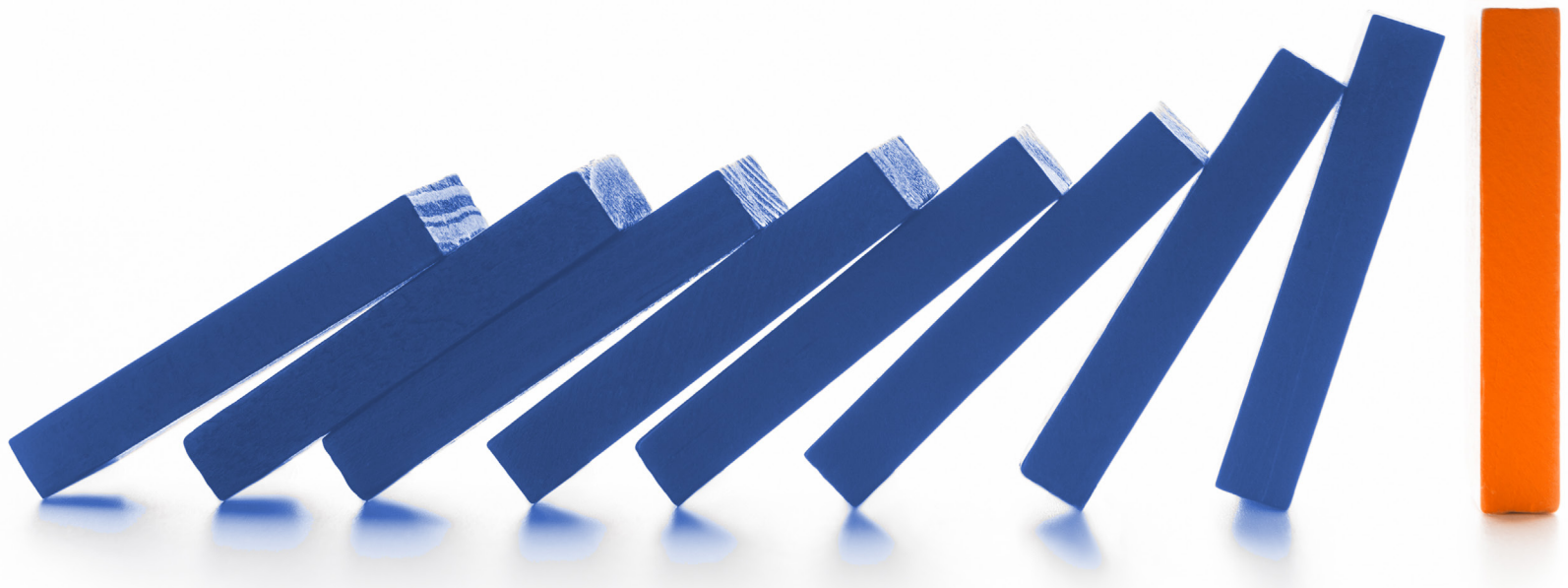
Effektives Third-Party-Risikomanagement:

SCHÜTZEN SIE IHRE MARKE UND IHR GESCHÄFTSERGEBNIS



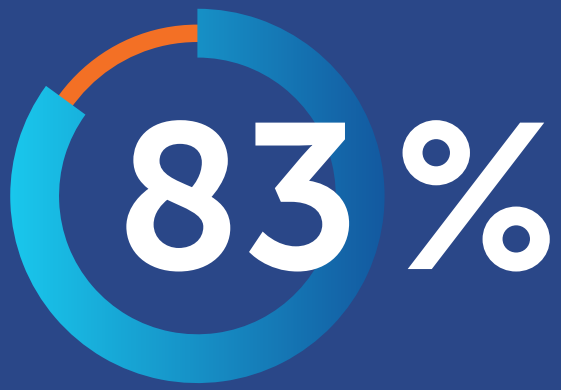
Einführung

Unternehmen greifen häufig auf Drittanbieter, Distributionspartner und freie Subunternehmer zurück, um Wachstum zu beschleunigen, sich Expertenwissen zu sichern oder um Kosten zu senken. Drittanbieter können dem Unternehmen nutzen, aber auch ein Risiko darstellen. Dies hängt davon ab, welche Dienstleistungen sie anbieten und auf welche Unternehmensressourcen sie Zugriff erhalten.

