Drittparteien

Topical Requirement

User Guide

The Institute of Internal Auditors

Übersetzung durch

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

Überblick über die Topical Requirements

Die Topical Requirements sind ein wesentlicher Bestandteil der Internationalen Grundlagen für die berufliche Praxis (International Professional Practices Framework®), zusammen mit den Global Internal Audit Standards™ und Global Guidance. Das Institute of Internal Auditors fordert, dass die Topical Requirements in Verbindung mit den Standards angewendet werden, die die maßgebliche Grundlage für die geforderten Praktiken darstellen. Dieses Dokument enthält Referenzierungen zu den Standards als Quelle für ausführlichere Informationen.

Die Topical Requirements formalisieren die Art und Weise, wie Interne Revisorinnen und Revisoren allgegenwärtige Risikobereiche angehen, um die Qualität und Konsistenz innerhalb des Berufsstandes zu fördern. Sie bilden eine Grundlage und liefern relevante Kriterien für die Durchführung von Prüfungsleistungen, die sich auf den Gegenstand eines Topical Requirement beziehen (Standard 13.4 „Bewertungskriterien“). Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich und wird für die Bewertung bei Beratungsleistungen empfohlen. Es ist nicht die Absicht der Topical Requirements, alle potenziellen Aspekte abzudecken, die bei der Durchführung von Prüfungsaufträgen zu berücksichtigen sind. Sie sollen vielmehr einen Mindestsatz an Anforderungen bereitstellen, um eine konsistente, zuverlässige Beurteilung des Themas zu ermöglichen.

Die Topical Requirements sind klar mit dem Drei-Linien-Modell des IIA und den Global Internal Audit Standards verlinkt. Governance, Risikomanagement und Kontrollprozesse sind, in Übereinstimmung mit Standard 9.1 „Verstehen von Governance-, Risikomanagement- und Kontrollprozessen“, die Hauptbestandteile der Topical Requirements. In Verbindung mit dem Drei-Linien-Modell beziehen sich Governance auf Leitungs- und Überwachungsorgane, Risikomanagement auf die zweite Linie und Kontrollen oder Kontrollprozesse auf die erste Linie. Das Management ist sowohl in der ersten als auch in der zweiten Linie vertreten. Die Interne Revision stellt als unabhängiger und objektiver Assurance Provider, der den Leitungs- und Überwachungsorganen Bericht erstattet, die dritte Linie dar (Prinzip 8 „Aufsicht durch das Leitungs- und Überwachungsorgan").

Anwendbarkeit, Risiko und professionelles Urteilsvermögen

Topical Requirements müssen befolgt werden, wenn Interne Revisionen Prüfungsaufträge zu Themen durchführen, für die es ein Topical Requirement gibt, oder wenn Aspekte des Topical Requirement in anderen Prüfungsaufträgen identifiziert werden.

Wie in den Standards beschrieben, ist die Risikobeurteilung ein wichtiger Teil der Planung durch die Revisionsleitung. Die Festlegung der in den Revisionsplan aufzunehmenden Prüfungsaufträge erfordert eine mindestens jährliche Beurteilung der Strategien, Ziele und Risiken der Organisation (Standard 9.4 „Revisionsplan“). Bei der Planung einzelner Prüfungsaufträge müssen die Internen Revisorinnen und Revisoren die für den Auftrag relevanten Risiken beurteilen (Standard 13.2 „Risikobeurteilung zu einem Auftrag“).

Wenn der Gegenstand eines Topical Requirement während des risikobasierten Planungsprozesses der Internen Revision identifiziert und in den Revisionsplan aufgenommen wird, müssen die im Topical Requirement dargelegten Anforderungen zur Beurteilung des Themas im Rahmen der betroffenen Aufträge angewendet werden. Zusätzlich muss das Topical Requirement im Rahmen eines Auftrags

auf seine Anwendbarkeit hin beurteilt werden, wenn die Interne Revision einen (im Plan enthaltenen oder nicht im Plan enthaltenen) Auftrag durchführt und Elemente des Topical Requirement identifiziert werden. Außerdem muss das Topical Requirement auf seine Anwendbarkeit hin beurteilt werden, wenn ein Auftrag erteilt wird, der ursprünglich nicht im Plan vorgesehen war und das Thema umfasst.

Bei der Anwendung des Topical Requirement spielt die professionelle Beurteilung eine wichtige Rolle. Risikobeurteilungen sind die Grundlage für Entscheidungen von Revisionsleitungen, welche Aufträge in den Revisionsplan aufgenommen werden sollen (Standard 9.4). Darüber hinaus nutzen Interne Revisorinnen und Revisoren ihre professionelle Beurteilung, um zu entscheiden, welche Aspekte im Rahmen der einzelnen Aufträge abgedeckt werden sollen (Standards 13.3 „Auftragsziele und Auftragsumfang“, 13.4 „Bewertungskriterien“ und 13.6 „Arbeitsprogramm“).

Es ist nachzuweisen, dass die Anwendbarkeit jeder Anforderung des Topical Requirement beurteilt wurde, einschließlich einer Begründung für den Ausschluss von Anforderungen. Die Einhaltung des Topical Requirement muss unter Nutzung des professionellen Urteils der Prüferinnen und Prüfer, wie in Standard 14.6 „Auftragsdokumentation“ beschrieben, dokumentiert werden.

Das Topical Requirement liefert einen Mindestrahmen für die zu berücksichtigenden Kontrollprozesse, aber Organisationen, die das Risikothema als sehr hoch einschätzen, müssen möglicherweise zusätzliche Aspekte beurteilen.

