Third-Party

Topical Requirement

Gebruikershandleiding

The Institute of Internal Auditors

Vertaald door

Instituut van Internal Auditors Nederland

Inhoud

Overzicht van Topical Requirements[1]

Topical Requirements vormen een essentieel onderdeel van het International Professional Practices Framework®, samen met de Global Internal Audit Standards™ en de Global Guidance. Het Institute of Internal Auditors vereist dat de Topical Requirements worden gebruikt in combinatie met de Global Internal Audit Standards, die de gezaghebbende basis vormen voor de beroepspraktijk. Verwijzingen naar de Standaarden zijn in deze gebruikershandleiding opgenomen als bron van meer gedetailleerde informatie.

Topical Requirements formaliseren hoe internal auditors omgaan met veelvoorkomende risicogebieden om kwaliteit en consistentie binnen de beroepsgroep te bevorderen. Topical Requirements leggen een basis en bieden relevante criteria voor het uitvoeren van assurancediensten met betrekking tot het onderwerp van een Topical Requirement (Standaard 13.4 Evaluatiecriteria). Conformiteit met de Topical Requirements is verplicht voor assurancediensten en wordt aanbevolen voor evaluatie tijdens adviesdiensten. Het is niet de bedoeling dat Topical Requirements alle mogelijke aspecten omvatten waarmee rekening moet worden gehouden bij het uitvoeren van assurance-opdrachten; ze zijn eerder bedoeld om een minimale set vereisten te bieden om een consistente, betrouwbare beoordeling van het onderwerp mogelijk te maken.

De Topical Requirements sluiten duidelijk aan bij het Three Lines Model van het IIA en de Global Internal Audit Standards. Governance-, risicomanagement- en beheersprocessen zijn de belangrijkste onderdelen van de Topical Requirements ,die aansluiten bij Standaard 9.1 Inzicht in governance-, risicomanagement- en beheersprocessen. In verwijzing naar het Three Lines Model, is governance gekoppeld aan het bestuur/het bestuursorgaan, risicomanagement aan de tweede lijn en beheersing of beheersprocessen aan de eerste lijn. Terwijl het management vertegenwoordigd is in zowel de eerste als de tweede lijn, wordt de internal auditfunctie weergegeven in de derde lijn als een onafhankelijke en objectieve leverancier van zekerheid, die rapporteert aan het bestuur/het bestuursorgaan (Principe 8 Onder toezicht van het bestuur).

Toepasbaarheid, risico en professionele oordeelsvorming

Topical Requirements moeten worden nageleefd wanneer internal auditfuncties assurance-opdrachten uitvoeren met betrekking tot onderwerpen waarvoor een Topical Requirement bestaat of wanneer aspecten van de Topical Requirement worden geïdentificeerd binnen andere assurance-opdrachten.

[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.

Zoals beschreven in de Standaarden, is het beoordelen van risico's een belangrijk onderdeel van de planning van de chief audit executive. Om te bepalen welke assurance-opdrachten in het internal auditplan moeten worden opgenomen, moeten de strategieën, doelstellingen en risico's van de organisatie ten minste jaarlijks worden beoordeeld (Standaard 9.4 Internal Auditplan). Bij het plannen van individuele assurance-opdrachten moeten internal auditors de risico's beoordelen die relevant zijn voor de opdracht (Standaard 13.2 Risicobeoordeling in de opdracht).

Wanneer het onderwerp van een Topical Requirement wordt geïdentificeerd tijdens het risicogebaseerde planningsproces van de internal audit en wordt opgenomen in het auditplan, dan moeten de in de Topical Requirement beschreven vereisten worden gebruikt om het topic binnen de van toepassing zijnde opdrachten te beoordelen. Bovendien, wanneer internal auditors een opdracht uitvoeren (al dan niet opgenomen in het plan) en elementen van een Topical Requirement naar voren komen, moet de Topical Requirement worden beoordeeld op toepasbaarheid als onderdeel van de opdracht. Tot slot, als een opdracht wordt aangevraagd die oorspronkelijk niet in het plan was opgenomen en het onderwerp bevat, moet de Topical Requirement worden beoordeeld op toepasbaarheid.

Professionele oordeelsvorming speelt een belangrijke rol bij de toepassing van de Topical Requirement. Risicobeoordelingen vormen de basis voor beslissingen van chief audit executives over welke opdrachten in het internal auditplan moeten worden opgenomen (Standaard 9.4). Daarnaast gebruiken internal auditors professionele oordeelsvorming om te bepalen welke aspecten binnen elke opdracht aan bod zullen komen (Standaard 13.3 Doelstellingen en scope van de opdracht, 13.4 Evaluatiecriteria en 13.6 Werkprogramma).