Richtlinien wie unter anderem die Europäische Datenschutzverordnung (DSGVO) machen das Third-Party-Risikomanagement zunehmend komplexer. Unternehmen sind nicht mehr nur für ihre eigenen Handlungen, sondern auch für die ihrer Geschäftspartner verantwortlich. Risiken können z. B. von Drittanbietern von Dienstleistungen oder IT-Plattformanbietern ausgehen, die Services für Unternehmen bereitstellen. Die Kosten für ein schlechtes Risikomanagement laufen schnell aus dem Ruder. Eine Verletzung der DSGVO kann mit bis zu 4 % des Umsatzes zu Buche schlagen.

IT-Risiken, Bestechung und Korruption, die soziale Verantwortung des Unternehmens, betriebliche Resilienz und sonstige Risiken in Verbindung mit Drittanbietern müssen sorgfältig gemanaged werden, um Verletzungen der Compliance, Strafen von Aufsichtsbehörden und einen Schaden für die Marke zu verhindern.

Bei einem unerwarteten globalen Ereignis wie COVID-19 werden diverse isolierte Systeme schnell zur Stolperfalle bei der Bewertung von Third-Party-Risks. Sie führen zu Verzögerungen, die sich Unternehmen in einer Krisensituation nicht leisten können. Lieferantenperformance und Lieferantenrisiken nehmen vor allem in unsicheren Zeiten Einfluss auf den Erfolg des Unternehmens.



der Unternehmen verzeichneten in den letzten 3 Jahren einen Vorfall mit einem Drittanbieter.

Bei 11 % hatte dies erhebliche Auswirkungen und bei 35 % moderate Auswirkungen auf den Kundendienst, die Unternehmensfinanzen, den Ruf des Unternehmens sowie die Compliance.

Deloitte Third Party Governance and Risk Management Extended Enterprise Report

Digitale Initiativen – eine unterschätzte Gefahr

Im Zuge digitaler Innovationen gaben viele Unternehmen zweitrangige Aktivitäten an Serviceanbieter und digitale Plattformen ab, um sich auf ihr Kerngeschäft zu konzentrieren.

Dies stellt Compliance-Teams jedoch vor eine große Herausforderung, wenn die entsprechenden Managementprozesse und -technologien unzureichend fundiert sind.

- **Unverhältnismäßig umfangreiche manuelle Prozesse:** Compliance-Teams und Chief Information Security Officers (CISOs) verlieren mit Spread Sheets oder veralteten Tools für die Identifikation von Third-Party-Risks schnell den Überblick.
- **Ständig wechselnde Risiken:** Die Beziehungen zu Drittanbietern ändern sich mit neuen Geschäftsinitiativen und auf Veränderungen bei Partnerunternehmen hat das Unternehmen selbst kaum Einfluss.
- **Komplexe Compliance-Richtlinien:** Stetig neue sowie sich überschneidende Richtlinien erhöhen die Komplexität durch umfassende Dokumentation und Audit-Anforderungen.

Eine vollständige Liste aller Verstöße in den USA finden Sie unter goodjobsfirst.org/violation-tracker.

Branchenführer gehen ihren eigenen Weg

Trotz aller Schwierigkeiten gibt es auch Unternehmen, die das Third-Party-Risikomanagement hervorragend meistern. Wie gehen führende Unternehmen vor, um teure und unangenehme Vorfälle zu vermeiden?

Sie stellen wichtige Fragen, um Probleme zu vermeiden:

- Wer sind unsere Geschäftspartner?
- Mit welchen Subunternehmen arbeiten diese zusammen, die ein Risiko für uns darstellen könnten?
- Sind die Bedingungen in unseren Verträgen klar und eindeutig?
- Was stellt das größte Risiko für unser Unternehmen dar?
- Wie können diese Risiken minimiert werden?

Der Aufbau eines nachhaltigen Programms für das Risikomanagement mag auf den ersten Blick kosten- und arbeitsintensiv erscheinen. Jene, die ihr Risikomanagement dennoch verbessern möchten, können sich an branchenführenden Unternehmen in diesem Bereich orientieren.