Verfügt die Interne Revision nicht über die erforderlichen Kompetenzen zur Durchführung von Aufträgen zu einem Thema der Topical Requirements, muss die Revisionsleitung bestimmen, wie die Ressourcen beschafft werden können, und der Geschäftsleitung und dem Überwachungsorgan zeitnah mitteilen, wie sich die Einschränkungen auswirken und wie eine etwaige Ressourcenknappheit gehandhabt werden soll. Die Revisionsleitung trägt die letztendliche Verantwortung dafür, dass die Interne Revision die Topical Requirements einhält, unabhängig davon, wie die Ressourcen beschafft werden (Standards 3.1 „Kompetenz“, 7.2 „Qualifikationen der Revisionsleitung“, 8.2 „Ressourcen“, 10.2 „Management personeller Ressourcen“).

Leistung, Dokumentation und Berichterstattung

Bei der Anwendung der Topical Requirements müssen Interne Revisorinnen und Revisoren auch die Standards einhalten und ihre Tätigkeiten im Einklang mit Domain V („Erbringung von Revisionsleistungen“) durchführen. Die Standards in Domain V beschreiben die Planung von Aufträgen (Prinzip 13 „Plane Aufträge wirksam“), die Durchführung von Aufträgen (Prinzip 14 „Führe die Auftragsarbeiten aus“) und die Kommunikation von Auftragsergebnissen (Prinzip 15 „Kommuniziere Auftragsergebnisse und überwache Maßnahmenpläne“).

Topical Requirements sind entwickelt worden, um konsistente und qualitativ hochwertige Revisionspraktiken zu unterstützen. Lokale Gesetze, Vorschriften, Erwartungen der Aufsichtsbehörden und andere fachlich anerkannte Rahmenwerke können zusätzliche oder spezifischere Anforderungen stellen. Interne Revisorinnen und Revisoren müssen die für die Branche und die Gerichtsbarkeit, in der die Organisation tätig ist, relevanten Gesetze und/oder Vorschriften verstehen und einhalten, einschließlich der erforderlichen Offenlegungen gemäß Standard 1.3 „Rechtmäßiges und ethisches Verhalten“. Interne Revisorinnen und Revisoren haben diese zusätzlichen Anforderungen möglicherweise bereits in ihre Prüfungsprogramme und Prüfverfahren integriert und sollten sie mit dem Topical Requirement abgleichen, um eine angemessene Abdeckung sicherzustellen.

Die Abdeckung des Topical Requirement kann auf Grundlage der professionellen Beurteilung der Prüferinnen und Prüfer entweder im Revisionsplan oder in den Arbeitspapieren des Auftrags dokumentiert werden. Die Anforderungen können von einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Der Nachweis, dass das Topical Requirement auf seine Anwendbarkeit hin geprüft wurde, muss, einschließlich einer Begründung für etwaige Ausschlüsse, aufbewahrt werden.

Qualitätssicherung

Die Standards verlangen, dass die Revisionsleitung ein Programm zur Qualitätssicherung und Verbesserung entwickelt, umsetzt und aufrechterhält, das alle Aspekte der Internen Revision abdeckt (Standard 8.3 „Qualität“). Die Ergebnisse sind der Geschäftsleitung und dem Überwachungsorgan mitzuteilen. In der Kommunikation muss über die Einhaltung der Standards durch die Interne Revision und die Erreichung der Leistungsziele berichtet werden.

Die Einhaltung der Topical Requirements wird im Rahmen von Qualitätsbeurteilungen beurteilt.

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, um der Organisation Produkte, Dienstleistungen, Arbeitskräfte, Fertigung oder IT-Lösungen, wie z. B. Datenspeicherung, -verarbeitung und -pflege, zur Verfügung zu stellen.

> Hinweis
>
> In den Topical Requirements wird die allgemeine Terminologie der Internen Revision verwendet, wie sie in den Global Internal Audit Standards definiert ist. Die Leser sollten die Begriffe und Definitionen im Glossar der Standards nachschlagen.

Der Begriff „Drittpartei“ kann je nach Branche oder anderen Zusammenhängen unterschiedlich verwendet werden. Jede Interne Revision verfügt über einen Ermessensspielraum bei der Anwendung des Topical Requirements, je nachdem, wie die primäre Organisation (die Organisation, die eine Vereinbarung mit einer Drittpartei eingeht) Drittparteien definiert. Im Topical Requirement Drittparteien und im User Guide bezieht sich der Begriff „Drittpartei“ auf Verkäufer, Lieferanten, Auftragnehmer, Unterauftragnehmer, ausgelagerte Dienstleister, andere Agenturen und Berater. Der Begriff „Drittpartei“ umfasst alle derartigen Vereinbarungen, einschließlich derjenigen zwischen einer Drittpartei und ihren Unterauftragnehmern, die häufig als „nachgelagerte Unterauftragnehmer“ oder „Viertpartei“, „Fünftpartei“ oder „n-te Partei“ bezeichnet 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 oder konzerninternen Dienstleistern.

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 Wirksamkeit der Prozesse einer Organisation zum Management ihrer Beziehungen zu Drittparteien kann organisationsweit und/oder auf der Ebene einzelner oder mehrerer Verträge,

Vereinbarungen oder Beziehungen beurteilt werden. Interne Revisorinnen und Revisoren sollten einen Top-Down-Ansatz anwenden, um ein Verständnis für die Richtlinien, Verfahren, Prozesse, Rahmenbedingungen und den Lebenszyklus für Drittparteien der Organisation zu entwickeln. Interne Revisorinnen und Revisoren sollten ihr Urteilsvermögen anwenden, um die Nuancen der Drittpartei-Risiken je nach Branche, Organisation und Auftragsgegenstand zu verstehen. In Übereinstimmung mit Standard 5.1 „Verwendung von Informationen“ sollten Interne Revisorinnen und Revisoren alle Richtlinien und Verfahren in Bezug auf die Informationen zu Drittparteien, auf die sie zugreifen können, kennen und einhalten.

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 Drittparteien und weitere nachgelagerte Parteien auf der Grundlage von Risiken 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 alle Ausschlüsse dokumentieren.

