen, den Erfolg des Programms und das Vertrauen der Stakeholder sicherzustellen.

Ein strukturiertes Programm sollte Drittparteien durch eine festgelegte Abfolge von Ereignissen führen, um Prozesskonsistenz zu gewährleisten. Ihr Programm sollte standardisierte Dokumentation und Praktiken umfassen, die über ein zentralisiertes System mit einer klar definierten Befehlskette für alle Programmänderungen, Ausnahmen oder Verbesserungen verwaltet werden. Dies stellt sicher, dass alle Mitarbeiter der Organisation bei Änderungen gleichermaßen informiert werden.

Überprüfung und Onboarding von Drittparteien

Entwickeln Sie klare Erwartungen an jede Drittpartei auf der Grundlage der zu erledigenden Arbeit. Definieren Sie eindeutig einzelne Führungskräfte und Ansprechpartner nach Name und Rolle, Service-Level-Vereinbarungen, Leistungserwartungen, spezifische Kriterien für die Beendigung und wer Maßnahmen ergreifen kann, um die Beendigung zu verfolgen, und unter welchen Bedingungen weitere Maßnahmen ergriffen werden sollten. Obwohl es vielleicht am einfachsten ist, Kontakte mit Namen zu identifizieren, sollten Sie darauf achten, Schlüsselrollen zu identifizieren, um sich auf unvermeidliche personelle Veränderungen vorzubereiten.

Obwohl es vielleicht am einfachsten ist, Kontakte mit Namen zu identifizieren, sollten Sie darauf achten, Schlüsselrollen zu identifizieren, um sich auf unvermeidliche personelle Veränderungen vorzubereiten.

Ihr Onboarding-Prozess für Drittparteien sollte vertraut und standardisiert sein, um zu vermeiden, dass wichtige Anforderungen fehlen – und damit Ihre Drittparteien den Prozess problemlos abschließen können. Stellen Sie sicher, dass Sie Schulungen von Drittparteien zu Ihren wichtigsten Richtlinien und Anforderungen einbeziehen.

Jedes Unternehmen hat einige spezifische Berichtsanforderungen oder Zusicherungen, aber die Kernschritte des Onboardings einer Drittpartei, einschließlich der anfänglichen Due-Diligence-Anfragen, sind wahrscheinlich ähnlich. Die Standardisierung von Prozessen und Dokumenten hilft Ihnen dabei, Schritte anzugehen und einzubeziehen, die bei der ersten Definition des Onboarding-Prozesses möglicherweise nicht offensichtlich sind.

Sie legen zwar den Zeitplan und die besonderen Anforderungen Ihres Unternehmens für die formelle Aufnahme einer neuen Drittpartei fest, müssen jedoch zu einem bestimmten Zeitpunkt eine eingehendere Überprüfung des Dritten durchführen, nachdem Sie die erforderlichen Informationen gesammelt haben, um ein Profil der Drittpartei zu erstellen. Die Überprüfung sollte Finanz- und Reputationsprüfungen, mehrere interne Überprüfungskanäle und Experten umfassen, die sich mit dem Dritten und seinen Vertretern befassen und unabhängige Recherchen durchführen.

Während des Onboardings und der Überlegungsphase ist es wichtig, Ihre Drittparteien auf regulatorische und Reputationsrisiken zu überprüfen, die sie für Ihr Unternehmen mit sich bringen können – diese Risiken können Indikatoren sein, die zu tiefergehenden Recherche- und Berichtspflichten führen können.

Negative Medienberichte

Suchen Sie nach Berichten über Geschichten in veröffentlichten Medien, in denen die Drittpartei oder ihre wichtigsten Stakeholder erwähnt werden. Achten Sie darauf, neben finanziellen und rufschädigenden Hinweisen auch Suchbegriffe einzuschließen, die nach Verstößen gegen die moderne Sklaverei oder anderen Menschenrechtsverletzungen suchen.

Sanktionen und Beobachtungslisten

Prüfen Sie behördliche Berichte über Unternehmen, gegen die Sanktionen verhängt wurden, und die Gründe dafür.

Politisch exponierte Personen

Suchen Sie nach Ressourcen, die die politischen Verbindungen von Führungskräften und Einzelpersonen, die mit der Drittpartei in Verbindung stehen, und deren Auswirkungen aufdecken.