Rufschädigung durch mangelhaftes Third-Party-Risikomanagement

2019 führte ein Datenleck bei einem Abrechnungsdienstleister dazu, dass fast 12 Millionen Kundendaten eines Fortune 500 Unternehmens im Bereich klinischer Labordienstleistungen offengelegt wurden. Bei der Untersuchung des Falls wurde festgestellt, dass persönliche Daten, Kreditkartendaten und medizinisch relevante Daten betroffen waren. Zwar trat dieses Datenleck nicht bei dem Labordienstleister selbst auf, doch das Versäumnis des Abrechnungsunternehmens brachte den Namen des Unternehmens in den Fokus der Öffentlichkeit und sein Ruf nahm großen Schaden.

Branchenführer nutzen 10 bewährte Vorgehensweisen für ein effektives Third-Party-Risikomanagement

Eine der größten Herausforderungen beim Risikomanagement ist die Bandbreite der Gefahren, denen ein Unternehmen durch die Zusammenarbeit mit diversen Partnerunternehmen, Dienstleistern und Vertragspartnern ausgesetzt ist.

Tipps für ein effektives Third-Party-Risikomanagement

1. **Unterstützung durch alle Führungsebenen:** Führende Unternehmen stellen sicher, dass Ihre Führungskräfte und die Unternehmensleitung sich der Bedeutung eines nachhaltigen Risikomanagements bewusst sind und sich dafür einsetzen.
2. **Bewertung Dritter anhand eines Due-Diligence-Prozesses:** Um potenzielle Probleme zu erkennen und Risiken zu minimieren müssen Sie Ihre Partner und deren Geschäftspraktiken kennen.
3. **Auswahl von Anbietern:** Das Third-Party-Risikomanagement sollte bereits bei der Überprüfung und der Auswahl neuer Partnerunternehmen eine Rolle spielen. Drittanbieter müssen Ihre eigenen Lieferanten und Partner auf Sicherheit, Compliance und ethisches Geschäftsgebaren überprüfen. Bei Vertragsabschluss müssen entsprechende Klauseln zur Vermeidung von Risiken in den Vertrag aufgenommen werden.
4. **Analyse der Verwaltung von Unternehmensressourcen:** Es ist wichtig, nachzuverfolgen, wie Dritte mit Unternehmensinformationen und sonstigen Ressourcen interagieren und wie diese Ressourcen nach Abschluss der Zusammenarbeit zurückgegeben oder vernichtet werden.
5. **Aufklärung von Mitarbeitern über Lieferantenrisiken:** Wenn Mitarbeiter von Lieferanten kaufen, die nicht überprüft wurden oder ein Risiko darstellen, ist selbst die beste Risikobewertung wertlos.
6. **Fortwährende Überwachung des Geschäftsgebarens von Partnern:** Jährliche oder regelmäßige Bewertungen können helfen, Risiken aufzudecken. Eine fortwährende Überwachung bietet darüber hinaus die Möglichkeit, sich auf neue Technologien oder Mitarbeiter einzustellen.

7. **Aufnahme der Leistung in die Risikokriterien:** Qualitative Informationen zur Performance des Partners, die idealerweise direkt nach der Erbringung der Leistung erfolgen, vervollständigen quantitative Leistungsdaten.

8. **Digitalisierung von Risikomanagement-Prozessen:** Verabschieden Sie sich von Tabellenkalkulationen oder veralteten Systemen. Mithilfe einer modernen Plattform für das Third-Party-Risikomanagement sammeln Sie Daten, erkennen Risiken in Echtzeit und reduzieren gleichzeitig die Kosten.

9. **Durchführen regelmäßiger umfassender Audits:** Engagieren Sie einen externen Experten, um eine unparteiische Meinung zur Performance Ihres Programms zu erhalten. Umfassende Überprüfungen können sowohl Probleme aufspüren, die bei automatisierten Prozessen übersehen werden, als auch externe Veränderungen, die eine Neugestaltung der Prozesse erforderlich machen.