Das Topical Requirement Drittparteien und der User Guide beziehen sich auf die Phasen in der Beziehung einer Organisation zu ihren Drittparteien, die auch als Lebenszyklusphasen bezeichnet werden: Auswahl, Vertragsabschluss, Onboarding, Überwachung und Offboarding. Diese Phasen werden für die Zwecke des Topical Requirement Drittpartien und den User Guide verwendet, auch wenn einige Branchen ihre eigenen Versionen des Lebenszyklus haben. Die Phasen sind:

- Auswahl: Umfasst Verfahren zur Ermittlung des Bedarfs für eine Drittpartei, den Plan für deren Einsatz und die Sorgfaltspflicht bei der Auswahl. Darüber hinaus sollten bei der Auswahl auch die Risiken potenzieller und bereits beauftragter Drittparteien beurteilt werden.
- Vertragsabschluss: Umfasst die Due-Diligence-Prozesse für den Entwurf, die Verhandlung, die Genehmigung und die Umsetzung einer rechtlichen Vereinbarung mit der Drittpartei.
- Onboarding: Beginnt mit der Unterzeichnung des Vertrages zur Aufnahme der Geschäftsbeziehung und schafft die Grundlage für die Erfüllung der Bedingungen des Vertrages oder der Vereinbarung durch die Drittparteien.
- Überwachung: Dazu gehören Verfahren für das „In-Life“-Management und die laufende Überwachung der Drittpartei, nachdem der Vertrag erstellt und genehmigt wurde. Der Ansatz ist in der Regel systematisch und risikobasiert und sollte kontinuierliche Verbesserungen berücksichtigen. Zur Überwachung gehört auch die Erneuerung laufender Verträge oder Vereinbarungen mit Drittparteien, wenn dies erforderlich ist.
- Offboarding: Umfasst Prozesse für die Beendigung von Verträgen und Vereinbarungen, die Aufrechterhaltung einer Ausstiegsstrategie für Drittparteien, die auf der Grundlage von Risiken priorisiert wurden, und die Beendigung von Beziehungen, wenn nötig. Die Prozesse folgen in der Regel einem risikobasierten Ansatz und können einen formellen Ausstiegsplan beinhalten.

Die primäre Organisation 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. Durch die Zusammenarbeit mit Drittparteien können die Kosten der Organisation für die Durchführung ihrer Prozessen möglicherweise gesenkt werden. Dies kann jedoch operationelle

Risiken mit sich bringen, da die primäre Organisation weniger Einblick in die Kontrollprozesse der Drittpartei und weniger Befugnisse über diese hat. 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.

Die primäre Organisation muss die Risiken durch geeignete Governance-, Risikomanagement- und Kontrollprozesse identifizieren, beurteilen und managen. Zu den Kategorien und Beispielen von Risiken im Zusammenhang mit Drittparteien gehören:

- Strategie, z. B. die Fähigkeit, den Auftrag der Organisation und/oder übergeordnete Ziele zu erreichen 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.

Interne Revisorinnen und Revisoren sollten bei der Beurteilung der Anforderungen an Governance-, Risikomanagement- und Kontrollprozesse jede Phase des Lebenszyklus einer Drittpartei berücksichtigen.

Die Anforderungen des Topical Requirements Drittparteien sind in drei Abschnitte unterteilt, so wie in Standard 9.1 „Verstehen von Governance-, Risikomanagement- und Kontrollprozessen“:

- Governance – Klar definierte grundlegende Ziele und Strategien für den Einsatz von Drittparteien zur Unterstützung von Zielen, Richtlinien und Verfahren der Organisation.
- Risikomanagement – Verfahren für Identifikation, Analyse, Management und Überwachung der Risiken beim Einsatz von Drittparteien, einschließlich eines Verfahrens zur unverzüglichen Eskalation von Vorfällen.
- Kontrollen – Vom Management eingerichtete und regelmäßig bewertete Kontrollverfahren zur Minderung der Risiken beim Einsatz von Drittparteien.

Zusätzlich zum Topical Requirement und diesem User Guide können Interne Revisorinnen und Revisoren weitere fachliche Leitlinien zu Drittparteien heranziehen, wie z. B. die IPPF Global Guidance und branchenspezifische Ressourcen.

Überlegungen

Die folgenden Überlegungen können Internen Revisorinnen und Revisoren bei der Umsetzung der Anforderungen im Topical Requirement Drittparteien helfen. Die mit Buchstaben versehenen Aussagen in jedem der nachstehenden Abschnitte geben die entsprechenden Anforderungen des Topical Requirement wieder oder umschreiben sie. Diese nicht verbindlichen Überlegungen dienen der Veranschaulichung, um Beispiele für die Beurteilung der Anforderungen zu geben. Interne Revisorinnen und Revisoren sollten ihr professionelles Urteilsvermögen anwenden, wenn sie entscheiden, was sie in ihre Beurteilungen aufnehmen.

Überlegungen zur Governance

Um zu beurteilen, wie die Governance-Prozesse, einschließlich der Beaufsichtigung durch Geschäftsleitung und Überwachungsorgan, auf die Ziele des Einsatzes von Drittparteien angewandt werden, können Interne Revisorinnen und Revisoren folgende Nachweise überprüfen:

A. Ein formalisierter und dokumentierter risikobasierter Ansatz oder eine Strategie, um zu entscheiden, ob eine Drittpartei eingesetzt werden soll. Der Ansatz wird regelmäßig überprüft und umfasst Folgendes:

- Ein klar definiertes und standardisiertes Verfahren zur Umsetzung des Ansatzes, das von der Organisation genehmigt wurde.
- Budgetierung von Ressourcen auf der Grundlage einer Kosten-Nutzen-Analyse, um die Beauftragung einer Drittpartei zu rechtfertigen und strategische Ausrichtung und Ressourceneffizienz sicherzustellen.
- Die Bewertung der Risiken und Kontrollen durch das Management, einschließlich derjenigen, die sich auf Probleme mit Drittparteien beziehen.
- Angemessene Ressourcen für Auftragsvergabe, Management und Überwachung der Leistung von Drittparteien.
- Die Einbeziehung des Feedbacks von Stakeholdern in den Ansatz oder die Strategie.