Neben dem Screening von Drittparteien auf regulatorische Risiken und Reputationsrisiken ist es wichtig zu verstehen, wie integriert jeder Dritte in die Abläufe Ihres Unternehmens sein wird. Der erste Schritt besteht darin, zu wissen, welche Drittparteien Zugriff auf interne Unternehmens- oder Kundendaten, Systeme, Prozesse oder andere privilegierte Informationen haben – und in welchem Umfang. Nachdem Sie diese Gruppe verstanden haben, sollte während der Erwägungsphase eine standardisierte Risikobewertung durchgeführt werden, um zu erfahren, wie Drittparteien mit Daten umgehen, welche Sicherheitsmaßnahmen vorhanden sind und welche Pläne für einen Verstoß oder eine Unterbrechung bestehen.

Das Ergebnis eines Screenings während des Onboarding-Prozesses sollte eine Genehmigung, Ablehnung oder Verschiebung des Auftrags sein.

Gewinnen Sie ein tieferes Verständnis der Risiken und wirtschaftlichen Eigentümer

Obwohl die Standardprüfung die meisten Ihrer Berichtspflichten abdecken sollte, kann es vorkommen, dass eine eingehendere Prüfung erforderlich ist. Je nachdem, wie Ihr Programm die Zusicherungen von Drittparteien definiert, kann es sein, dass ein bestimmter Prozentsatz Ihrer Drittparteien nach den Standardprüfungen zusätzliche Sorgfaltspflichten erfüllen muss, bevor Sie mit ihnen Geschäfte tätigen können.

Unternehmen sollten die Freiheit haben, mehrere Filterrahmen zu entwickeln, die die Ergebnisse ihrer Überprüfungsmaßnahmen so konfigurieren, dass sie spezifische Risikotoleranzen erfüllen, die sich je nach Größe und Art eines Vertrags, geografischer Lage und Branchenzugehörigkeit unterscheiden können. Im Wesentlichen sollten Sie in der Lage sein, Hochrisikokunden aus einer Jurisdiktion gegen alle verfügbaren Daten, Hochrisikokunden aus einer anderen Jurisdiktion gegen eine andere Untergruppe und weitere Niedrigrisikokunden gegen einen kleineren Datensatz zu screenen. Durch diese Filterung wird die Qualität der zurückgegebenen Datenwarnungen erheblich verbessert, wodurch sowohl die Relevanz als auch die Wesentlichkeit für jede Risikostufe deutlich erhöht werden.

Bei der Aufnahme von Beziehungen mit höherem Risiko ist es wichtig, Bedenken hinsichtlich des wirtschaftlichen Eigentums zu identifizieren – was mehrere Komplexitätsebenen umfassen kann –, Prozessunterlagen aufzudecken und Interviews mit ehemaligen Mitarbeitern, Aufsichtsbehörden und Partnern der Drittpartei zu führen. Darüber hinaus sollten Sie alle möglichen Risikofaktoren ermitteln und feststellen, ob wirtschaftliche Eigentümer auf Sanktionsbeobachtungslisten stehen.

Ein automatisiertes System kann Ihnen dabei helfen, Ihr Risiko richtig einzustufen und die Prozesse zu steuern, die sicherstellen, dass im Rahmen der ordnungsgemäßen Sorgfaltspflicht alle potenziellen Risiken während des gesamten Auftrags aufgedeckt werden.

Drittparteien kontinuierlich überwachen

Beziehungen zu Drittparteien sind fließend und es ist wichtig, die aktuellsten Informationen aufrechtzuerhalten, wenn sich Prozesse und Status von Drittparteien ändern. Die laufende Überwachung kann eine regelmäßige erneute Überprüfung bestehender Dritter oder eine erneute Überprüfung aufgrund einer Warnmeldung über eine Änderung des Status des Dritten umfassen. Wenn Sie regelmäßig Bewertungen Ihrer Drittparteien durchführen lassen, erhalten Sie außerdem die notwendigen Informationen, um zu erfahren, ob diese weiterhin Ihren Erwartungen entsprechen. Eine kontinuierliche Überwachung ermöglicht es Ihnen, Ihr Drittparteienrisiko schnell und genau zu identifizieren und zu bewerten, sodass Sie handeln können, um das Risiko zu beseitigen oder zu reduzieren, bevor es sich auf Ihr Unternehmen auswirkt.

