10 Schritte zur Einführung eines soliden Risikomanagement-Programms für Drittparteien

1. **Definieren und beschreiben Sie die Risikotoleranz des Unternehmens.**

Berücksichtigen Sie die Branche und die verschiedenen Gerichtsbarkeiten, in denen Ihr Unternehmen tätig ist, sowie die unternehmenseigene Risikotoleranz. Gibt es spezifische Risiken, die mit der Geschäftstätigkeit in einem bestimmten Wirtschaftssektor, Land oder einer Region verbunden sind? Hat das Unternehmen diese Risiken im Rahmen der Risikobewertung sorgfältig identifiziert? Welche mildernden oder anderen Vorsichtsmaßnahmen hat das Unternehmen vereinbart, um diese Risiken zu bewältigen?

2. **Ausarbeitung und Verabschiedung einer Richtlinie für das Risikomanagement von Drittparteien (TPRM), die das Vorgehen des Unternehmens bei der ordnungsgemäßen Prüfung, Einbindung und ggf. Trennung von Lieferanten festlegt.**

Das Unternehmen sollte eine spezifische Richtlinie beschliessen, die als Grundlage für das Risikomanagement von Drittparteien im gesamten Unternehmen dient. Die Richtlinie sollte den **Prozess, des Unternehmens *zur Identifizierung, Überprüfung, Auswahl, Bewertung* und *Überwachung* potenzieller Lieferanten**, detailliert beschreiben.

Idealerweise sollte die TPRM-Richtlinie auch *einen Ethik- oder Verhaltenskodex für Geschäftspartner enthalten*. Auf sehr hohem Niveau sollte der Kodex die Erwartungen des Unternehmens in Bezug auf akzeptables Verhalten darlegen. Alle Dritten, mit denen das Unternehmen Verträge schließt, sollten zur Einhaltung des Kodex verpflichtet sein. Ein Verstoß gegen den Kodex sollte ein sofortiger Grund für die Vertragskündigung sein.

Die TPRM-Richtlinie sollte *auch Rollen und Verantwortlichkeiten* klar festlegen. Dazu gehört zu identifizieren, welche Geschäftseinheiten oder Personen für die Ausführung bestimmter Richtlinienkomponenten wie die Auswahl von Lieferanten, das Screening abgelehnter Partner, Vertragsverhandlungen, Audits/Inspektionen, Verlängerungen und Kündigungen usw. verantwortlich sind.

3. **Jede Drittpartei anhand einer Risikoskala einstufen.**

Eine TPRM-Skala sollte Risiken klar in drei primäre Kategorien - *hohes Risiko, mittleres Risiko und geringes Risiko* - unterteilen und sich auf objektive Kriterien stützen, um die Compliance-Funktion bei der ganzheitlichen Identifizierung der kritischsten Risiken, denen das Unternehmen ausgesetzt ist, zu unterstützen.

Externe Ressourcen – wie der Korruptionswahrnehmungsindex ("CPI") von Transparency International - können diesen Prozess in Bezug auf bestimmte Problembereiche vereinfachen. Für jeden Anbieter sollte dann ein Score berechnet werden, der alle Risiken berücksichtigt, die das Unternehmen als relevant identifiziert. Der Beurteilungsspielraum ist von entscheidender Bedeutung, um sicherzustellen, dass nur ein kleiner Prozentsatz der Risiken tatsächlich als hohes Risiko eingestuft wird. Dies ermöglicht es dem Unternehmen wiederum, die erforderlichen Ressourcen für Maßnahmen zur Risikominderung effektiver einzusetzen.

4. **Soweit möglich, die gesamte Lieferkette des Unternehmens abbilden, um die Transparenz über den gesamten Produkt-/Dienstleistungslebenszyklus zu maximieren und visuell zu identifizieren, wo genau die größten Risiken liegen.**

Auch wenn es mühselig erscheinen mag, ist die Zusammenarbeit mit sachkundigen internen Stakeholdern im Rahmen des modernen TPRM unbedingt notwendig, und hilft zu verstehen, welchen Beitrag verschiedene Dritte zum Produkt-/Dienstleistungslebenszyklus des Unternehmens beitragen. Dies gilt insbesondere dann, wenn das Unternehmen unter anderem Gesetzgebungen wie der Corporate Sustainability Due Diligence Directive der Europäischen Union, dem deutschen Lieferkettengesetz oder dem Uigurischen Zwangsarbeitspräventionsgesetz unterliegen kann.

In jedem Fall ist eine Abbildung der Lieferkette erforderlich, um die Nichteinhaltung vorgeschriebener Umwelt- und/oder Menschenrechtsstandards zu identifizieren. Betrachtet man das Unternehmensrisiko, kann das Mapping dem Unternehmen auch dabei helfen, betriebliche Schwachstellen, die sich aus der Abhängigkeit von einem bestimmten Dritten ergeben könnten, konkret zu identifizieren und zu beheben.

5. Auswahl und Einführung eines automatisierten TPRM-Systems zur Nutzung im Zusammenhang mit der Administration des TPRM-Programms.

