

## Wie Sie Drittanbieterrisiken für die DORA-Compliance minimieren: Eine Checkliste für Best Practices

Die Einhaltung der Anforderungen des DORA an das Risikomanagement von Drittanbietern umfasst die Implementierung einer Reihe von Best Practices, die darauf ausgelegt sind, Risiken effektiv zu identifizieren, zu bewerten und zu mindern. Diese Best Practices für das Risikomanagement von Drittanbietern sind umsetzbare Schritte, die jeder IT-, Risiko- und Compliance-Fachmann in Betracht ziehen sollte:

-  **1. Gründliche Due-Diligence-Prüfung durchführen:** Bewerten Sie die operationelle Resilienz, Datenschutzmaßnahmen und das gesamte Risikoprofil eines Drittanbieters. Untersuchen Sie deren finanzielle Stabilität, Compliance-Historie und Cybersecurity-Protokolle.
-  **2. Klare Verträge festlegen:** Stellen Sie sicher, dass alle Verträge mit Drittparteien spezifische Klauseln bezüglich Risikomanagement, Datenschutz und DORA-Konformität enthalten. Definieren Sie Rollen, Verantwortlichkeiten und Erwartungen klar.
-  **3. Implementieren Sie kontinuierliches Monitoring:** Richten Sie Mechanismen für die kontinuierliche Überwachung von Aktivitäten und Leistungen Dritter ein. Dies kann regelmäßige Audits, Leistungsbewertungen und Echtzeitüberwachung von Schlüsselrisikoindikatoren umfassen.
-  **4. Bewerten Sie Risiken regelmäßig:** Führen Sie periodische Risikobewertungen durch, um die Auswirkungen von Drittanbietern auf die operationelle Resilienz Ihres Unternehmens zu evaluieren. Dies hilft dabei, neue Risiken zu identifizieren und die Wirksamkeit bestehender Minderungsstrategien zu bewerten.
-  **5. Entwickeln Sie Notfallreaktionspläne:** Arbeiten Sie mit Drittanbietern zusammen, um Notfallreaktionspläne zu entwickeln und zu testen. Stellen Sie sicher, dass diese Pläne mit dem gesamten Vorfallmanagementrahmen Ihrer Organisation und den DORA-Anforderungen übereinstimmen.
-  **6. Pflegen Sie starke Beziehungen:** Bauen und erhalten Sie starke Beziehungen zu Ihren Drittparteien. Entwickeln und pflegen Sie Kommunikationskanäle; regelmäßiger Austausch kann dabei helfen, potenzielle Risiken zu identifizieren und anzugehen.
-  **7. Dokumentation pflegen:** Führen Sie detaillierte Aufzeichnungen über alle Risikomanagementaktivitäten, Bewertungen und Minderungsmaßnahmen. Diese Dokumentation ist entscheidend, um die Einhaltung während regulatorischer Prüfungen und Bewertungen nachzuweisen.
-  **8. Richtlinien überprüfen und aktualisieren:** Überprüfen Sie Ihre Richtlinien für das Risikomanagement bei Drittparteien regelmäßig und aktualisieren Sie diese, um Änderungen in der regulatorischen Landschaft, aufkommende Bedrohungen und Erkenntnisse aus vergangenen Vorfällen zu berücksichtigen.