Bewertung der ESG-Leistung von Drittparteien

Die Zusammenarbeit mit Dritten birgt unvermeidbare Risiken. Aber auch wenn Sie diese Risiken managen, ist es wichtig sicherzustellen, dass die Unternehmen, mit denen Sie zusammenarbeiten, dieselben Werte vertreten, die Sie auch intern erwarten. Da Unternehmen daran arbeiten, ethischer, vielfältiger und verantwortungsbewusster zu werden, müssen sie dieselben Stärken auch bei den Anbietern erkennen, mit denen sie zusammenarbeiten.

Nicht nur Sie erwarten diese Werte von Ihren Partnern, sondern neue globale Vorschriften – wie das deutsche Lieferkettengesetz – verlangen von Unternehmen auch, dass sie einen solchen Ansatz beim Thema Drittparteienrisiko verfolgen. Mit besonderem Fokus auf Menschenrechtsrisiken in der Lieferkette müssen Unternehmen auch die ESG-Bemühungen von Drittparteien berücksichtigen – was dem Risikomanagement von Dritten eine neue Dimension verleiht.

Alle Risiken mit einer umfassenden Risikobewertung betrachten

Drittparteien sind ein integraler Bestandteil des Geschäftsbetriebs, aber es ist wichtig zu beachten, dass die mit ihnen verbundenen Risiken weiter reichen, je stärker Partner in Ihr Unternehmen integriert werden.

Ein wichtiger Schritt zur Risikobewältigung besteht darin, den Einfluss Ihrer Drittparteien auf Ihr gesamtes Unternehmen zu verstehen. Die Erfassung von Risikoinformationen – einschließlich betrieblicher, informationssicherheits-, finanzieller und compliance-bezogener Risiken – ist der erste Schritt. Indem Sie das Risiko durch Drittparteien als Teil des Gesamtrisikos betrachten dem Ihr Unternehmen ausgesetzt ist, können Sie die Wirksamkeit Ihres Programms verstehen, und vor allem Bereiche identifizieren, auf die Sie sich konzentrieren müssen.

Informieren Sie sich, wie Drittparteien ihre IT-Risiken schützen

IT-Risiken haben das Potenzial, den geschäftlichen Wert zu schädigen und resultieren oft aus einem schlechten Management von Prozessen und Ereignissen. IT-Risikoprogramme, einschließlich solcher, die das IT-Risiko des Lieferanten verstehen, konzentrieren sich auf die Identifizierung und Minderung von Ereignissen, die die IT-Funktionen gefährden.

Dazu können Schwierigkeiten bei der Netzwerkkommunikation, Hardware- und Softwareausfälle, Naturkatastrophen, menschliche Fehler und böswillige Angriffe gehören. Wenn Sie den Betrieb an eine Drittpartei auslagern, ist es ein notwendiger Schritt, detaillierte Einblicke in die Richtlinien, Prozesse und Praktiken jedes Dritten zu erhalten – und sicherzustellen, dass die vorhandenen Sicherheitsvorkehrungen umfassend sind –, um Ihr Unternehmen zu schützen. Das erfolgreiche Management aller betrieblichen

oder systembezogenen Risiken erfordert einen systematischen Ansatz, der folgende Schritte umfasst:

- Risikobewertung und -analyse
- Risikobeurteilung
- Priorisierung
- Kontrollprüfungen

Drittparteien gelten als Teil Ihres Unternehmens und sollten denselben Prozessen unterliegen, die Ihre internen Mitarbeiter zum Schutz Ihrer Daten anwenden.

Decken Sie die Integrität der Lieferkette auf und planen Sie Unterbrechungen ein

Das Verständnis dafür, wie Ihre Lieferketten funktionieren, ist entscheidend für den Erfolg Ihres Unternehmens. In unserem digitalen Zeitalter sind Unterbrechungen häufiger und schwerwiegender als je zuvor. Ereignisse, die Unternehmen daran hindern, ihre Mission zu erfüllen, sind nicht nur die offensichtlichen wie Naturkatastrophen, IT-Ausfälle oder Sicherheitsverletzungen. Es gehören auch Ausfälle in der Lieferkette, behördliche Bußgelder, Probleme mit der sozialen Unternehmensführung und mehr dazu.

Bei der Zusammenarbeit mit Drittparteien müssen Unternehmen Pläne zur Geschäftskontinuität und Risikominderung entwickeln, bevor potenzielle Lieferkettenausfälle auftreten. Wenn Abhilfepläne vorhanden sind, können Ihre Teams in solchen Szenarien schnell handeln, notwendige Ressourcen verschieben und auf unerwartete Situationen reagieren, um weiterhin die Geschäftsanforderungen zu erfüllen.