Für alle Unternehmen erfordert das Management der Beziehungen zu Dritten den Einsatz einer **automatisierten TPRM-Lösung**, die die TPRM-Verwaltungsfunktionen in einer einzigen Plattform zusammenfasst. Manuelle Prozesse sind unzureichend und können die Erwartungen der Behörden nicht erfülle. Diese legen großen Wert darauf, dass Unternehmen in der Lage sind, Due-Diligence-Prüfungen durchzuführen, Schulungen zu organisieren, Audits durchzuführen, Compliance-Zertifikate auszustellen und Unternehmens- und Compliance-Risiken effektiv zu koordinieren.

Dies erfordert die Einführung einer automatisierten Lösung wie dem NAVEX One Governance, Risk, and Compliance Information System (GRC-IS), das es der Compliance-Funktion ermöglicht, Risikoinformationen von Lieferanten in Echtzeit zu integrieren, zu überprüfen, zu priorisieren und zu überwachen.

6. Überprüfen Sie alle Standardverträge, die typischerweise mit Lieferanten und Anbietern des Unternehmens verwendet werden, um die wichtige Compliance-Verpflichtungen, Zusicherungen und Garantien beinhalten.

Ein wesentlicher Bestandteil eines effektiven TPRM ist die Abgrenzung klarer vertraglicher Standards im Rahmen endgültiger Vereinbarungen zwischen des Vertragsunternehmens und dem Drittpartner.

Neben der Verpflichtung durch den Kodex der Organisation sollte der Vertrag selbst verlangen, dass das Drittunternehmen die Prüfung und Einsichtnahme in seine Bücher und Aufzeichnungen mit angemessener Frist zulässt. Der Vertrag sollte auch die Inanspruchnahme von Kündigungsrechten für den Fall vorsehen, dass der Dritte den Kodex oder eine materielle Bestimmung der endgültigen Vereinbarung, die die Einhaltung bestimmter Gesetze oder Vorschriften fordert, nicht einhält.

7. Erwägen Sie, Schulungen für Drittparteien in Problembereichen anzubieten.

Die Bereitstellung von Schulungen für Dritte ist ein praktisches Mittel, um zu betonen, dass Ihr Unternehmen seine Compliance-Verpflichtungen ernst nimmt. Dazu kann das Unternehmen seinen Drittpartnern Schulungen in den Bereichen mit dem höchsten Risiko anbieten, die im Rahmen des Screening- und Onboarding-Prozesses der Drittpartei identifiziert wurden. Beispielsweise würde in einem Land mit einem unterdurchschnittlichen CPI-Score (ein Hinweis auf systemische Korruption) eine gezielte Schulung in Form einer Exposition gegenüber Anti-Bestechungs- und Korruptionsgrundsätzen (ABAC) die Botschaft verstärken, dass das Unternehmen eine Null-Toleranz für die Beeinflussung Dritter durch die illegale Zahlung von Bestechungsgeldern oder die Gewährung von Geschenken praktiziert.

8. Sicherstellen, dass Dritte Verstöße gegen den Kodex des Unternehmens oder andere ethische und rechtliche Verstöße melden können.

Wenn möglich, sollten Unternehmen erwägen, ihr bestehendes Vorfall-Meldesystem zu nutzen, um externen Parteien – einschließlich der Mitarbeiter von Geschäftspartnern – die Meldung von Verstößen gegen den Kodex oder andere ethische und/oder rechtliche Verstöße durch Mitarbeiter, Auftragnehmer und Vertreter des Unternehmens zu ermöglichen. Diese Berichtsfähigkeit wird zunehmend von regulatorischen Systemen gefordert, die sich auf Transparenz in der Lieferkette konzentrieren.

9. Verhindern Sie, soweit möglich, die Aufspaltung von Informationen durch Dritte.

Die vielleicht größte Herausforderung für moderne Unternehmen ist die Konsolidierung bestehender Informationssilos. Um effektiv zu sein, sollten alle Informationen, die einen bestimmten Dritten betreffen, an einem einzigen Ort gespeichert werden, der für wichtige Stakeholder der Organisation weitgehend zugänglich ist. Der Zugriff auf eine vollständige Datei mit Lieferanteninformationen ist entscheidend für die Aufrechterhaltung eines zuverlässigen Risikoprofils.

10. Regelmäßige Überprüfung und Aktualisierung der TPRM-Richtlinien und -Prozesse im Lichte regulatorischer Entwicklungen und gewonnener Erkenntnisse.

Es versteht sich von selbst, dass Unternehmen ihre eigenen Richtlinien und Prozesse im Bereich TPRM regelmäßig prüfen sollten, um auf der Grundlage der gemachten Erfahrungen und der neuen rechtlichen Anforderungen Verbesserungsmaßnahmen vorzunehmen. Um die Wirksamkeit des TPRM-Programms zu maximieren, sollten die Richtlinien und Verfahren mindestens einmal jährlich überprüft werden, um möglicherweise erforderliche Änderungen vorzunehmen.