Er moet bewijs worden bewaard dat elke vereiste in de Topical Requirement is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor de uitsluiting van eisen. Conformiteit met de Topical Requirement moet worden gedocumenteerd op basis van de professionele oordeelsvorming van auditors zoals beschreven in Standaard 14.6 Documentatie van de opdracht.

Hoewel de Topical Requirement een basislijn geeft van beheersprocessen die moeten worden overwogen, moeten organisaties die het risicothema als zeer hoog beoordelen mogelijk aanvullende aspecten beoordelen.

Indien de internal auditfunctie niet over de vereiste competenties beschikt om opdrachten uit te voeren met betrekking tot een onderwerp uit de Topical Requirement, moet de chief audit executive bepalen hoe de middelen kunnen worden verkregen en tijdig aan het bestuur en het senior management de impact van de beperkingen communiceren en hoe eventuele tekorten aan middelen zullen worden aangepakt. De chief audit executive behoudt de eindverantwoordelijkheid om ervoor te zorgen dat de internal auditfunctie voldoet aan de Topical Requirement, ongeacht hoe de middelen worden verkregen (Normen 3.1 Competentie, 7.2 Kwalificaties van hoofd van de internal auditfunctie, 8.2 Middelen, 10.2 Personeelsbeheer).

Prestaties, documentatie en rapportage

Bij het toepassen van Topical Requirements moeten internal auditors ook voldoen aan de Standaarden en hun werk uitvoeren in overeenstemming met Domein V: Uitvoeren van internal auditdiensten. De standaarden in domein V beschrijven het plannen van opdrachten (Principe 13 Plan Opdrachten Effectief), het uitvoeren van opdrachten (Principe 14 Voer

opdrachtwerkzaamheden uit) en het communiceren van de resultaten van opdrachten (Principe 15 Communiceer opdrachtresultaten en monitor actieplannen).

De Topical Requirements zijn bedoeld om consistente internal auditpraktijken van hoge kwaliteit te ondersteunen. Lokale wetten, voorschriften, verwachtingen van toezichthouders en andere professioneel erkende kaders kunnen aanvullende of meer specifieke vereisten opleggen. Internal auditors moeten de wet- en/of regelgeving begrijpen en naleven die relevant is voor de bedrijfstak en jurisdicties waarin de organisatie actief is, inclusief de vereiste openbaarmakingen, volgens Standaard 1.3 Juridisch en ethisch gedrag. Internal auditors hebben deze aanvullende vereisten mogelijk al geïntegreerd in auditprogramma's en testprocedures en moeten deze afstemmen op het actuele vereiste om ervoor te zorgen dat deze voldoende worden gedekt.

De dekking van het Topical Requiremkan worden gedocumenteerd in het internal auditplan of in de werkdocumenten op basis van het professionele oordeel van de auditors. Een of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kan het zijn dat niet alle vereisten van toepassing zijn. Er moet bewijsmateriaal worden bewaard waaruit blijkt dat de onderhavige vereiste is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor eventuele uitsluitingen.

Kwaliteit

De Standaarden vereisen dat het hoofd van de internal auditfunctie een programma voor kwaliteitsborging en -verbetering ontwikkelt, implementeert en onderhoudt dat alle aspecten van de internal auditfunctie omvat (Standaard 8.3 Kwaliteit). De resultaten moeten worden gecommuniceerd naar het bestuur en het senior management. In de communicatie moet worden gerapporteerd over de conformiteit van de internal auditfunctie met de Standaarden en het behalen van de prestatiedoelstellingen.

Conformiteit met de Topical Requirements wordt geëvalueerd in kwaliteitsbeoordelingen.

Third Party

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 om de organisatie te voorzien van producten, diensten, arbeid, productie of IT-oplossingen, zoals gegevensopslag, -verwerking en -onderhoud.

> **Opmerking**
>
> In de Topical Requirements wordt gebruik gemaakt van algemene terminologie voor internal auditing zoals gedefinieerd in de Global Internal Audit Standards. Lezers dienen de termen en definities in de verklarende woordenlijst van de standaarden te raadplegen.