Messen

Der allgemeine Zweck der Messung der Effektivität Ihres Programms für das Risikomanagement von Dritten besteht darin, sicherzustellen, dass das Programm seine Ziele erreicht und Ihr Unternehmen gut vor Risiken geschützt ist.

Die Messung der Wirksamkeit ist oft für jedes Unternehmen einzigartig, je nach Branche, geografischem Standort und Art der beteiligten Drittparteien. Es gibt mehrere Möglichkeiten, die Effektivität Ihres Programms zu messen, darunter:

- Die Skalierbarkeit Ihrer einheitlichen und zentralisierten Lösung
- Die Geschwindigkeit und Genauigkeit, mit der Sie neue Drittparteien onboarden können
- Die Konsistenz und Umsetzbarkeit Ihrer Programmberichterstattung
- Der Zeitrahmen und die Kosten im Zusammenhang mit der Behebung von Screening- und Überwachungsalarman

Alternativ können Sie Ihre Programmleistung mit einem früheren Zustand vergleichen durch:

- Die verbesserte Qualität Ihrer Drittparteiengagements im Hinblick auf die Anzahl der von Ihnen identifizierten Risiken
- Ihre Fähigkeit, Merkmale Dritter genauer zu identifizieren, die ein erhöhtes Risiko für Ihr Unternehmen darstellen
- Ihre Fähigkeit, damit verbundene Risiken besser zu verwalten oder zu mindern, einschließlich des Austauschs leistungsschwacher Drittparteien durch reaktionsschnellere Partner
- Die relativen Geschäftskosten für Onboarding, Screening, Überwachung und Lebenszyklusmanagement sowie die Auswirkungen Ihrer Lösung auf die Verkürzung von Ausfallzeiten und die Senkung der damit verbundenen Kosten

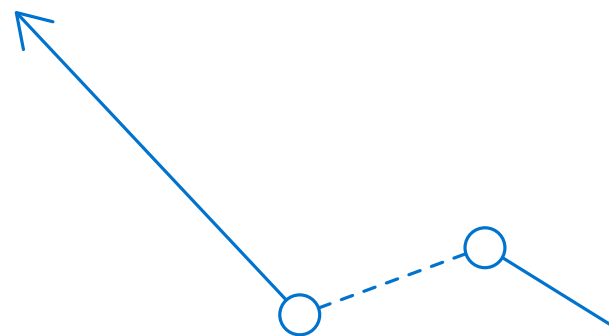
Berücksichtigen Sie schließlich bei der Überprüfung Ihrer Programmleistung die anfängliche Risikobewertung, die Sie abgeschlossen haben. Diese Risikobewertung sollte Aufschluss über Ihren ROI geben. Indem Sie Ihr Risiko auf Grundlage des regulatorischen Umfelds, der Anzahl der Drittparteien, mit denen Sie zusammenarbeiten, ihrer Bedeutung für Ihren Betrieb und der finanziellen Risiken, die von diesen Drittparteien ausgehen, berechnet haben, haben Sie eine Risikobewertung erstellt.

Diese Risikobewertung kann mit den Zielen eines Programms für das Risikomanagement von Dritten und Ihren Fortschritten bei diesen Zielen verglichen werden. Diese Ziele sind:

- Vermeidung von Bußgeldern, Strafverfolgungsmaßnahmen und Rechtskosten
- Förderung der Kultur Ihres Unternehmens
- Förderung eines genaueren Risikobildes
- Kontinuität fördern
- Förderung des Rufs des Unternehmens

Wenn Ihr Programm dem Unternehmen geholfen hat, Bußgelder zu vermeiden, die Verteidigungsfähigkeit zu verbessern und die Programmpräzision durch dokumentierte Prozesse, Kontrollen, Protokolle und Ergebnisse zu steigern, können Sie es mit einer reduzierten Risikobewertung verknüpfen.

