Third-Party

Topical Requirement

The Institute of Internal Auditors

Vertaald door

Instituut van Internal Auditors Nederland

Third-Party Topical Requirement[1]

Het International Professional Practices Framework® bestaat uit Global Internal Audit Standards™, Topical Requirements en Global Guidance. Topical Requirements zijn verplicht en moeten worden gebruikt in combinatie met de Global Internal Audit Standards, die de gezaghebbende basis vormen voor de beroepspraktijk.

Topical Requirements bieden duidelijke verwachtingen voor internal auditors door een minimum baseline vast te stellen voor het auditen van specifieke risicogebieden. Het risicoprofiel van de organisatie kan vereisen dat internal auditors aanvullende aspecten van het onderwerp in overweging nemen.

Naleving van de Topical Requirements verhoogt de consistentie waarmee internal auditdiensten worden uitgevoerd en verbetert de kwaliteit en betrouwbaarheid van internal auditdiensten en -resultaten. Uiteindelijk zullen de Topical Requirements het beroep van internal auditor op een hoger plan brengen.

Internal auditors moeten de Topical Requirements toepassen in overeenstemming met de Global Internal Audit Standards. Conformiteit met de Topical Requirements is verplicht voor assurancediensten en wordt aanbevolen voor adviesdiensten. De Topical Requirement is van toepassing als het onderwerp één van de volgende is:

1. Het onderwerp van een opdracht in het interne auditplan.
2. Geïdentificeerd tijdens het uitvoeren van een opdracht.
3. Het onderwerp van een opdrachtverzoek dat niet in het oorspronkelijke interne auditplan stond.

Bewijs dat elke vereiste in de Topical Requirement is beoordeeld op toepasbaarheid moet worden gedocumenteerd en bewaard. Het is mogelijk dat niet alle individuele vereisten in elke opdracht van toepassing zijn; als vereisten worden uitgesloten, moet een reden hiervoor worden gedocumenteerd en bewaard. Conformiteit met de Topical Requirement is verplicht en wordt geëvalueerd tijdens kwaliteitstoetsingen.

Third parties

Een third party is een externe persoon, groep of entiteit waarmee een organisatie ("de primaire organisatie") een zakelijke relatie aangaat om producten of diensten te verkrijgen. De relatie kan worden geformaliseerd door middel van een contract, overeenkomst of andere middelen. In deze Topical Requirement wordt de term "third party" gebruikt om te verwijzen naar verkopers, leveranciers, aannemers, onderaannemers, uitbestede dienstverleners, andere instanties en consultants. De term omvat overeenkomsten tussen een third party en zijn onderaannemers, vaak "downstream" onderaannemers genoemd.

[1]Deze vertaling is met de grootste zorgvuldigheid uitgevoerd, maar bij discussie over de vertaling en in het kader van het CIA-examen is de originele, Engelstalige tekst van toepassing. In deze vertaling zijn Engelse termen behouden voor woorden die in het spraakgebruik ingeburgerd zijn danwel tot mogelijke onduidelijkheid zouden leiden bij een vertaling. Voor deze vertalingen geldt het Auteursrecht.

De Topical Requirement is van toepassing wanneer de interne auditfunctie assurance-opdrachten uitvoert naar third parties en/of eventuele uitbestede relaties, inclusief die vierde of verder stroomafwaarts, die zijn toegestaan door het contract of de overeenkomst van de third party met de primaire organisatie. Internal auditors moeten third parties en verdere downstreampartijen prioriteren op basis van risico, zoals beschreven in het gedeelte over risicomanagement hieronder. Internal auditors moeten alle vereisten toepassen zoals aangegeven door de resultaten van de risicobeoordeling, en uitzonderingen moeten worden gedocumenteerd.

Deze Topical Requirement is niet bedoeld voor indirecte externe relaties, belangen of betrokkenheid bij de primaire organisatie, zoals regelgevers, vertegenwoordigers, trustees/bestuursleden, of interne relaties, zoals werknemers.

De term "third party" kan verschillend gedefinieerd en gebruikt worden op basis van de sector of andere context. Internal auditors hebben flexibiliteit en moeten vertrouwen op hun professionele oordeel om de Topical Requirement aan te passen aan de definitie van third party van de primaire organisatie.

