Drittparteien

Topical Requirement

The Institute of Internal Auditors

Übersetzung durch

DIIR Deutsches Institut für Interne Revision e.V.

Drittparteien Topical Requirement

Das International Professional Practices Framework® (Internationale Grundlagen für die berufliche Praxis) umfasst die Global Internal Audit Standards™, die Topical Requirements und Global Guidance. Die Topical Requirements sind verbindlich und in Verbindung mit den Standards zu verwenden, welche die maßgebliche Grundlage für die erforderlichen Praktiken darstellen.

Die Topical Requirements formulieren klare Erwartungen an die Internen Revisorinnen und Revisoren, indem sie einen Mindestrahmen für die Prüfung bestimmter Risikothemen vorgeben. Das Risikoprofil der Organisation kann es erforderlich machen, dass die Interne Revision zusätzliche Aspekte des Themas berücksichtigt.

Die Einhaltung der Topical Requirements sorgt für konsistente Revisionsleistungen und verbessert die Qualität und Zuverlässigkeit der Revisionsleistungen und -ergebnisse. Letztlich werten die Topical Requirements den Berufsstand der Internen Revision auf.

Interne Revisorinnen und Revisoren müssen gemäß den Global Internal Audit Standards die Topical Requirements anwenden. Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich. Für Beratungsleistungen wird sie empfohlen. Das Topical Requirement ist anwendbar, wenn das Thema:

1. Gegenstand eines Auftrags im Revisionsplan ist,
2. Während der Durchführung eines Auftrags identifiziert wurde oder
3. Gegenstand eines Auftrags ist, der nicht im ursprünglichen Revisionsplan enthalten war.

Nachweise dafür, dass die Anwendbarkeit jeder einzelnen Anforderung des Topical Requirement beurteilt wurde, sind zu dokumentieren und aufzubewahren. Nicht alle einzelnen Anforderungen sind bei jedem Auftrag anwendbar. Wenn Anforderungen ausgeklammert werden, muss eine Begründung dokumentiert und aufbewahrt werden. Die Einhaltung des Topical Requirement ist verbindlich und wird im Rahmen der Qualitätsbeurteilung bewertet.

Drittparteien

Eine Drittpartei ist eine externe Einzelperson, Gruppe oder Einrichtung, mit der eine Organisation (die „primäre Organisation“) eine Geschäftsbeziehung aufbaut, um Produkte oder Dienstleistungen zu erhalten. Die Beziehung kann durch einen Vertrag, eine Vereinbarung oder auf andere Weise formalisiert werden. In diesem Topical Requirement wird der Begriff „Drittpartei“ verwendet. Er bezieht sich auf Verkäufer, Lieferanten, Auftragnehmer, Unterauftragnehmer, ausgelagerte Dienstleister, andere Agenturen und Berater. Der Begriff umfasst Vereinbarungen zwischen einer Drittpartei und ihren Unterauftragnehmern, die oft als „nachgeschaltete“ Unterauftragnehmer bezeichnet werden.

Das Topical Requirement gilt, wenn die Interne Revision Prüfungsaufträge zu Drittparteien und/oder Unterauftragnehmern durchführt, einschließlich solcher, die an vierter oder weiter nachgelagerter Stelle stehen und durch einen Vertrag oder eine Vereinbarung der Drittpartei mit der primären Organisation begründet sind. Interne Revisorinnen und Revisoren sollten dritte und weiter nachgelagerte Parteien auf der Grundlage des Risikos priorisieren, so wie im nachstehenden Abschnitt über das Risikomanagement beschrieben. Interne Revisorinnen und Revisoren müssen alle

Anforderungen anwenden, die sich aus den Ergebnissen der Risikobeurteilung ergeben, und Ausnahmen müssen dokumentiert werden.

Dieses Topical Requirement bezieht sich nicht auf indirekte externe Beziehungen, Interessen oder Verflechtungen mit der primären Organisation, z. B. mit Aufsichtsbehörden, Bevollmächtigten, Treuhändern/Vorstandsmitgliedern, oder interne Beziehungen, z. B. mit Mitarbeitern.