B. Richtlinien, Verfahren und andere relevante Unterlagen, die für Definition, Beurteilung und Management der Beziehungen zu Drittparteien während des gesamten Lebenszyklus verwendet werden. Die Richtlinien und Verfahren können Folgendes umfassen:

- Standardisierte Tools und Vorlagen zur Erleichterung wichtiger Governance-, Risikomanagement- und Kontrollprozesse.
- Verfahren zur regelmäßigen Evaluierung der Richtlinien und Verfahren, um ihre Angemessenheit zu bestimmen und sie bei Bedarf zu aktualisieren.
- Festlegung von Kriterien für die Auswahl, die Beauftragung, das Onboarding, die Überwachung und das Offboarding von Drittparteien.
- Identifizierung und regelmäßige Überprüfung der geltenden rechtlichen Anforderungen auf ihre Übereinstimmung mit den Richtlinien und Verfahren.
- Benchmarking-Verfahren zur Ermittlung und zum Vergleich führender Managementpraktiken für Drittparteien.

C. Definierte Rollen und Verantwortlichkeiten, die das Erreichen der Ziele des Einsatzes von Drittparteien unterstützen. Weitere Nachweise können sein:

- Verfahren zur Bewertung, ob die Werte, die Ethik und die soziale Verantwortung der Drittpartei mit den Grundsätzen der primären Organisation übereinstimmen. Das Verfahren sollte vorsehen, wie potenzielle Interessenkonflikte oder unethische Praktiken umgehend angegangen werden können.
- Regelmäßige Schulung des Personals, das Managementaufgaben für den Einsatz von Drittparteien wahrnimmt, und regelmäßige Beurteilung seiner Kompetenzen.
- Ein Verfahren zur Bewertung, ob Schulungen durchgeführt wurden, um ein organisationsweites Bewusstsein für Drittparteien zu schaffen.
- Die Rollen und Verantwortlichkeiten sind auf das Drei-Linien-Modell abgestimmt.

D. Rechtzeitige Kommunikation und Einbindung relevanter Stakeholder während des gesamten Lebenszyklus einer Drittpartei (z. B. Überwachungsorgan, Geschäftsleitung, Beschaffung, Betrieb, Risikomanagement, Compliance, Recht, IT, Informationssicherheit, Personal und andere), einschließlich:

- Informationen über Drittpartei-Risiken und bekannte potenzielle Schwachstellen in Sitzungsprotokollen, Berichten oder E-Mails.
- Informationsaustausch über das Management von Drittparteien und die Förderung der Zusammenarbeit (z. B. durch regelmäßige funktionsübergreifende Sitzungen).

Überlegungen zum Risikomanagement

Um zu beurteilen, wie die Risikomanagementprozesse auf Drittparteien-Ziele angewandt werden, können Interne Revisorinnen und Revisoren Nachweise für Folgendes überprüfen:

A. Standardisierte und umfassende Risikomanagement-Prozesse für die Nutzung von Drittparteien-Dienstleistungen beinhalten definierte Rollen und Verantwortlichkeiten und befassen sich in ausreichendem Maße mit den für die Organisation relevanten Schlüsselrisiken:

- Zu den Verfahren für die Beurteilung und das Management von Drittparteien-Risiken gehört die Frage, wie Schlüsselrisiken
  - ursprünglich identifiziert und berichtet werden,
  - analysiert werden, um ihre Auswirkungen auf die Erreichung der Organisationsziele zu bewerten,
  - gemildert werden, einschließlich Maßnahmenpläne zur Verringerung des Risikos auf ein akzeptables Niveau,
  - überwacht werden, einschließlich Erkennung und Reaktion auf Frühwarnungen und eines Plans für die laufende Berichterstattung, bis die Bedrohungen vollständig beseitigt sind.
- Es wird überwacht, ob die Prozesse eingehalten werden, und bei Abweichungen werden korrigierende Maßnahmen eingeleitet, um zu verhindern, dass die langfristigen Ziele oder die Strategie der Organisation untergraben werden.
- Ein Risikomanagementausschuss oder eine andere Gruppe sorgt für die direkte Beaufsichtigung über Drittparteien und liefert Input für Geschäftsleitung und

Überwachungsorgan. Der Ausschuss hat eine definierte Zielsetzung und tritt regelmäßig zusammen. Zu den Nachweisen können Sitzungsprotokolle gehören.

B. Die Risiken im Zusammenhang mit Drittparteien werden während des gesamten Lebenszyklus regelmäßig ermittelt und beurteilt. Bei der Risikobeurteilung werden Drittparteien eingestuft und priorisiert. Die Reaktionen auf die Risiken werden eingestuft und priorisiert.

- Die primäre Organisation berücksichtigt bei der Risikobeurteilung für Drittparteien Faktoren wie Größe, Reifegrad und Anzahl der beteiligten Drittparteien.
- Die Risikobeurteilung wird dokumentiert und zeigt inhärente Risiken und Restrisiken auf.
- Die Organisation folgt einem Due-Diligence-Verfahren zur Überprüfung und Aktualisierung der Risikobeurteilung.
- Es werden Kriterien festgelegt, um Drittparteien nach ihren Risiken einzustufen und zu priorisieren. Beispiele für solche Kriterien sind:
  - Die erbrachten Dienstleistungen sind für den Betrieb der Organisation von entscheidender Bedeutung.
  - Der finanzielle Wert der Vereinbarung ist wesentlich.
  - Die Beziehung ist neu, wurde schnell eingegangen und/oder ist von langer Dauer.
  - Mehrere externe Parteien sind beteiligt.
  - Die Drittpartei plant, einige oder alle Tätigkeiten an Subunternehmer zu vergeben.
- Die Organisation hält sich an allgemein anerkannte Praktiken zur Risikobeurteilung, einschließlich der Vorgabe, dass die Risikobeurteilung zum frühestmöglichen Zeitpunkt durchgeführt wird, in der Regel in der Auswahlphase bei der Analyse des Angebots und vor dem Onboarding.
- Die Anbieter füllen einen Fragebogen aus, damit Risikoeinstufung und Priorität auf der Grundlage der inhärenten Risiken bestimmt werden können. Die Organisation stellt sicher, dass die Fragebögen von den zuständigen Mitarbeitern ausgefüllt und auf ihre Richtigkeit überprüft werden.
- Die Organisation holt regelmäßig Beiträge zum Drittparteien-Risikomanagement aus Funktionsbereichen wie IT, Beschaffung, unternehmensweites Risikomanagement, Personal, Recht, Compliance, Betrieb, Buchhaltung und Finanzen ein.