De term "third party" kan op verschillende manieren worden gebruikt, afhankelijk van de sector of andere context. Elke internal auditfunctie heeft de flexibiliteit om haar eigen oordeel te gebruiken bij de toepassing van de Topical Requirement, afhankelijk van hoe de primaire organisatie (de organisatie die een overeenkomst met een third party aangaat) third parties definieert. In Third-Party Topical Requirement en de gebruikershandleiding verwijst de term "third party" naar verkopers, leveranciers, aannemers, onderaannemers, uitbestede dienstverleners, andere

instanties en adviseurs. De term "third party" omvat alle dergelijke overeenkomsten, inclusief die tussen een third party en zijn onderaannemers, vaak "downstream" onderaannemers genoemd, of "vierde partijen," "vijfde partijen," of "n-de partijen"

Deze Topical Requirement is niet bedoeld voor indirecte externe relaties, belangen of betrokkenheid bij de primaire organisatie, zoals regelgevers, agenten, makelaars, investeerders, trustees/leden van de raad van bestuur, openbare diensten en leden van het algemene publiek, of interne relaties, zoals werknemers of dienstverleners binnen de groep.

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

De effectiviteit van de processen van een organisatie voor het beheren van relaties met third parties kan worden beoordeeld voor de hele organisatie en/of op het niveau van een of meer individuele contracten, overeenkomsten of relaties. Internal auditors moeten een top-down benadering hanteren om inzicht te krijgen in het beleid, de procedures, de processen, het raamwerk en de levenscyclus van de organisatie met betrekking tot derden. Internal auditors moeten hun beoordelingsvermogen gebruiken om de nuances in third party-risico's te begrijpen op basis van individuele bedrijfstakken, organisaties en opdrachtonderwerpen. In overeenstemming met norm 5.1 Gebruik van informatie moeten internal auditors zich bewust zijn van en voldoen aan alle beleidsregels en procedures met betrekking tot de informatie van third parties waartoe ze toegang hebben.

De Topical Requirement is van toepassing wanneer de internal 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.

De Third-Party Topical Requirement en de gebruikershandleiding verwijzen naar fasen in de relatie van een organisatie met haar third parties, ook wel levenscyclusfasen genoemd: selecteren, contracteren, onboarding, monitoring en offboarding. Deze fasen zullen worden gebruikt voor de doeleinden van de Third-Party Topical Requirement en de gebruikershandleiding, ook al hebben sommige bedrijfstakken hun eigen versies van de levenscyclus. De fasen zijn:

- Selecteren: omvat processen om de behoefte aan een third party te bepalen, het plan voor het gebruik ervan en de due diligence voor selectie. Daarnaast moeten bij de selectie de risico's van potentiële en ingeschakelde derden worden beoordeeld.
- Contracteren: omvat due diligence processen voor het opstellen, onderhandelen, goedkeuren en implementeren van een juridische overeenkomst met de third party.

- Onboarding: begint wanneer het contract wordt getekend om de relatie te starten en legt een basis voor third parties om te voldoen aan de voorwaarden van het contract of de overeenkomst.
- Monitoring: omvat processen voor "in-life" management en doorlopende monitoring van de third party nadat het contract is opgesteld en goedgekeurd. De aanpak is meestal systematisch en gebaseerd op risico's en moet rekening houden met voortdurende verbetering. Het monitoren omvat het verlengen van lopende contracten of overeenkomsten met third parties indien nodig.
- Offboarding: omvat processen voor het beëindigen van contracten en overeenkomsten, het onderhouden van een exit-strategie voor third partyen die zijn geprioriteerd op basis van risico, en het beëindigen van relaties indien nodig. De processen maken meestal gebruik van een risicogebaseerde aanpak en kunnen een formeel exitplan omvatten.

De primaire organisatie 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. Het inschakelen van third parties kan de kosten van de organisatie voor het uitvoeren van processen verlagen. Het kan echter operationele risico's met zich meebrengen omdat de primaire organisatie minder zicht heeft op en zeggenschap heeft over de beheersprocessen van de third party. Als een third party niet presteert zoals gecontracteerd, deelneemt aan onethische praktijken of een bedrijfsstoring ondervindt, kan dit gevolgen hebben voor de primaire organisatie.

De primaire organisatie moet risico's identificeren, beoordelen en beheren door middel van passende bestuurs-, risicomanagement- en beheersprocessen. Categorieën en voorbeelden van risico's met betrekking tot third parties zijn onder andere:

- Strategisch, zoals het vermogen om de missie en/of doelstellingen van de organisatie op hoog niveau te realiseren of om de gevolgen van fusies en overnames te beheersen.
- 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.

Internal auditors moeten elke fase van de levenscyclus van een third party in overweging nemen bij het beoordelen van de vereisten voor governance, risicomanagement en beheersprocessen.