Der Begriff „Drittpartei“ kann je nach Branche oder anderen Zusammenhängen unterschiedlich definiert und verwendet werden. Internen Revisorinnen und Revisoren haben einen gewissen Spielraum und sie sollten sich auf ihr fachliches Urteilsvermögen verlassen, um das Topical Requirement an die Definition des Begriffs „Drittpartei“ der primären Organisation anzupassen.

Die primäre Organisation (die Organisation, die eine Vereinbarung mit einer Drittpartei eingeht) behält die Verantwortung für die Risiken, die mit dem Erreichen ihrer Ziele verbunden sind, selbst wenn sie eine Drittpartei beauftragt, ihr beim Erreichen eines oder mehrerer Ziele zu helfen. Die Zusammenarbeit mit Drittparteien birgt Risiken, die gemäß diesem Topical Requirement identifiziert, beurteilt und durch geeignete Governance-, Risikomanagement- und Kontrollprozesse gesteuert werden müssen. Wenn eine Drittpartei nicht die vertraglich vereinbarte Leistung erbringt, sich an unethischen Praktiken beteiligt oder eine Disruption ihres Geschäfts erfährt, kann dies Auswirkungen auf die primäre Organisation haben. Zu den Kategorien und Beispielen von Risiken im Zusammenhang mit Drittparteien gehören:

- Strategische Aspekte, z. B. die Fähigkeit, die Mission der primären Organisation und/oder übergeordnete Ziele zu erfüllen oder die Auswirkungen von Fusionen und Übernahmen zu bewältigen.
- Reputation, wie z. B. Schäden an der Umwelt oder für die Beziehungen der primären Organisation zu Auftraggebern, Kunden und Stakeholdern oder für deren Vertrauen.
- Ethische Aspekte, wie mangelnde Integrität, Interessenkonflikte, Schmiergelder und Korruption.
- Operative Aspekte wie physische und Informationssicherheit, Insider-Risiko, Unterbrechung von Services und Nichterreichen der Ziele.
- Finanzielle Aspekte, wie die Insolvenz von Drittparteien oder Fraud.
- Die Einhaltung geltender lokaler, nationaler und internationaler regulatorischer Anforderungen.
- Cybersicherheit und sonstige Datensicherheit, z. B. die Kompromittierung und Weitergabe sensibler Daten.
- IT-Aspekte, z. B. der Ausfall von Services zur Unterstützung kritischer Vorgänge.
- Rechtliche Aspekte, wie z. B. Interessenkonflikte, Streitigkeiten und gerichtliche Auseinandersetzungen wegen Vertragsverletzungen.
- Nachhaltigkeit, z. B. in den Bereichen Umwelt, Soziales und Governance. Beispiele hierfür sind Risiken im Zusammenhang mit den Auswirkungen einer Organisation auf die natürliche Umwelt und Risiken im Zusammenhang mit der Interaktion einer Organisation mit dem Gemeinwesen.
- Geopolitische Faktoren, wie Handelsstreitigkeiten/Sanktionen und politische Instabilität.

Der Lebenszyklus eines Drittanbieters besteht aus Auswahl, Vertragsabschluss, Onboarding, Überwachung und Offboarding. Interne Revisorinnen und Revisoren sollten diese Phasen bei der Beurteilung der Anforderungen an Governance, Risikomanagement und Kontrollprozesse berücksichtigen.

Bewertung und Beurteilung von Drittparteien-Governance, -Risikomanagement und -Kontrollprozessen

Dieses Topical Requirement bietet einen konsistenten und umfassenden Ansatz für die Beurteilung der Konzeption und Implementierung von Drittparteien-Governance, -Risikomanagement und -Kontrollprozessen. Die Anforderungen stellen einen Mindestrahmen für die Beurteilung dar.

