Drittparteien Topical Requirement

Public Consultation Draft

Das International Professional Practices Framework® (Internationalen 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, zusätzliche Aspekte des Themas zu berücksichtigen. 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:

A. Gegenstand eines Auftrags im Revisionsplan ist,
B. während der Durchführung eines Auftrags identifiziert wurde oder
C. 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 Person, Gruppe oder Einheit, mit der eine Organisation eine Geschäftsbeziehung unterhält. Eine Beziehung zu einer Drittpartei kann durch einen Vertrag, eine Vereinbarung oder andere Mittel zur Bereitstellung von Produkten oder Dienstleistungen für die Organisation formalisiert werden. Die Verwendung des Begriffs „Drittpartei“ kann je nach Branche oder anderen Kontexten unterschiedlich sein. Diese Anleitung verwendet den Begriff „Drittpartei“ für Verkäufer, Lieferanten, Auftragnehmer, Unterauftragnehmer, ausgelagerte Dienstleister, andere Agenturen und Berater. Dies umfasst Vereinbarungen zwischen einer Drittpartei und ihren Unterauftragnehmern, die oft als „nachgelagerte“ Auftragnehmer bezeichnet werden.

Dieses Topical Requirement bezieht sich nicht auf indirekte Beziehungen, Interessen oder Verflechtungen mit der primären Organisation, wie z. B. Mitarbeiter, Finanzpartner, Aufsichtsbehörden, Vertreter oder Treuhänder.

Obwohl die primäre Organisation eine Drittpartei damit beauftragen kann, sie bei der Erreichung eines oder mehrerer ihrer Geschäftsziele zu unterstützen, behält die primäre Organisation die Verantwortung für die mit der Erreichung dieser Ziele verbundenen Risiken. Wenn der Vertrag oder die Vereinbarung einer Drittpartei mit der Organisation es dieser erlaubt, Unterverträge mit einer vierten oder weiteren „nachgelagerten" Partei zu schließen, gilt dieses Topical Requirement auch für die Lieferung von Prüfungssicherheit über die Governance und Beaufsichtigung dieser nachgelagerten Beziehungen. In diesen Fällen müssen Interne Revisorinnen und Revisoren alle Anforderungen anwenden, die sich aus den Ergebnissen einer Risikobeurteilung ergeben. Die Ausschlüsse müssen dokumentiert werden.

Die Zusammenarbeit mit Drittparteien birgt Risiken, die gemäß diesem Topical Requirement dargelegt, 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. Kategorien und Beispiele für Risiken in Bezug auf Drittparteien sind:

- Operationelle, wie z. B. Unterbrechung der Leistung oder Nichterreichen der Geschäftsziele.
- Cybersicherheit, z. B. kompromittierte sensible Daten.
- Finanzielle, wie z. B. die Insolvenz eines Anbieters.
- Einhaltung geltender lokaler, nationaler und internationaler regulatorischer Anforderungen.
- Rechtliche, wie z. B. Interessenkonflikte, Streitigkeiten und gerichtliche Auseinandersetzungen wegen Vertragsverletzungen.
- Reputation, wie z. B. Schäden für die Umwelt oder für die Klienten, Kunden oder Stakeholder der primären Organisation.

Der Lebenszyklus einer Drittpartei umfasst die Auswahl, den Vertragsabschluss, das Onboarding, die Überwachung und das Offboarding. Interne Revisorinnen und Revisoren sollten diese Phasen bei der Beurteilung der Anforderungen an Governance, Risikomanagement und Kontrollprozesse berücksichtigen.

Bewertung und Beurteilung von Drittpartei Governance, Risikomanagement und Kontrollprozessen

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

Governance: Bewertung und Beurteilung der Drittparteien-Governance

Anforderungen:

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

A. Es wird ein formeller Ansatz festgelegt, implementiert und regelmäßig überprüft, um zu entscheiden, ob ein Vertrag mit einer Drittpartei abgeschlossen werden soll, um bei der Erreichung eines Geschäftsziels durch die Bereitstellung eines Produkts oder einer Dienstleistung zu unterstützen. Der Ansatz umfasst geeignete Kriterien für die Festlegung und Beurteilung der zur Erreichung der Ziele verfügbaren Ressourcen.

B. Es werden Richtlinien, Verfahren und Prozesse eingeführt, um Beziehungen und Risiken mit Drittparteien über den gesamten Drittpartei-Lebenszyklus hinweg zu definieren, zu beurteilen und zu steuern. Die Richtlinien, Verfahren und Prozesse sind auf die geltenden regulatorischen Anforderungen abgestimmt und werden regelmäßig überprüft und aktualisiert, um das Kontrollumfeld zu stärken.

C. Die Aufgaben und Zuständigkeiten im Drittparteien-Management innerhalb der Organisation sind definiert, wobei im Einzelnen festgelegt wird, wer Drittparteien auswählt, anleitet, steuert, mit ihnen kommuniziert und sie überwacht und wer über die Aktivitäten der Drittparteien informiert werden muss. Es gibt einen Prozess, der sicherstellt, dass die Personen, die mit Aufgaben und Verantwortlichkeiten von Drittparteien betraut werden, über die geeigneten Kenntnisse, Fähigkeiten und Fertigkeiten verfügen.