De eisen in de Third Party Topical Requirement zijn onderverdeeld in drie secties volgens norm 9.1 Inzicht in bestuur, risicomanagement en beheersprocessen:

- Governance - duidelijk gedefinieerde basisdoelstellingen en strategieën voor het gebruik van third partyen om de doelen, het beleid en de procedures van de organisatie te ondersteunen.
- Risicomanagement - processen om de risico's van het gebruik van third parties te identificeren, analyseren, beheren en monitoren, inclusief een proces om incidenten direct te escaleren.
- Beheersing - door het management vastgestelde, periodiek geëvalueerde beheersprocessen om de risico's bij het gebruik van third parties te beperken.

Naast de Topical Requirement en deze gebruikershandleiding kunnen internal auditors ook aanvullende professionele richtlijnen over third parties raadplegen, zoals de IPPF Global Guidance en sectorspecifieke bronnen.

Overwegingen

De volgende overwegingen kunnen internal auditors helpen bij het implementeren van de vereisten in de Third-Party Topical Requirement. De met letters aangegeven verklaringen in elke sectie hieronder herhalen of parafraseren de corresponderende vereisten van de Topical Requirement. Deze niet-verplichte overwegingen zijn illustratief om voorbeelden te geven van manieren om de vereisten te beoordelen. Internal auditors moeten hun professionele oordeel gebruiken om te bepalen wat ze in hun beoordelingen moeten opnemen.

Overwegingen voor governance

Om te beoordelen hoe de bestuursprocessen, inclusief het toezicht door het bestuur, worden toegepast op de doelstellingen van third parties, kunnen internal auditors een review uitvoeren van:

A. Een geformaliseerde en gedocumenteerde risicogebaseerde aanpak of strategie om te bepalen of een third party moet worden ingeschakeld. De aanpak wordt periodiek herzien en omvat:
   - Een duidelijk gedefinieerd en gestandaardiseerd proces om de aanpak te implementeren, goedgekeurd voor gebruik door de organisatie.
   - Gebudgetteerde middelen op basis van een kosten-batenanalyse om het inschakelen van een third party te rechtvaardigen, om strategische afstemming en efficiënt gebruik van middelen te garanderen.
   - De evaluatie door het management van risico's en controles, inclusief die welke betrekking hebben op problemen met third parties.
   - Voldoende middelen om de prestaties van third parties te contracteren, beheren en controleren.
   - De integratie van feedback van belanghebbenden in de aanpak of strategie.

B. Beleid, procedures en andere relevante documentatie die worden gebruikt om relaties met third parties gedurende de gehele levenscyclus te definiëren, beoordelen en beheren. De beleidsregels en procedures kunnen het volgende omvatten:
   - Gestandaardiseerde tools en sjablonen om belangrijke governance-, risicomanagement- en beheersprocessen te vergemakkelijken.
   - Processen om beleid en procedures periodiek te evalueren, vast te stellen of ze adequaat zijn en ze waar nodig bij te werken.
   - Vastgestelde criteria voor het selecteren, contracteren, in dienst nemen, monitoren en uit dienst nemen van third parties.
   - Het identificeren en periodiek herzien van toepasselijke regelgevende vereisten voor afstemming met beleid en procedures.

- Benchmarking om toonaangevende third party-management-praktijken te identificeren en te vergelijken.

C. Gedefinieerde rollen en verantwoordelijkheden die het bereiken van de doelstellingen ten aanzien van third parties ondersteunen. Verdere bewijzen kunnen zijn:

- Processen om te evalueren of de waarden, ethiek en maatschappelijke verantwoordelijkheid van de third party overeenkomen met de principes van de primaire organisatie. In het proces moet worden opgenomen hoe potentiële belangenconflicten of onethische praktijken direct kunnen worden aangepakt.
- Regelmatige training van personeel dat third party-managementfuncties vervult en periodieke beoordeling van hun competenties.
- Een proces om te evalueren of training is geïmplementeerd om organisatiebreed bewustzijn over third parties te creëren.
- De rollen en verantwoordelijkheden zijn afgestemd op het Three Lines Model.

D. Tijdige communicatie en betrokkenheid met relevante belanghebbenden gedurende de gehele levenscyclus van third parties (bijvoorbeeld het bestuur, senior management, inkoop, operations, risicomanagement, compliance, juridische zaken, informatietechnologie, informatiebeveiliging, personeelszaken en anderen), waaronder:

- Informatie over risico's voor third parties en bekende potentiële kwetsbaarheden in notulen van vergaderingen, rapporten of e-mails.
- Een uitwisseling van informatie over het beheer van derden en de bevordering van samenwerking (bijvoorbeeld door periodieke cross-functionele bijeenkomsten).