GOVERNANCE

Anforderungen:

Interne Revisorinnen und Revisoren müssen die folgenden Aspekte der Governance von Drittparteien der primären Organisation beurteilen, einschließlich der Beaufsichtigung durch das Leitungs- und Überwachungsorgan:

A. Es wird ein formeller Ansatz festgelegt, umgesetzt und regelmäßig überprüft, um zu entscheiden, ob ein Vertrag mit einer Drittpartei abgeschlossen werden soll. Der Ansatz umfasst geeignete Kriterien zur Definition und Beurteilung der Ressourcen, die zur Erreichung der Ziele durch die Bereitstellung eines Produkts oder eines Services erforderlich und verfügbar sind.

B. Es werden Richtlinien und Verfahren eingeführt, um Beziehungen mit Drittparteien und Risiken während des gesamten Lebenszyklus der Drittpartei zu definieren, zu beurteilen und zu managen. Die Richtlinien und Verfahren sind auf die geltenden regulatorischen Anforderungen abgestimmt und werden regelmäßig überprüft und aktualisiert, um das Kontrollumfeld zu stärken.

C. Die Aufgaben und Zuständigkeiten der Organisation in Bezug auf das Management von Drittparteien sind definiert, wobei im Einzelnen festgelegt ist, wer Drittparteien auswählt, anleitet, managt, mit ihnen kommuniziert und sie überwacht und wer über die Aktivitäten von Drittparteien informiert werden muss. Es gibt einen Prozess, mit dem sichergestellt wird, dass Personen, denen Aufgaben und Zuständigkeiten für Drittparteien übertragen werden, über die geeigneten Kompetenzen verfügen.

D. Es werden Verfahren für die Kommunikation mit den relevanten Stakeholdern festgelegt, die eine zeitnahe Berichterstattung über den Status der Leistung, der Risiken und der Compliance (insbesondere Verstöße gegen Gesetze und Vorschriften) von vorrangig zu behandelnden Drittparteien umfassen. Drittparteien werden auf Basis von Risiken priorisiert. Zu den relevanten Stakeholdern gehören die Geschäftsleitung und das Überwachungsorgan sowie die Funktionen Beschaffung, Betrieb, Risikomanagement, Compliance, Recht, IT, Informationssicherheit, Personal und andere.

RISIKOMANAGEMENT

Anforderungen:

Interne Revisorinnen und Revisoren müssen die folgenden Aspekte des Risikomanagements für Drittparteien der Organisation beurteilen:

A. Die Prozesse für das Risikomanagement von Drittparteien und deren Dienstleistungen sind standardisiert und umfassend, beinhalten definierte Rollen und Zuständigkeiten und berücksichtigen in ausreichendem Maße die für die Organisation relevanten Hauptrisiken (z. B. strategische, Reputations-, ethische, operative, finanzielle, Compliance-, Cybersicherheits-,

IT-, rechtliche, Nachhaltigkeits- und geopolitische Risiken). Die Einhaltung der Prozesse wird überwacht. Bei Abweichungen werden korrigierende Maßnahmen ergriffen.

B. Die Risiken im Zusammenhang mit Drittparteien werden während ihrer gesamten Lebenszyklen regelmäßig ermittelt und beurteilt. Die Risikobeurteilung dient der Einstufung und Priorisierung von Drittparteien, einschließlich der nachgelagerten Parteien. Auch die Risikoreaktionen werden eingestuft und priorisiert. Die Risikobeurteilung wird regelmäßig überprüft und aktualisiert.

C. Die Risikoreaktionen sind angemessen und genau und entsprechen der Einstufung. Die Risikoreaktionen werden implementiert, überprüft, genehmigt, überwacht, bewertet und bei Bedarf angepasst.

D. Es gibt Prozesse, mit denen von Drittparteien verursachte Probleme gemanagt und gegebenenfalls eskaliert werden, um die Verantwortlichkeit für die Ergebnisse zu gewährleisten und die Wahrscheinlichkeit zu erhöhen, dass die in Verträgen oder anderen Vereinbarungen genannten Bedingungen eingehalten werden. Für den Fall, dass eine Drittpartei nicht auf eskalierte Bedenken reagiert, gibt es Prozesse, mit denen das Management die Risiken der laufenden Geschäftsbeziehung bewertet und je nach Bedarf weitere Aktionen, Abhilfemaßnahmen oder die Beendigung der Geschäftsbeziehung verfolgt.