10. **Zentrale Kontrolle des Risikomanagements:** Durch eine zentrale Kontrolle sparen Unternehmen Kosten und vermeiden Überschneidungen bei der Genehmigung von Anbietern bzw. bei deren Überprüfung.

Risiken können variieren

Führende Unternehmen unterscheiden zwischen riskanten Drittanbietern und riskanten Geschäftsbeziehungen mit Drittanbietern. Grundsätzlich gilt, dass einige Unternehmen, wie z. B. Unternehmen, die auf Beobachtungslisten von Regierungsstellen stehen, auf keinen Fall beauftragt werden sollten. Bei Geschäftsbeziehungen, die Zugriff auf sensible Informationen, wie z. B. Kundendaten erfordern, oder bei umfassenden Geschäftsbeziehungen mit ein und demselben Anbieter (Konzentrationsrisiko) ist eine umfassende Überprüfung erforderlich.

Integration des Risikomanagements in das Business Spend Management zur Bewältigung von Herausforderungen

Erfolgreiche Unternehmen integrieren das Third-Party-Risikomanagement in eine Lösung zum Business Spend Management. Es sollte im Fokus des Unternehmens sowie der betrieblichen Prozesse und Systeme stehen und nicht nur am Rande berücksichtigt werden.

Bewährte Vorgehensweisen:

- **Umfassende Bewertung der Geschäftsbeziehungen mit Lieferanten:** Sammeln Sie Informationen und analysieren Sie Lieferantenrisiken, bevor Sie einen Vertrag abschließen. Bewerten Sie Lieferanten kontinuierlich über den gesamten Lebenszyklus eines Projekts.
- **Mehrstufiger Ansatz:** Sammeln Sie Informationen zu Vertragspartnern sowie deren Geschäftsbeziehungen mit Lieferanten und deren Lieferanten.
- **Proaktives Risikomanagement:** Informieren Sie Entscheidungsträger über potenzielle Risiken, damit sie die richtigen Entscheidungen zu Ausgaben und zum Risikomanagement treffen können. Anhand dieser Daten können Sie Maßnahmenpläne entwerfen, um Risiken in der Lieferkette zu minimieren.

Benchmarks für Third-Party-Risikomanagement

Unternehmen, die auf bewährte Vorgehensweisen setzen, kombinieren das Third-Party-Risikomanagement mit wichtigen betrieblichen Leistungsindikatoren (KPIs), um die Effizienz von Maßnahmen zu messen und diese zu verbessern. Laufen Prozesse effizient, bleibt mehr Zeit für Lieferanten und Geschäftspartner und Risiken können vermieden werden. Benchmarks bieten Anhaltspunkte, um die aktuelle Performance mit branchenführenden Unternehmen in puncto Risikomanagement zu vergleichen.

In diesem Bericht gehen wir auf Benchmarks von Coupa Community Intelligence ein. Hierbei handelt es sich um eine mit KI betriebene Analyse-Engine, die anonymisierte Transaktionsdaten von mehr als 1.000 Coupa-Kunden überwacht. Diese Benchmarks repräsentieren das Top-Quartil der Leistungen aller Coupa-Kunden.

1. Durchlaufzeit der externen Risikobewertung: **81,1 Stunden**
   Dieser KPI misst die Zeit, die verstreicht, bis Dritte auf eine Risikobewertung reagieren. Je schneller die Reaktion Dritter ist, desto besser ist der Servicelevel für das beauftragende Unternehmen.
2. Abschlussquote der externen Risikobewertung: **88,8 %**
   Dieser KPI misst den prozentualen Anteil der Bewertungen, die an Dritte gesendet wurden, und online abgeschlossen werden. Je mehr Bewertungen online abgeschlossen werden, desto weniger Arbeit haben Compliance Manager mit der Nachverfolgung.
3. Durchlaufzeit für interne Maßnahmenpläne **90,1 Stunden**
   Dieser KPI misst die Zeit, die vergeht, bis ein Plan für die Risikominimierung erstellt wurde. Je schneller das Risikomanagement Dritter erfolgt, desto besser ist der Servicelevel für das beauftragende Unternehmen.
4. Pro Ressource verwaltete Lieferanten: **107 Lieferanten**
   Dieser KPI misst die Anzahl der Lieferanten, die von einer einzigen Compliance-Ressource verwaltet werden können. Unternehmen mit effizienten digitalen Prozessen haben mehr Zeit für wichtige Aktivitäten im Rahmen des Risikomanagements.