D. Es werden Kommunikationsprotokolle mit den relevanten Stakeholdern festgelegt, die auch die Berichterstattung über den Status der Leistung, der Risiken und der Einhaltung der Vorschriften durch vorrangig zu behandelnde Drittparteien umfassen. Zu den relevanten Stakeholdern gehören u. a. Geschäftsleitung und Überwachungsorgan, operativer Betrieb, Risikomanagement, Personalabteilung, Informationssicherheit, Rechtsabteilung, Compliance-Abteilung und Einkaufsabteilung.

RISIKOMANAGEMENT: Bewertung und Beurteilung des Drittparteien-Risikomanagements

Anforderungen:

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

A. Die Risikomanagementprozesse für Drittparteien sind standardisiert und umfassend, beinhalten definierte Aufgaben und Verantwortlichkeiten und decken die wichtigsten Risiken (wie finanzielle, operationelle, strategische, Cybersicherheits-, Compliance-, Reputations-, ethische, Nachhaltigkeits-, geopolitische und rechtliche Risiken) ausreichend ab. Die Einhaltung der Prozesse wird überwacht. Bei Abweichungen werden korrigierende Maßnahmen ergriffen.

B. Risiken im Zusammenhang mit Drittparteien werden während des gesamten Lebenszyklus ermittelt und beurteilt. Die Risikobeurteilung dient der Klassifizierung und dem Ranking von Drittparteien und der Priorisierung von Risikoreaktionen. Die Beurteilung wird regelmäßig überprüft und aktualisiert.

C. Die Reaktionen auf die Risiken sind angemessen und genau und entsprechen dem Ranking. Risikoreaktionen werden implementiert, überprüft, genehmigt, überwacht, bewertet und bei Bedarf angepasst.

D. Es gibt Prozesse, mit denen von Drittparteien aufgeworfene Probleme gehandhabt 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 für Abhilfemaßnahmen bis hin zur Beendung der Beziehung.

KONTROLLEN: Bewertung und Beurteilung von Drittpartei-Kontrollen

Anforderungen:

Interne Revisorinnen und Revisoren müssen die folgenden Kontrollen für priorisierte Drittparteien beurteilen, einschließlich der Prozesse des Managements für die laufende Beurteilung und Überwachung der Drittparteien der Organisation:

A. Ein dokumentierter und genehmigter Business Case oder ein anderes einschlägiges Dokument beschreibt und rechtfertigt die Notwendigkeit und die Art der Beziehung zu einer Drittpartei.

B. Es gibt einen soliden Due-Diligence-Prozess für die Beschaffung und Auswahl von Drittparteien. Der Prozess umfasst Kriterien für wichtige Aspekte, wie die Überprüfung von Cybersicherheitsprotokollen, die Durchführung von finanziellen Hintergrundprüfungen und die Verifizierung von Bankdaten.

C. Auftragsvergabe und -genehmigung erfolgen gemäß den Richtlinien, Verfahren und Prozessen der Organisation für das Drittpartei-Risikomanagement und beinhalten die Zusammenarbeit mit den geeigneten Abteilungen der Organisation.

D. Die endgültigen Verträge oder Vereinbarungen werden von allen relevanten Stakeholdern überprüft und genehmigt, falls erforderlich einschließlich Rechtsabteilung und Compliance-Abteilung, von autorisierten Personen beider Parteien unterzeichnet und sicher aufbewahrt. Für alle Verträge wird ein verantwortlicher Vertragsmanager oder Administrator ernannt.

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

F. Es werden dokumentierte Onboarding-Prozesse eingerichtet und befolgt, die es den Drittparteien ermöglichen, die Bedingungen des Vertrags oder der Vereinbarung zu erfüllen.

G. Es gibt fortlaufende Überwachungsprozesse, um zu beurteilen, ob priorisierte Drittparteien während des gesamten Lebenszyklus die Vertrags- oder Vereinbarungsbedingungen erfüllen und ihren vertraglichen Verpflichtungen nachkommen. Zu den Prozessen gehören die Verifizierung der Zuverlässigkeit der bereitgestellten Informationen und die regelmäßige Neubewertung der Leistung bei jeder Änderung der Vereinbarung.

H. 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.

I. Die Termine für Vertragsverlängerungen werden überwacht, und bei Bedarf werden Verlängerungsmaßnahmen ergriffen.

J. Für priorisierte Drittparteien wird ein formalisierter Offboarding-Plan implementiert und befolgt. Zu den Prozessen gehört, wie man:
   - Die Beziehung zu einer Drittpartei beendet.
   - Die Drittpartei ersetzt, falls erforderlich.
   - Die Zuständigkeit neu zuordnet und die gespeicherten sensiblen Daten der Organisation zurückgibt oder vernichtet, die bei der Drittpartei liegen.
   - Der Drittpartei den Zugang auf Systeme, Tools und Einrichtungen entzieht.

Über das Institute of Internal Auditors

Das Institute of Internal Auditors (IIA) ist ein internationaler Berufsverband, der weltweit mehr als 260.000 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 in den Bereichen Standards, Zertifizierungen, Bildung, Forschung und fachliche Leitlinien für den Berufsstand der Internen Revision anerkannt. Weitere Informationen finden Sie unter www.theiia.org.

Haftungsausschluss

Copyright

Februar 2025