C. Maßnahmen zur Risikominderung, -akzeptanz, -beseitigung und -teilung werden festgelegt und passen zur Risikoeinstufung.

- Die Reaktionen auf die Risiken werden dokumentiert und umfassen auch die Berücksichtigung des Kontrollumfelds der Drittpartei.
- Dokumentation, dass Reaktionen auf Risiken, die die Risikotoleranz der primären Organisation überschreiten, auf ihre Angemessenheit hin überprüft werden, insbesondere wenn die Risiken akzeptiert werden. Zu den Maßnahmen gehören auch solche, die sich auf mögliche Interessenkonflikte mit Drittparteien beziehen.

D. Prozesse zum Management und zur Eskalation von Drittparteien-Risiken, einschließlich der Art und Weise, wie der Grad der Bedrohung oder des Risikos bewertet, zugewiesen und priorisiert wird. Die Überprüfung kann auch Folgendes identifizieren:

- Definitionen und Erklärungen der Risikostufen der Organisation – z. B. hoch, mittel und niedrig – sowie Eskalationsverfahren für jede Risikokategorie.
- Liste der Drittparteien, geordnet nach den identifizierten Risiken und dem Stand der Risikominderung für alle Risikoereignisse.
- Anwendbare rechtliche, regulatorische und Compliance-Anforderungen.
- Auswirkungen von Risiken finanzieller und nicht-finanzieller Art (z. B. Reputation).
- Verfahren zur Unterrichtung des Managements und der Mitarbeiter über Drittparteien-Risiken, einschließlich einer regelmäßigen Berichterstattung über das Risikoprofil an Geschäftsleitung und Überwachungsorgan (oder ein anderes geeignetes Gremium). Die Mitteilungen sollten aktuelle Informationen über die Behebung von bei priorisierten Drittenparteien festgestellten Problemen beinhalten.
- Verfahren zur Neubeurteilung der Einstufung und Priorisierung, wenn sich Risikobereitschaft und Risikotoleranz der primären Organisation ändern.

Überlegungen zu Kontrollen

Um zu beurteilen, wie die Kontrollprozesse auf die Beziehungen zu Drittparteien angewandt werden, können Interne Revisorinnen und Revisoren die Nachweise für Folgendes überprüfen:

A. Es gibt ein solides Due-Diligence-Verfahren für die Beschaffung und Auswahl von Drittparteien mit einem dokumentierten und genehmigten Business Case oder anderen relevanten Unterlagen, in denen der Bedarf für und die Art der Beziehung mit der Drittpartei beschrieben und begründet werden.

- Der Business Case kann auch
  - auf die Risiken für die Fähigkeit der Drittpartei, die Erwartungen zu erfüllen, und die möglichen Auswirkungen auf die Organisation eingehen,
  - eine detaillierte Kosten-Nutzen-Analyse umfassen.
- Etablierte Beschaffungsprozesse – wie Ausschreibungen, Angebotsanfragen und Sole Sourcing – werden eingehalten. Die Prozesse umfassen:
  - Kriterien für wichtige Aspekte, wie z. B. die Überprüfung von Cybersicherheitsverfahren, die Überprüfung von Bankdaten, die Durchführung von finanziellen Hintergrundprüfungen und die Untersuchung der Organisationsstruktur der Drittpartei, des Strafregisters, von Führungszeugnissen, von politischen Aktivitäten und der Verbindungen zu kriminellen Aktivitäten.
  - Gut definierte Auswahlkriterien, u. a. zur Beurteilung der bisherigen Leistungen, der Referenzen, der Reputation und der Vertragskosten.
  - Due-Diligence-Prüfung zur Gewährleistung einer angemessenen Auswahl von Anbietern, z. B. Bildung funktionsübergreifender Teams zur Überprüfung von Angeboten. Um das Risiko der Voreingenommenheit zu mindern, umfassen die Kontrollen für Prüfungsteams Verfahren für die Teamzusammensetzung und Anforderungen für die Offenlegung potenzieller Interessenkonflikte.
  - Gebührende Sorgfalt bei der Beurteilung des Kontrollumfelds des Dritten, z. B. durch einen Besuch vor Ort oder die Überprüfung der folgenden Unterlagen der Drittpartei:

- Berichte zur System- und Organisationskontrolle (SOC).
- Finanzielle Stabilität.
- Gründungsurkunde oder Bescheinigung der guten Reputation.
- Transparenz bei der Entscheidungsfindung durch das Management und wichtige Stakeholder.
- Organisationsstruktur.
- Operative Stabilität.
- Cybersicherheitsverfahren.
- Einhaltung einschlägiger Gesetze, Vorschriften und Standards.
- Ethik.
- Geschichte mit der primären Organisation.
- Reputation.

  - Nachweis, dass potenzielle Anbieter oder Auftragnehmer erst dann in die Vertragsphase des Lebenszyklus eintreten, wenn die relevanten Due-Diligence-Prozesse durchgeführt und die Ergebnisse analysiert wurden.