Kosten von Compliance-Verstößen

Berücksichtigen Sie bei Überlegungen zum ROI des Third-Party-Risikomanagements nicht nur den Schaden durch Rufschädigung, finanzielle Verluste sowie Strafen von Aufsichtsbehörden, sondern auch die Kosten, die durch Analysen und Überwachung entstehen. Die Kosten, die für die Analyse eines Problems entstehen, entsprechen in etwa den Kosten von Strafzahlungen. Die Kosten für die Überwachung nach einer Strafzahlung belaufen sich auf etwa die Hälfte. Geht es um Bestechung und Korruption, können sich die Kosten auf das 2,5-fache der Strafe belaufen.

Governance, Risikomanagement und Compliance (GRC)

Unter GRC versteht man die Fähigkeit, Ziele zuverlässig zu erreichen (Governance), Unsicherheiten auf dem Weg dorthin zu berücksichtigen (Risikomanagement) und mit Integrität zu handeln (Compliance).[1] Unternehmen und Experten steht heutzutage eine Vielzahl von GRC Software Services zur Verfügung. Eine erfolgreiche Implementierung von GRC bietet viele Vorteile, z. B. bessere Entscheidungsfindung und effizientere Investitionen in IT-Ressourcen.

Individuelle GRC-Software-Lösungen sind jedoch häufig sehr umfassend und komplex. Sie stellen möglicherweise nicht den einfachsten Weg zu führendem Third-Party-Risikomanagement dar. Viele Unternehmen können jedoch von der Integration des Third-Party-Risikomanagements mit BSM profitieren.

1 www.oceg.org/about/what-is-grc/

Führendes Telekommunikationsunternehmen verbessert sein Risikomanagement nach einer Strafzahlung von 800 Millionen USD für Korruption

Ein multinationales Telekommunikationsunternehmen verließ sich auf regionale Partner, um sich benötigte Frequenzen in Zentralasien zu sichern und setzte sich im Zuge dessen dem Risiko von Bestechung und Korruption aus. Das Third-Party-Risikomanagement des Unternehmens griff nicht. Ein Drittanbieter wurde in Korruption verwickelt und es wurde eine Strafzahlung in Höhe von fast 800 Millionen USD über das Unternehmen verhängt.

Der Ruf des Unternehmens nahm erheblichen Schaden und es musste sogar seine Marke ändern. Im Zuge dessen wendete es sich an Coupa, um eine zuverlässige Lösung für das Risikomanagement und Einblicke in die Aktivitäten von Drittanbietern zu erhalten. Heute hat das Unternehmen eine zuverlässige Lieferantenbasis und ist auf dem besten Weg, die verstärkte Überprüfung durch Aufsichtsbehörden hinter sich zu lassen.

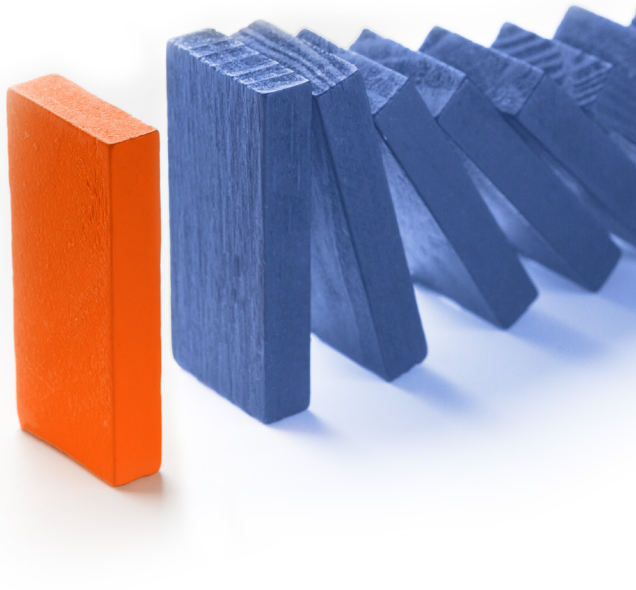
Mit effektivem Risikomanagement und BSM ans Ziel