KONTROLLEN

Anforderungen:

Interne Revisorinnen und Revisoren müssen, priorisiert nach Risiko, die folgenden Kontrollen für Drittparteien beurteilen. Die Bewertung muss die Prozesse des Managements für die laufende Beurteilung und Überwachung von Drittparteien der Organisation umfassen.

A. Es gibt einen soliden Due-Diligence-Prozess für die Beschaffung und Auswahl von Drittparteien mit einem dokumentierten und genehmigten Business Case oder einem anderen relevanten Dokument, das den Bedarf und die Art der Beziehung mit der Drittpartei beschreibt und rechtfertigt.

B. Die Auftragsvergabe und -genehmigung erfolgt gemäß den Richtlinien und Verfahren der Organisation für das Risikomanagement von Drittparteien und umfasst die Zusammenarbeit zwischen den geeigneten Funktionen der Organisation.

C. Die endgültigen Verträge oder Vereinbarungen werden von allen relevanten Stakeholdern, einschließlich Rechts- und Complianceabteilung, überprüft und genehmigt, von autorisierten Personen beider Parteien unterzeichnet und sicher aufbewahrt. Für jeden Vertrag ist ein Vertragsmanager oder Administrator zuständig.

D. Es wird ein genaues, vollständiges und aktuelles Verzeichnis aller Beziehungen zu Drittparteien geführt, z. B. in einem zentralisierten Vertragsmanagementsystem.

E. Dokumentierte Onboarding-Prozesse werden eingerichtet und befolgt, um eine Grundlage dafür zu schaffen, dass Drittparteien die Bedingungen des Vertrags oder der Vereinbarung erfüllen.

F. Es gibt kontinuierliche Überwachungsprozesse, um zu beurteilen, ob Drittparteien während des gesamten Lebenszyklus die Bedingungen des Vertrags oder der Vereinbarung einhalten und ob sie ihren vertraglichen Verpflichtungen nachkommen. Zu den Verfahren gehören die Überprüfung der Zuverlässigkeit der bereitgestellten Informationen sowie die regelmäßige und bei jeder Änderung der Vereinbarung durchgeführte Neubewertung der Leistung.

G. Es werden Verfahren etabliert, um korrigierende Maßnahmen einzuleiten, wenn eine Drittpartei die Erwartungen nicht erfüllt oder ein erhöhtes oder unerwartetes Risiko

darstellt. Diese Verfahren umfassen die Eskalation von Vorfällen je nach Schweregrad, die Durchführung von Überprüfungen nach Vorfällen und die Analyse der Ursachen.

H. Die Termine für das Auslaufen und die Erneuerung von Verträgen werden überwacht, und bei Bedarf werden Verlängerungsmaßnahmen ergriffen.

I. Ein formalisierter Offboarding-Plan wird eingeführt und befolgt, um sicherzustellen, dass die vertraglichen Anforderungen hinsichtlich des Zeitplans und der Erwartungen angemessen berücksichtigt werden. Zu den Prozessen gehören:

- Die Beendigung der Beziehung zu einer Drittpartei.
- Das Ersetzen der Drittpartei, falls erforderlich.
- Die Neuzuweisung der Verwahrung und die Rückgabe oder Vernichtung der bei der Drittpartei gespeicherten sensiblen Daten der Organisation.
- Der Widerruf des Zugriffs der Drittpartei auf Systeme, Tools and Einrichtungen.

Über das Institute of Internal Auditors

Das IIA ist ein internationaler Berufsverband, der weltweit mehr als 265.000 Mitglieder betreut und mehr als 200.000 Zertifizierungen zum Certified Internal Auditor® (CIA®) vergeben hat. Das IIA wurde 1941 gegründet und ist weltweit als führend für Standards, Zertifizierungen, Ausbildung, Forschung und fachlichen Leitlinien für den Berufsstand der Internen Revision anerkannt. Weitere Informationen finden Sie unter theiia.org.

Copyright

September 2025, Übersetzung durch DIIR – Deutsches Institut für Interne Revision e.V.

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