B. Richtlinien und Verfahren für die Auftragsvergabe sind festgelegt und werden befolgt.

- Verträge werden in eindeutiger Form abgefasst.
- Die wichtigsten Risiken werden bereits bei der Vertragsgestaltung berücksichtigt und dafür relevante Klauseln werden aufgenommen. Probleme, die einer Lösung bedürfen, werden in dieser Phase mit der Drittpartei besprochen.
- Die wesentlichen Bestandteile von Verträgen werden auf der Grundlage der Vertragsrichtlinien und -verfahren der Organisation und der Prioritätsstufe der Drittpartei festgelegt. Die Elemente können umfassen:
  - Geheimhaltungsvereinbarungen (Datenschutz).
  - Beendigungsklauseln und definierte Parameter für den Datenzugriff.
  - Anforderungen an die Cybersicherheit, u. a. für den Zugang und die gemeinsame Nutzung aller Daten und die Meldung von Vorfällen oder Verstößen innerhalb einer bestimmten Frist.
  - Anforderungen an die Benachrichtigung über eine Sicherheitsverletzung, die die Daten der primären Organisation betrifft.
  - Ein standardisiertes Verfahren zur Überprüfung der Identität der Drittpartei, einschließlich des vollständigen juristischen Namens, der Adresse, des/der physischen Standorts/e und der Website. Eine gängige Praxis ist die Verwendung einer Checkliste während des Identifizierungsprozesses und die Überprüfung der Richtigkeit der Informationen.
  - Klar definierte Leistungsvereinbarungen, in denen die erwarteten Ergebnisse und die Rechte, Pflichten, Sanktionen, Belohnungen und Verantwortlichkeiten jeder Partei festgelegt sind, einschließlich der Verantwortung für die Bezahlung der Arbeitskosten (einschließlich nachgeordneter Subunternehmer).
  - Eine Klausel über das Prüfungsrecht, die auch nachgelagerte Unterauftragnehmer einschließt, oder die Forderung nach einem Nachweis, dass ein seriöser,

unabhängiger Assurance Provider die Parteien geprüft hat. Ohne eine Klausel über das Prüfungsrecht kann die Fähigkeit der Internen Revision, Prüfungssicherheit zu erlangen oder zu liefern, eingeschränkt sein.

- Die primäre Organisation hat Zugriff auf die Berichte zur Beurteilung der Kontrollen von unabhängigen Prüfern, z. B. zu den Berichten über Finanzen, Compliance, Datensicherheit, wie z. B. International Standard on Assurance Engagements oder SOC-Berichte.
  - Wenn man sich auf die Arbeit der externen Prüfer der Drittpartei verlässt, werden die Dokumente überprüft, um die Zuverlässigkeit zu gewährleisten.
  - SOC-Berichte werden verwendet, um unzureichende Risiko- und Änderungsmanagementprozesse aufzuzeigen.

- Die Richtlinien und Verfahren betreffen alle Komponenten, die für bestimmte Organisationen oder Vertragsarten wichtig sind:
  - Umwelt- und Nachhaltigkeitsklauseln.
  - Whistleblowing-Verfahren.
  - Anforderungen für die Beurteilung von Leistungsmessungen.
  - Geprüfter Business-Continuity-Plan für Drittparteien.
  - Einsatz von künstlicher Intelligenz bei der Erbringung von Dienstleistungen.
  - Klare Identifizierung, Offenlegung und Bedingungen und klarer Umfang für alle nachgelagerten Tätigkeiten durch Unterauftragnehmer.
  - Änderungsmanagementprozess, der festlegt, wie mit Änderungen des Umfangs, der Bedingungen oder der betrieblichen Anforderungen (z. B. technologische Änderungen oder Aktualisierungen von Vorschriften) während der Vertragslaufzeit umgegangen werden soll.
  - Begrenzung der Anzahl der Änderungsaufträge oder der Beträge, die in Rechnung gestellt werden können.

- Richtlinien und Verfahren erfordern eine formelle Abnahme der Endprodukte, bevor eine Zahlung erfolgt oder ein Einbehalt freigegeben wird.
- Drittparteien sind verpflichtet, ihre Ethikrichtlinien oder ihren Verhaltenskodex mitzuteilen und/oder sich an die Richtlinien der primären Organisation zu halten.
- Wenn die Drittpartei den Vertrag anbietet, hat die primäre Organisation eine rechtliche Prüfung durchgeführt, und die Hauptrisiken sind bekannt und werden durch eine geeignete Strategie zur Risikominderung unterstützt.

C. Finalisierte Verträge oder Vereinbarungen werden von den zuständigen Stakeholdern, einschließlich der Rechtsabteilung und der Compliance-Abteilung, überprüft und genehmigt, sicher aufbewahrt und einem Vertragsmanager oder -administrator zur Verantwortung zugewiesen.

- Ein Vertrag oder ein anderes offizielles Dokument, das eine ausgelagerte Beziehung und die Verpflichtung der Drittpartei bestätigt, sowie ein Nachweis über alle erforderlichen rechtlichen und Compliance-Überprüfungen.

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

- Ein Prozess zur Aufnahme neuer Verträge oder Vereinbarungen mit Drittparteien in das Verzeichnis oder System.
- Ein Prozess zur Eingabe potenzieller Drittparteien in das Lieferantensystem und zu deren Löschung, wenn der Vertrag nicht genehmigt wird.
- Ein Prozess zur Entfernung von Verträgen oder Vereinbarungen mit Drittparteien aus dem Verzeichnis oder System.
- Ein Nachverfolgungssystem, um Probleme mit bestimmten Auftragnehmern oder Lieferanten zu dokumentieren.
- Ein Überprüfungsprozess, um festzustellen, ob die Grundgesamtheit der Drittparteien korrekt und vollständig ist.

E. Es werden dokumentierte Onboarding-Prozesse eingerichtet und befolgt, die es den Drittparteien ermöglichen, die Bedingungen des Vertrags oder der Vereinbarung zu erfüllen. Bei den Überprüfungen kann auch Folgendes verifiziert werden:

- Standardisierte Onboarding-Verfahren stellen sicher, dass alle erforderlichen Unterlagen, Schulungen und Compliance-Überprüfungen abgeschlossen sind.
- Die Systeme und Prozesse der Drittparteien können nahtlos in die Technologie der primären Organisation integriert werden.
- Gemeinsame Systeme sind kompatibel und sicher. Der Nachweis kann ergänzende Kontrollen der Anwenderunternehmen im Rahmen der SOC-Berichterstattung umfassen.
- Die primäre Organisation beurteilt die Business-Continuity-Pläne der Drittpartei, die die Aufrechterhaltung des Services in Notfällen gewährleisten. Für mögliche Störungen sind Notfallpläne vorgesehen.