Overwegingen voor risicomanagement

Om te beoordelen hoe risicomanagementprocessen worden toegepast op doelstellingen ten aanzien van third parties, kunnen internal auditors een review uitvoeren van:

A. Gestandaardiseerde en allesomvattende risicomanagementprocessen voor de gebruiker van diensten van third parties omvatten gedefinieerde rollen en verantwoordelijkheden en richten zich voldoende op de belangrijkste risico's die relevant zijn voor de organisatie:

- Processen voor het beoordelen en beheren van risico's van derden omvatten hoe de belangrijkste risico's worden beoordeeld:
  - In eerste instantie geïdentificeerd en gerapporteerd
  - Geanalyseerd om hun impact op het bereiken van de doelstellingen van de organisatie te evalueren
  - Beperkt, inclusief actieplannen om het risico tot een aanvaardbaar niveau terug te brengen.
  - Bewaakt, inclusief detectie en reactie op vroegtijdige waarschuwingen en een plan voor doorlopende rapportage totdat bedreigingen volledig zijn opgelost.

- Er wordt gecontroleerd of de processen worden nageleefd en er worden corrigerende maatregelen genomen voor eventuele afwijkingen, om te voorkomen dat de langete rmijn doelen of -strategie van de organisatie worden ondermijnd.
- Een risicomanagementcommissie of andere groep houdt direct toezicht op third parties en levert input aan het bestuur. De commissie heeft een welomschreven doel en komt regelmatig bijeen. Bewijs kan bestaan uit notulen van vergaderingen.

B. Risico's met betrekking tot third parties gedurende de levenscyclus worden regelmatig geïdentificeerd en beoordeeld. De risicobeoordeling rangschikt en prioriteert third parties. Reacties op risico's worden gerangschikt en geprioriteerd.

- Bij het ontwikkelen van een risicobeoordeling van third parties houdt de primaire organisatie rekening met factoren zoals de omvang, volwassenheid en het aantal ingeschakelde third parties.
- De risicobeoordeling is gedocumenteerd en identificeert inherente en restrisico's.
- De organisatie volgt een due diligence proces voor het herzien en bijwerken van de risicobeoordeling.
- Er worden criteria opgesteld om third parties te rangschikken en te prioriteren op basis van risico's. Voorbeelden van dergelijke criteria zijn:
  - De geleverde diensten zijn essentieel voor de activiteiten van de organisatie.
  - De financiële waarde van de overeenkomst is materieel.
  - De relatie is nieuw, snel aangegaan en/of duurt lang.
  - Er zijn verschillende externe partijen bij betrokken.
  - De third party is van plan om al het werk of een deel ervan uit te besteden.
- De organisatie houdt zich aan algemeen aanvaarde risicobeoordelingspraktijken, inclusief het feit dat de risicobeoordeling in een zo vroeg mogelijk stadium wordt uitgevoerd, meestal wanneer het voorstel wordt geanalyseerd tijdens de selectiefase, en vóór het in dienst nemen.
- Leveranciers vullen een vragenlijst in om hun risicorangschikking en prioriteit op basis van inherente risico's te bepalen. De organisatie zorgt ervoor dat de vragenlijsten worden ingevuld door relevant personeel en worden gecontroleerd op nauwkeurigheid.
- De organisatie krijgt periodiek input over risicomanagement van third parties van functionele gebieden, zoals informatietechnologie, inkoop, risicomanagement van de onderneming, personeelszaken, juridische zaken, naleving, bedrijfsvoering, boekhouding en financiën.

C. Reacties op risico's, zoals beperken, accepteren, elimineren en delen, worden geïdentificeerd en in verhouding gebracht met de risicorangschikking.

- Reacties op risico's worden gedocumenteerd en omvatten het in overweging nemen van de controleomgeving van de third party.

- Documentatie dat reacties op risico's die de risicotolerantie van de primaire organisatie overschrijden, worden beoordeeld op geschiktheid, vooral wanneer de risico's worden geaccepteerd. In de antwoorden komen mogelijke belangenconflicten met derden aan de orde.