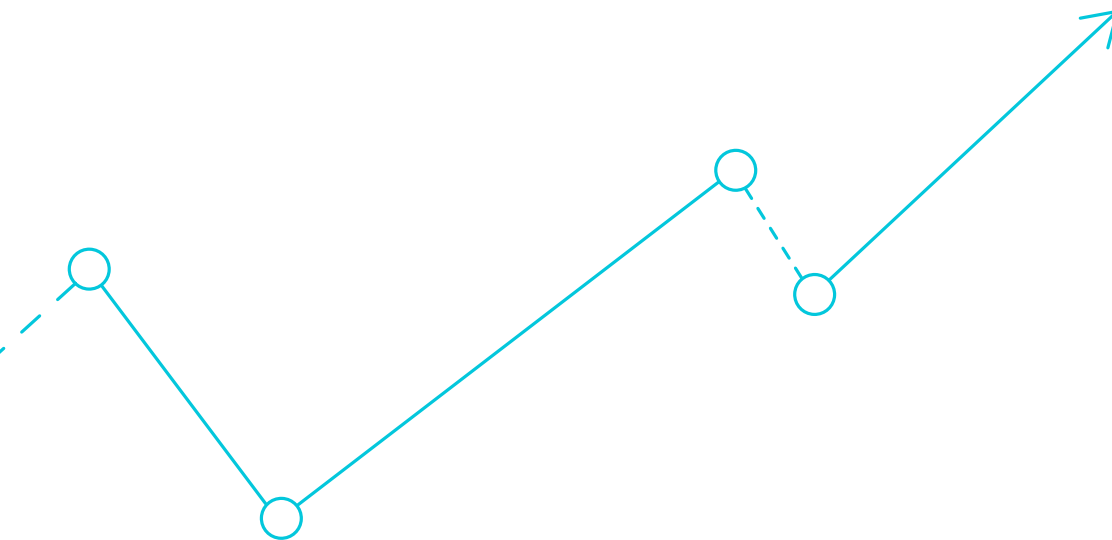
Wenn Sie einen Anbieter für das Risikomanagement von Dritten nutzen, können Sie Reporting-Tools verwenden, um Probleme zu erkennen, Trends zu analysieren und das Programm zu automatisieren, ohne sich auf internes Personal und Reporting verlassen zu müssen. Die besten und effektivsten Berichtsprogramme sind solche, die Daten nutzen, um den Erfolg von Interventionen zu messen, Trends zu verfolgen und den allgemeinen Zustand von Beziehungen zu Drittparteien zu bewerten.



Fazit

Ein effektives, gut ausgestattetes und konsequent angewandtes Programm für das Risikomanagement von Dritten ist in Ihrem besten Interesse. Sie können nicht nur sicher mit einem wachsenden Netzwerk von Anbietern, Lieferanten, Wiederverkäufern und Distributoren zusammenarbeiten, sondern auch einen positiven Einfluss auf das GRC-Programm als Ganzes haben.

Ein effektives Risikomanagement von Dritten ist ein entscheidender Bestandteil von Geschäftsprogrammen. Wie in diesem Leitfaden ausführlich beschrieben, erfordert ein zusammenhängendes Programm Engagement, Konzentration und Struktur. Ein besseres Management Ihres Drittparteienrisikos erfordert nicht unbedingt ein großes Budget oder Personal. Konzentrieren Sie sich stattdessen auf den Aufbau eines effektiven Programms, das auf das Niveau und die Arten von Risiken skalierbar ist, denen Ihr Unternehmen in seiner Drittanbieterlandschaft ausgesetzt ist.



NAVEX® | Navigator Series

Über 13.000 Unternehmen – darunter 70% der Fortune 100- und 500-Unternehmen – vertrauen auf NAVEX, dem weltweit führenden Anbieter von Risiko- und Compliance-Lösungen. Die NAVEX One-Plattform stärkt Risiko- und Compliance-Programme und unterstützt Unternehmen mit beispiellosen Benchmark-Daten und branchenspezifischen Erkenntnissen. NAVEX One bietet einen 360-Grad-Blick auf Risiken innerhalb des Unternehmens, bei Drittparteien und im gesamten Geschäftsumfeld – für eine bessere Einhaltung gesetzlicher Vorschriften und einem proaktiven Risikomanagement. Mit Niederlassungen in den USA, Europa und Asien und einem globalen Kundenstamm definiert NAVEX weiterhin die Zukunft von Governance, Risiko und Compliance.

Besuchen Sie unseren [Blog](#) oder folgen Sie uns auf [LinkedIn](#), [Facebook](#), und [YouTube](#).

NORD- UND SÜDAMERIKA

5885 Meadows Road, Suite 500
Lake Oswego, OR, 97035
USA

info@navex.com
www.navex.com
+1(866)297 0224

EMEA + APAC

London
1 Queen Caroline St.
Londres W6 9YN
Großbritannien

info@navex.com
www.navex.com/en-gb/
+44(0)20 8939 1650