F. Prozesse für die laufende Überwachung der Leistung von Anbietern in Bezug auf die Vertrags- oder Vereinbarungsziele, einschließlich der Bewertung der wichtigsten Leistungsindikatoren.

- Die Überwachungsprozesse fließen in die Risikobeurteilung für Drittparteien ein, und festgestellte Kontrollschwächen werden überprüft, eskaliert und bei Bedarf behoben.
- Berichte oder Beobachtungen zu Prozessen, Technologien und Tools, die für die Überwachung in Echtzeit eingesetzt werden.
- Prozesse, die sicherstellen, dass die Zahlungen gemäß den Vertrags- oder Vereinbarungsbedingungen erfolgen, z. B. Einhaltung von Projektzeitplänen, Meilensteinen und Kommunikationsanforderungen. Zahlungen werden nur an zugelassene Auftragnehmer geleistet, die die Onboarding-Phase abgeschlossen haben und in das Zahlungssystem für Lieferanten aufgenommen wurden. Wenn im Vertrag Leistungen festgelegt sind, werden die Abschlusszahlungen erst geleistet, wenn die Leistungen überprüft worden sind.
- Überwachung der Kontrollkosten im Zusammenhang mit Vereinbarungen mit Drittparteien, um den Wert und die Rentabilität der Investition zu ermitteln. Ergebnisse von Kosten-Nutzen-Analysen werden für die Neuverhandlung von Verträgen genutzt.

- Prozesse zur Verhängung von Sanktionen bei Nichteinhaltung von vertraglichen oder vereinbarten Leistungen. Sanktionen werden berechnet und in Rechnung gestellt, wenn sie anfallen.
- Die risikobasierte Einstufung der priorisierten Drittparteien wird regelmäßig neu bewertet, wenn es Änderungen an einer Vereinbarung gibt und wenn ein Vertrag kurz vor dem Auslaufen oder der automatischen Erneuerung steht.
- Überprüfungen von priorisierten Drittparteien, z. B. vor Ort oder durch vierteljährliche Geschäftsüberprüfungen, um Kontrollen und betriebliche Integrität zu validieren.
- Belege für eine zusätzliche laufende Überwachung können sein:
  - Analysen der finanziellen Stabilität der Drittpartei.
  - Beurteilungen von Beschwerden über die Drittpartei.
  - Überprüfung von Berichten unabhängiger Prüfer durch das Management, z. B. International Standard on Assurance Engagements, Statements on Standards for Attestation Engagements, Finanz-, Prüfungs-, Compliance- und Datensicherheitsberichte von Drittparteien, ISO-Zertifizierungen.
  - Überprüfungen der von der Drittpartei durchgeführten Business-Resilience-Tests durch das Management, einschließlich aller wesentlichen festgestellten Probleme.
  - Bedingungen und Beschränkungen für den Einsatz von Unterauftragnehmern oder nachgeschalteten Stellen.
  - Bewertung der ethischen Werte, der Kultur und des Verhaltens der Drittpartei.
  - Antworten auf Medienanfragen.
  - Bewertung von Datenschutz- und Cybersicherheitsverfahren zum Schutz der Speicherung und Übertragung von Daten und Informationen der primären Organisation, einschließlich der Nutzung fortschrittlicher Technologien wie künstlicher Intelligenz.
  - Identifizierung von Möglichkeiten zur kontinuierlichen Verbesserung der Leistung und zur Erfüllung der Vertrags- oder Vereinbarungsziele durch die Organisation.
  - Überprüfung der Funktionstrennung.

G. Verfahren zur Einleitung korrigierender Maßnahmen bei festgestellten Vorfällen, wenn eine Drittpartei die Anforderungen eines Vertrags oder einer Vereinbarung nicht erfüllt oder wenn die Handlungen der Drittpartei das Risiko für die primäre Organisation erhöhen.

- Verfahren für die Eskalation von Vorfällen auf der Grundlage der Schwere des Vorfalls und der Priorität der Drittpartei.
- Überprüfung nach einem Vorfall, einschließlich Analyse der Grundursache.

H. Prozesse zur Bereitstellung von Warnmeldungen für Verträge und Vereinbarungen, die bald ablaufen oder automatisch erneuert werden. Zu den Prozessen der automatischen Erneuerung gehört die Überprüfung von Folgendem:

- Leistung der Drittpartei.
- Vertrags- oder Vereinbarungsbedingungen und etwaige Nachträge.
- Risikofaktoren.

I. Ein formalisierter Offboarding-Plan ist implementiert und wird befolgt, um sicherzustellen, dass die vertraglichen Anforderungen in Bezug auf Zeitplan und Erwartungen angemessen berücksichtigt werden, auch für alle nachgelagerten Subunternehmer.

- Checklisten oder Interviews mit den wichtigsten Stakeholdern, um die Wirksamkeit der Sicherheitsmaßnahmen zu gewährleisten.
- Informationen oder Daten über die Organisation, die sich in der Obhut einer Drittpartei befinden, wurden zurückgegeben oder vernichtet.
- Der Zugriff der Drittpartei auf die Daten, Systeme oder Einrichtungen der Organisation wurde widerrufen.
- Die Vermögenswerte der primären Organisation, wie Geräte, Softwarelizenzen, geistiges Eigentum und Dokumentation, wurden zurückgegeben.
- Wenn einer Drittpartei aus wichtigem Grund gekündigt wird, werden die mildernden Umstände oder Risiken ermittelt und an die Geschäftsleitung und/oder das Überwachungsorgan weitergeleitet.
- Wenn der Vertrag einer priorisierten Drittpartei gekündigt wird, ist er auf der Grundlage derselben Risikobeurteilung zu ersetzen, es sei denn, der Vertrag ist erfüllt oder wird nicht mehr benötigt.