D. De processen voor het beheren en escaleren van risico's van third parties, inclusief hoe het niveau van bedreiging of risico wordt geëvalueerd, toegewezen en geprioriteerd. De beoordeling kan het identificeren omvatten van de:

- Definities en uitleg van de risiconiveaus van de organisatie - zoals hoog, gemiddeld en laag - en escalatieprocedures voor elke risicocategorie.
- Lijst van third partyen gerangschikt volgens geïdentificeerde risico's en de risicobeperkingsstatus van eventuele risicogebeurtenissen
- Van toepassing zijnde wettelijke, regelgevende en nalevingsvereisten
- Gevolgen van risico's, zowel financieel als niet-financieel (bijvoorbeeld reputatie)
- Processen voor het communiceren van risico's van third parties aan management en werknemers, inclusief regelmatige rapportage van het risicoprofiel aan het bestuur (of een ander geschikt orgaan). Mededelingen moeten updates bevatten over het oplossen van problemen die zijn geconstateerd bij prioritaire third partyen.
- Processen voor het opnieuw beoordelen van de rangschikking en prioritering wanneer de risicobereidheid en risicotolerantieniveaus van de primaire organisatie veranderen.

Overwegingen voor beheersprocessen

Om te beoordelen hoe beheersprocessen worden toegepast op relaties met third parties, kunnen internal auditors een review uitvoeren van:

A. Er is een robuust due diligence proces voor het zoeken en selecteren van third partyen met een gedocumenteerde en goedgekeurde business case of andere relevante documentatie die de noodzaak voor en de aard van de relatie met de third party beschrijft en rechtvaardigt.

- De business case kan ook:
  - Ingaan op risico's voor het vermogen van de third party om aan de verwachtingen te voldoen en de mogelijke gevolgen voor de organisatie.
  - Een gedetailleerde kosten-batenanalyse omvatten.
- Gevestigde inkoopprocessen - zoals concurrerende biedingen, verzoeken om voorstellen en exclusieve inkoop - worden gevolgd. De processen omvatten:
  - Criteria voor belangrijke aspecten, zoals het beoordelen van cyberbeveiligingsprotocollen, het verifiëren van bankgegevens, het uitvoeren van financiële achtergrondcontroles en het onderzoeken van de organisatiestructuur, strafrechtelijke en juridische antecedenten, rij-records, politieke activiteiten en banden met criminele activiteiten van de third party.

- Goed gedefinieerde selectiecriteria voor het beoordelen van prestaties uit het verleden, referenties, reputatie en contractkosten.
- Due diligence om te zorgen voor de juiste selectie van leveranciers, zoals het vormen van cross-functionele teams om voorstellen te beoordelen. Om het risico op vooringenomenheid te verkleinen, omvatten de controles voor beoordelingsteams procedures voor het samenstellen van teams en eisen voor het bekendmaken van potentiële belangenconflicten.
- Zorgvuldigheid bij het beoordelen van de controleomgeving van de third party; bijvoorbeeld het uitvoeren van een bezoek ter plaatse of het beoordelen van de controleomgeving van de third party:
  - System and Organization Control (SOC) rapporten.
  - Financiële stabiliteit.
  - Oprichtingsakte of certificaat van goede reputatie.
  - Transparantie in de besluitvorming van het belangrijkste management en belanghebbenden.
  - Organisatiestructuur.
  - Operationele stabiliteit.
  - Cybersecurity protocollen.
  - Naleving van relevante wetten, regels en normen.
  - Ethiek.
  - Geschiedenis met de primaire organisatie.
  - Reputatie.
- Bewijs dat potentiële verkopers of aannemers pas overgaan naar de contractfase van de levenscyclus nadat relevante due diligence-processen zijn uitgevoerd en de resultaten zijn geanalyseerd.

B. Beleid en procedures voor contracten worden opgesteld en gevolgd.

- Contracten worden geschreven in ondubbelzinnige termen.
- Tijdens het opstellen van het contract wordt rekening gehouden met de belangrijkste risico's en worden relevante clausules opgenomen. Problemen die opgelost moeten worden, worden in deze fase met de third party gecommuniceerd.
- Essentiële onderdelen van contracten worden bepaald op basis van het contracteerbeleid en de contractprocedures van de organisatie en het prioriteitsniveau van de third party. Elementen kunnen zijn:
  - Geheimhoudingsovereenkomsten (privacy).
  - Beëindigingsclausules en gedefinieerde parameters voor gegevenstoegang.
  - Cybersecurity vereisten, waaronder de vereisten voor toegang tot en het delen van alle gegevens en het rapporteren van incidenten of inbreuken binnen een bepaalde periode.