De primaire organisatie (de organisatie die een overeenkomst met een third party aangaat) blijft verantwoordelijk voor de risico's die gepaard gaan met het behalen van haar doelstellingen, zelfs als ze een third party inschakelt om haar te helpen één of meerdere doelstellingen te behalen. Werken met third parties brengt risico's met zich mee die moeten worden geïdentificeerd, beoordeeld en beheerd door middel van passende bestuurs-, risicomanagement- en controleprocessen, zoals uiteengezet in deze thematische vereiste. Als een third party niet presteert zoals gecontracteerd, deelneemt aan onethische praktijken of een bedrijfsstoring ondervindt, kan dit gevolgen hebben voor de primaire organisatie. Categorieën en voorbeelden van risico's met betrekking tot third parties zijn onder andere:

- Strategisch, zoals het vermogen om de missie en/of doelstellingen op hoog niveau van de primaire organisatie te realiseren of om de impact van fusies en overnames te managen.
- Reputatieschade, zoals schade aan het milieu of aan de relatie en het vertrouwen van de primaire organisatie met klanten, cliënten en belanghebbenden.
- Ethisch, zoals gebrek aan integriteit, belangenverstrengeling, smeergeld en corruptie.
- Operationeel, zoals fysieke en informatiebeveiliging, insiderrisico, dienstverstoringen en het niet behalen van de doelstellingen.
- Financieel, zoals insolventie van third parties en fraude.
- Voldoen aan toepasselijke lokale, nationale en internationale regelgevende vereisten.
- Cyberbeveiliging en andere gegevensbescherming, zoals het compromitteren en lekken van gevoelige gegevens.
- Informatietechnologie, zoals het ontbreken van diensten om kritieke operaties te ondersteunen.
- Juridisch, zoals belangenverstrengeling, geschillen en rechtszaken wegens contractbreuk.

- Duurzaamheid, zoals milieu, maatschappij en bestuur. Voorbeelden hiervan zijn risico's met betrekking tot de impact van een organisatie op de natuurlijke omgeving en risico's met betrekking tot de interacties van een organisatie met gemeenschappen.
- Geopolitiek, zoals handelsgeschillen/sancties en politieke instabiliteit.

De levenscyclus van een third party bestaat uit selecteren, contracteren, onboarding, monitoring en offboarding. Internal auditors moeten rekening houden met deze fasen bij het beoordelen van de vereisten voor governance, risicomanagement en beheersprocessen.

Governance, risicomanagement en beheersprocessen van third parties evalueren en beoordelen

Deze Topical Requirement biedt een consistente, allesomvattende aanpak voor het beoordelen van het ontwerp en de implementatie van governance-, risicomanagement- en beheersprocessen van third parties. De vereisten vormen een minimale basis voor de beoordeling.

GOVERNANCE

Vereisten:

Internal auditors moeten de volgende aspecten van het bestuur van third parties door de primaire organisatie beoordelen, inclusief het toezicht door de raad van bestuur:

A. Er wordt een formele aanpak opgesteld, geïmplementeerd en periodiek herzien om te bepalen of er een contract met een third party moet worden gesloten. De aanpak omvat passende criteria voor het definiëren en beoordelen van de middelen die nodig en beschikbaar zijn om doelstellingen te halen door een product of dienst te leveren.

B. Beleid en procedures worden opgesteld om relaties en risico's met third parties te definiëren, beoordelen en beheren gedurende de gehele levenscyclus van third parties. Het beleid en de procedures zijn afgestemd op de toepasselijke wettelijke vereisten en worden periodiek herzien en bijgewerkt om de controleomgeving te versterken.

C. De managementrollen en -verantwoordelijkheden van de organisatie met betrekking tot third parties zijn gedefinieerd, waarbij gedetailleerd is vastgelegd wie third parties selecteert, aanstuurt, beheert, met hen communiceert en toezicht houdt en wie op de hoogte moet worden gesteld van activiteiten van third parties. Er bestaat een proces om ervoor te zorgen dat personen die rollen en verantwoordelijkheden bij third parties krijgen de juiste competenties hebben.

D. Protocollen voor communicatie met relevante belanghebbenden zijn gedefinieerd en omvatten tijdige rapportage over de status van de prestaties, risico's en naleving (met name overtredingen van wet- en regelgeving) van geprioriteerde third parties. Third parties krijgen prioriteit op basis van risico. Relevante belanghebbenden kunnen het bestuur, het senior management, inkoop, operations, risicomanagement, compliance, juridische zaken, informatietechnologie, informatiebeveiliging, personeelszaken en anderen zijn.

RISICOMANAGEMENT

Vereisten:

Internal auditors moeten de volgende aspecten van het risicomanagement voor third parties van de organisatie beoordelen.

A. Processen voor risicomanagement van derde partijen en hun diensten zijn gestandaardiseerd en uitgebreid, omvatten gedefinieerde rollen en verantwoordelijkheden en richten zich voldoende op de belangrijkste risico's die relevant zijn voor de organisatie (zoals strategisch, reputatie, ethisch, operationeel, financieel,

compliance, cyberbeveiliging, informatietechnologie, juridisch, duurzaamheid en geopolitiek). De naleving van processen wordt gecontroleerd en bij afwijkingen worden corrigerende maatregelen genomen.