Anhang A. Praktische Anwendungsbeispiele

Die folgenden Beispiele beschreiben Szenarien, in denen das Topical Requirement Drittparteien anwendbar wäre:

Beispiel 1: Ein Revisionsauftrag im Revisionsplan umfasst eine Dienstleistung oder ein Ergebnis, dass derzeit von einer Drittpartei geliefert wird..

Wenn die Interne Revision ihren risikobasierten Planungsprozess abschließt und einen oder mehrere Aufträge in den Revisionsplan aufnimmt, deren Leistungen oder Ergebnisse derzeit von Drittparteien im Rahmen eines Vertrags oder einer Vereinbarung erbracht werden, ist die Anwendung des Topical Requirements verbindlich.

Nicht jede Anforderung im Topical Requirement wird für jeden Auftrag anzuwenden sein. Wenn Interne Revisorinnen und Revisoren nach ihrem fachlichen Ermessen zu dem Schluss kommen, dass eine oder mehrere Anforderungen des Topical Requirements Drittparteien nicht anwendbar sind und diese daher aus einem Auftrag ausgeklammert werden sollen, müssen sie die Gründe für den Ausschluss dieser Anforderungen dokumentieren und aufbewahren. Der Grund für den Ausschluss bestimmter Anforderungen könnte beispielsweise darin liegen, dass die Interne Revision festgestellt hat, dass die Organisation bei geschäftskritischen Dienstleistungen nur in geringem Maße auf Drittparteien angewiesen ist, oder dass es sich um eine etablierte Beziehung mit geringen finanziellen Auswirkungen handelt.

Beispiel 2: Drittpartei-Risiken werden im Rahmen eines Prüfungsauftrags zu einem anderen Thema als Drittparteien oder Vertragsmanagement festgestellt.

Interne Revisorinnen und Revisoren können bei der Beurteilung eines Prozesses, der ursprünglich nicht mit Drittparteien oder dem Vertragsmanagement in Verbindung gebracht wurde, ein erhebliches Drittparteien-Risiko feststellen. Zum Beispiel erfahren sie bei der Planung eines Auftrags zur Beurteilung von Datenspeicherungen, dass Cloud-Dienste durch eine Drittpartei erbracht werden. Bei Gesprächen mit dem Management der von der Drittpartei erbrachten Dienstleistung stellen die Internen Revisorinnen und Revisoren Cybersicherheits-Risiken im Zusammenhang mit der Drittpartei fest.

Sobald relevante Risiken identifiziert sind, müssen Interne Revisorinnen und Revisoren sowohl die Topical Requirements Drittparteien als auch die Topical Requirements Cybersicherheit überprüfen und ermitteln, welche Anforderungen anwendbar sind. Die Prüfer könnten den Governance-Prozess für Drittparteien oder den Risikomanagementprozess für Drittparteien aus dem Auftragsumfang ausschließen und sich auf die Kontrollen über die von der Drittpartei erbrachten und zu prüfenden Services konzentrieren. Dieselbe fachliche Beurteilung gilt für die Anwendung des Topical Requirements Cybersicherheit. Die Prüfer müssen in den Arbeitspapieren zu dem Auftrag die Gründe für den Ausschluss von Anforderungen aus den Topical Requirements Drittparteien und Cybersicherheit dokumentieren und die Dokumentation aufbewahren.

Beispiel 3: Ein Auftrag bezüglich einer Drittpartei, der ursprünglich nicht im Revisionsplan enthalten war, wird benötigt.

Innerhalb der Organisation tritt ein Problem auf, in das eine priorisierte Drittpartei verwickelt ist und das die sofortige Aufmerksamkeit der Internen Revision erfordert. Es handelte sich um ein Kontrollversagen. Die Revisionsleitung sollte sich mit Geschäftsleitung und Überwachungsorgan darüber verständigen, dass der Revisionsplan und die Ressourcen der Internen Revision neu priorisiert werden, um dem Bedarf Rechnung zu tragen. Die Prüfer sollten gemeinsam mit dem betroffenen Management Auftragsziele für die Bewertung der Situation und Empfehlungen zur Vermeidung künftiger Vorfälle entwickeln. Die Revisionsleitung sollte die Topical Requirements überprüfen, um den Umfang des Auftrags festzulegen, zu bestimmen, welche Anforderungen anzuwenden sind, und etwaige Ausnahmen entsprechend dokumentieren.

Anhang B. Optionales Dokumentationstool

Von Internen Revisorinnen und Revisoren wird erwartet, dass sie mithilfe ihres fachlichen Urteils die Anwendbarkeit der Anforderungen auf der Grundlage der Risikobeurteilung bestimmen und die Ausnahmen von bestimmten Anforderungen angemessen dokumentieren. Das Topical Requirement kann auf der Grundlage des professionellen Urteils der Prüfer im Revisionsplan oder in den Arbeitspapieren zum Auftrag dokumentiert werden. Die Anforderungen können in einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Das nachstehende druckbare Formular bietet eine Möglichkeit, die Einhaltung des Topical Requirements Drittparteien zu dokumentieren, seine Verwendung ist aber nicht verbindlich.

Drittparteien-Governance

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Drittparteien-Risikomanagement

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Drittparteien-Kontrollen

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.

Haftungsausschluss

Das IIA veröffentlicht dieses Dokument zu Informations- und Bildungszwecken. Dieses Material soll keine endgültigen Antworten auf spezifische individuelle Umstände geben und ist daher nur als Leitlinie gedacht. Das IIA empfiehlt, für jede spezifische Situation unabhängigen Expertenrat einzuholen. Das IIA übernimmt keine Verantwortung, falls sich jemand ausschließlich auf dieses Material verlässt.

Copyright

September 2025

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