- Vereisten voor meldingen van een inbreuk op de gegevens van de primaire organisatie.
- Een gestandaardiseerd proces voor het verifiëren van de identificatie van de third party, inclusief volledige wettelijke naam, adres, fysieke locatie(s) en website. Een standaardpraktijk is om een checklist te gebruiken tijdens het identificatieproces en de nauwkeurigheid van de informatie te controleren.
- Duidelijk gedefinieerde overeenkomsten op serviceniveau, waarin de verwachte resultaten en de rechten, plichten, boetes, beloningen en verantwoordelijkheden van elke partij worden gespecificeerd, inclusief de verantwoordelijkheid voor het betalen van arbeidskosten (inclusief downstream onderaannemers).
- Een right-to-audit clausule die ook geldt voor downstream onderaannemers, of een eis voor bewijs dat een gerenommeerde, onafhankelijke assurance provider de partijen heeft gecontroleerd. Zonder een clausule over het right-to-audit kan het vermogen van de internal auditfunctie om zekerheid te verkrijgen of te verschaffen beperkt zijn.

- De primaire organisatie heeft toegang tot de srapporten van onafhankelijke auditors over de beheersing, bijvoorbeeld over financiën, compliance en gegevensbeveiliging, zoals de International Standard on Assurance Engagements of SOC-rapporten.
  - Als wordt vertrouwd op het werk van de externe assurance providers van de third party, worden documenten beoordeeld om de betrouwbaarheid te garanderen.
  - SOC-rapporten worden gebruikt om inadequate risico- en veranderingsbeheerprocessen te identificeren.

- Beleid en procedures behandelen alle onderdelen die essentieel zijn voor specifieke organisaties of soorten contracten:
  - Milieu- en duurzaamheidsclausules.
  - Klokkenluidersprotocollen.
  - Vereisten voor prestatiebeoordeling.
  - Bedrijfscontinuïteitsplan voor third parties getest.
  - Gebruik van kunstmatige intelligentie in dienstverlening.
  - Duidelijke identificatie, openbaarmaking, voorwaarden en reikwijdte voor alle downstream uitbestede werkzaamheden.
  - Wijzigingsbeheerproces, waarin wordt beschreven hoe om te gaan met wijzigingen in de reikwijdte, voorwaarden of operationele vereisten (zoals wijzigingen in technologie of regelgevende updates) tijdens de looptijd van het contract.
  - Beperkingen op het aantal wijzigingsopdrachten of bedragen die kunnen worden gefactureerd.

- Beleid en procedures vereisen een formele acceptatie van eindproducten voordat betaling plaatsvindt of aanbetalingen worden vrijgegeven.

- Third parties zijn verplicht om hun ethisch beleid of gedragscode te delen en/of die van de primaire organisatie na te leven.
- Als de third party het contract levert, heeft de primaire organisatie een juridische beoordeling uitgevoerd en worden de belangrijkste risico's begrepen en ondersteund door een geschikte risicobeperkingsstrategie.

C. Afgeronde contracten of overeenkomsten worden beoordeeld en goedgekeurd door de juiste belanghebbenden, waaronder juridische en compliance afdelingen, veilig opgeslagen en toegewezen aan een contractmanager of beheerder voor verantwoordelijkheid.

- Een contract of ander officieel document dat een uitbestedingsrelatie en de verplichting van de third party aangeeft, en bewijs van alle vereiste juridische en nalevingscontroles.

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

- Een proces voor het toevoegen van nieuwe contracten of overeenkomsten met third parties aan de lijst of het systeem.
- Een proces voor het invoeren van potentiële third partyen in het leverancierssysteem en het verwijderen ervan als het contract niet wordt goedgekeurd.
- Een proces voor het verwijderen van contracten of overeenkomsten van third parties uit de lijst of het systeem.
- Een volgsysteem om problemen met specifieke aannemers of leveranciers te documenteren voor toekomstig gebruik.
- Een beoordelingsproces om te bepalen of de populatie van third parties nauwkeurig en volledig is.

E. Er worden gedocumenteerde inwerkprocessen opgesteld en gevolgd om third parties in staat te stellen te voldoen aan de voorwaarden van het contract of de overeenkomst. Bij beoordelingen kan worden nagegaan of:

- Gestandaardiseerde onboardingprocedures zorgen ervoor dat alle benodigde documentatie, training en nalevingscontroles zijn voltooid.
- De systemen en processen van de third party kunnen naadloos integreren met de technologie van de primaire organisatie.
- Gedeelde systemen zijn compatibel en veilig. Bewijs kan aanvullende controles van gebruikersentiteiten omvatten als onderdeel van SOC-rapportage.
- De primaire organisatie beoordeelt de bedrijfscontinuïteitsplannen van de third party, die ervoor zorgen dat de dienstverlening doorgaat tijdens noodgevallen. Er zijn rampenplannen opgenomen om mogelijke verstoringen aan te pakken.