B. Risico's met betrekking tot third parties gedurende de gehele levenscyclus worden regelmatig geïdentificeerd en beoordeeld. De risicobeoordeling wordt gebruikt om third parties te rangschikken en te prioriteren, inclusief de partijen die verder stroomafwaarts liggen. Risicomaatregelen worden ook gerangschikt en geprioriteerd. De risicobeoordeling wordt regelmatig herzien en bijgewerkt.

C. De reacties op risico's zijn adequaat en nauwkeurig, in overeenstemming met de rangorde. Risicomaatregelen worden geïmplementeerd, beoordeeld, goedgekeurd, gecontroleerd, geëvalueerd en waar nodig aangepast.

D. Er zijn processen om problemen met third parties te beheren en indien nodig te escaleren, zodat de verantwoordelijkheid voor de resultaten wordt gewaarborgd en de kans toeneemt dat de voorwaarden van contracten of andere overeenkomsten worden nagekomen. Als een third party niet reageert op geëscaleerde kwesties, beschikt het management over processen om de risico's van de lopende zakenrelatie te evalueren en verdere actie, herstel of beëindiging na te streven, indien gerechtvaardigd.

BEHEERSING

Vereisten:

Internal auditors moeten de volgende beheersmaatregelen beoordelen voor de derde partijen die zijn geprioriteerd op risico. De evaluatie moet de processen van het management bevatten voor de voortdurende beoordeling en monitoring van de derde partijen van de organisatie.

A. Er is een robuust due diligence proces voor het zoeken en selecteren van third parties met een gedocumenteerde en goedgekeurde business case of ander relevant document dat de noodzaak voor en de aard van de relatie met de third party beschrijft en rechtvaardigt.

B. Contractering en goedkeuring worden uitgevoerd volgens het beleid en de procedures van de organisatie voor risicomanagement van third parties en omvatten samenwerking tussen de juiste onderdelen van de organisatie.

C. Definitieve contracten of overeenkomsten worden beoordeeld en goedgekeurd door alle relevante belanghebbenden, inclusief de juridische afdeling en compliance, ondertekend door bevoegde personen van beide partijen en veilig opgeslagen. Voor elk contract wordt een contractmanager of -beheerder aangesteld.

D. Er wordt een nauwkeurige, volledige en actuele lijst bijgehouden van alle relaties met third parties, bijvoorbeeld in een gecentraliseerd contractbeheersysteem.

E. Gedocumenteerde inwerkprocessen worden opgesteld en gevolgd om een basis te leggen voor third parties om te voldoen aan de voorwaarden van het contract of de overeenkomst.

F. Er bestaan doorlopende beheersprocessenom te beoordelen of derde partijen gedurende de hele levenscyclus presteren in overeenstemming met de voorwaarden van het contract of de overeenkomst en of de derde partijen hun contractuele verplichtingen nakomen. De processen omvatten het verifiëren van de betrouwbaarheid van de

verstrekte informatie en het periodiek en bij elke wijziging van de overeenkomst opnieuw evalueren van de prestaties.

G. Er zijn protocollen opgesteld om corrigerende maatregelen te initiëren als een third party niet aan de verwachtingen voldoet of een verhoogd of onverwacht risico vormt. De protocollen omvatten het escaleren van incidenten op basis van ernst, het uitvoeren van beoordelingen na een incident en het analyseren van de hoofdoorzaak van incidenten.

H. Contractverval- en verlengingsdata worden in de gaten gehouden en indien nodig worden er verlengingsacties ondernomen.

I. Er wordt een geformaliseerd offboardingplan geïmplementeerd en gevolgd om ervoor te zorgen dat contractvereisten met betrekking tot timing en verwachtingen adequaat worden aangepakt. Processen omvatten het

- Beëindigen van de third party.
- Vervangen van de third party indien nodig.
- Opnieuw aanwijzen van het beheer en retourneren of vernietigen van de gevoelige gegevens van de organisatie die bij de third party zijn opgeslagen.
- Ontzeggen van de third party'stoegang tot systemen, hulpmiddelen en faciliteiten.

Over het Instituut van Internal Auditors

Het IIA is een internationale beroepsvereniging die wereldwijd meer dan 265.000 leden telt en wereldwijd meer dan 200.000 Certified Internal Auditor® (CIA®) certificeringen heeft uitgereikt. Het IIA is opgericht in 1941 en wordt over de hele wereld erkend als de leider van het internal auditberoep op het gebied van standaarden, certificeringen, onderwijs, onderzoek en technische begeleiding. Ga voor meer informatie naar theiia.org.

Copyright

September 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, VS
Telefoon: +1-407-937-1111
Fax: +1-407-937-1101