Die Integration einer umfassende Plattform für das Third-Party-Risikomanagement in eine moderne digitale Plattform bietet den entscheidenden Vorsprung:

1. **Schützen Sie Ihren Ruf:** Schwachstellen, wie Datenlecks, können langfristige Verluste nach sich ziehen, da Kunden zu anderen Wettbewerbern abwandern. Digitale Plattformen zeigen Entscheidungsträgern Risiken umgehend auf, um risikobehaftete Lieferanten zu meiden und den Shareholder-Value zu schützen.
2. **Vermeiden Sie aufsichtsbehördliche Maßnahmen:** Strafzahlungen gehen schnell in die Millionen und die Gesamtkosten belaufen sich auf weit mehr. Digitale Risiko- und Ausgabenplattformen verbessern die Effizienz der Risikokontrolle, zeichnen Maßnahmen zur Risikominimierung auf und helfen Unternehmen, Compliance-Richtlinien einzuhalten.
3. **Bewältigen Sie Zwischenfälle:** Unternehmen mit digitalen Plattformen erholen sich schneller von unerwarteten Zwischenfällen. Optimierte Systeme stoppen relevante Transaktionen umgehend und schlagen alternative Lieferanten vor. So können negative Auswirkungen umgehend minimiert werden.
4. **Verbessern Sie die Agilität in der Lieferkette:** Mithilfe effektiver Prozesse können Lieferanten schneller überprüft werden, neue Produkte gelangen schneller auf den Markt und Ausfälle werden minimiert, sollten mehrere Lieferanten gleichzeitig ausgetauscht werden müssen (z. B. in einer Rezession).

Schlussfolgerung

Führungskräfte und Vorstände zeichnen dafür verantwortlich, dass die notwendigen Ressourcen eingesetzt werden, um die Marke des Unternehmens zu schützen. Die Tipps und bewährten Vorgehensweisen in diesem Dokument unterstützen Organisationen, Third-Party-Risks proaktiv zu verwalten, Schäden für das Unternehmen zu vermeiden, und Gewinne zu sichern. In Zeiten einer globalen Krise, in der die Zukunft ungewiss ist, ist ein effizientes Risikomanagement unverzichtbar.



Erfahren Sie mehr darüber, wie Coupa Ihr Unternehmen voranbringt.
Laden Sie unser Datenblatt herunter, um mehr darüber zu erfahren, wie Coupa Ihr Unternehmen dabei unterstützt, Third-Party-Risks zu minimieren. >

Möchten Sie unsere Lösungen in Aktion kennenlernen?
Nehmen Sie an einer Live-Demo teil, in der Sie erfahren, wie Coupa Ihr Unternehmen unterstützt, um Compliance-Ziele zu erreichen und Third-Party-Risks zu minimieren. >

Coupa verwaltet insgesamt fast 1,7 Billionen US-Dollar an kumulierten Geschäftsausgaben seines globalen Kundenstamms und bietet Unternehmen aller Größenordnungen–von Fortune-1000-Unternehmen bis zu den am schnellsten wachsenden Start-ups–auf einer einzigen umfassenden und offenen, cloudbasierten Plattform die Transparenz und Kontrolle, die sie brauchen, um Kosten im Griff zu behalten, Risiken zu minimieren und weiter zu wachsen. Die einzigartige Community Intelligence stützt sich auf die gewaltigen Mengen an Daten, die bei Coupa verarbeitet werden. Sie bietet Echtzeit-Benchmarks und Best-Practice-Vorgaben, die an den messbaren Ergebnissen von Unternehmen auf der ganzen Welt getestet wurden.

Die Business-Spend-Management (BSM)-Plattform versetzt Finanz- und Beschaffungsverantwortliche in die Lage, ihre Ausgaben intelligenter zu verwalten und sich das kollektive Wissen der Coupa Community zunutze zu machen. Investieren auch Sie cleverer.

Weitere Informationen finden Sie auf Coupa.com.

coupa