F. Processen voor het doorlopend monitoren van de prestaties van verkopers ten opzichte van de doelstellingen van het contract of de overeenkomst, inclusief evaluaties van belangrijke prestatie-indicatoren.

- De monitoringprocessen vormen de basis voor de risicobeoordeling door third parties en vastgestelde zwakke punten in de controle worden beoordeeld, geëscaleerd en indien nodig aangepakt.
- Rapporten of observaties van processen, technologieën en tools die zijn ingesteld om monitoring in realtime te beheren.
- Processen om ervoor te zorgen dat betalingen worden gedaan in overeenstemming met contract- of overeenkomstvoorwaarden, zoals het voldoen aan projecttijdlijnen, mijlpalen en communicatievereisten. Betalingen worden alleen gedaan aan goedgekeurde contractanten die de onboarding-fase hebben voltooid en zijn ingevoerd in het betalingssysteem voor leveranciers. Als de te leveren prestaties in het contract worden gespecificeerd, worden de uiteindelijke betalingen pas gedaan nadat de te leveren prestaties zijn geverifieerd.
- Bewaking om de kosten in verband met overeenkomsten met third parties te beheersen om de waarde te garanderen en het rendement op investering te bepalen. De resultaten van kosten-batenanalyses worden gebruikt om opnieuw over contracten te onderhandelen.
- Processen voor het bepalen van boetes voor het niet naleven van eventuele service-level agreements in het contract of de overeenkomst. Boetes worden berekend en in rekening gebracht op het moment dat ze worden opgelegd.
- De op risico gebaseerde rangschikking van geprioriteerde third partyen wordt periodiek opnieuw geëvalueerd, wanneer er wijzigingen zijn in een overeenkomst en wanneer een contract bijna afloopt of automatisch wordt verlengd.
- Beoordelingen van geprioriteerde third parties, zoals beoordelingen ter plaatse of driemaandelijkse bedrijfsbeoordelingen, om controles en operationele integriteit te valideren.
- Bewijs van aanvullende voortdurende controle kan zijn:
    - Analyses van de financiële stabiliteit van de third party.
    - Beoordeling van klachten tegen third parties.
    - Beoordelingen door het management van rapporten van onafhankelijke auditors, zoals International Standard on Assurance Engagements, Statements on Standards for Attestation Engagements, financiële, audit-, compliance- en gegevensbeveiligingsrapporten van third parties; ISO-certificeringen.
    - Beoordelingen door het management van de bedrijfsweerbaarheidstesten die door de third party zijn uitgevoerd, inclusief eventuele significante problemen die zijn geïdentificeerd.
    - Voorwaarden voor en beperkingen op het gebruik van onderaannemers of downstreampartijen.
    - Evaluaties van ethische waarden, cultuur en gedrag van third parties.
    - Reacties op vragen van de media.

- Evaluaties van privacy- en cybersecurity protocollen om de opslag en overdracht van gegevens en informatie van de primaire organisatie te beschermen, inclusief het gebruik van geavanceerde technologieën zoals kunstmatige intelligentie.
- De identificatie door de organisatie van mogelijkheden voor continue verbetering van de prestaties en het voldoen aan de doelstellingen van het contract of de overeenkomst.
- Beoordeling van functiescheiding.

G. Protocollen om corrigerende maatregelen te initiëren voor geïdentificeerde incidenten wanneer een third party niet voldoet aan de vereisten van een contract of overeenkomst, of wanneer acties van third parties het risico voor de primaire organisatie vergroten.

- Protocollen voor het escaleren van incidenten op basis van de ernst van het incident en de prioriteit van de third party.
- Evaluatie na het incident, inclusief analyse van de hoofdoorzaak.

H. Processen om waarschuwingen te geven voor contracten en overeenkomsten die bijna aflopen of automatisch verlengd worden. Automatische verlengingsprocessen omvatten het beoordelen:

- De prestaties van de third party.
- Contract- of overeenkomstvoorwaarden en eventuele addenda.
- Risicofactoren.

I. Er wordt een geformaliseerd offboardingplan geïmplementeerd en gevolgd om ervoor te zorgen dat contractvereisten met betrekking tot timing en verwachtingen adequaat worden aangepakt, ook voor eventuele downstream onderaannemers.

- Checklists of interviews met de belangrijkste belanghebbenden om ervoor te zorgen dat de beveiligingsmaatregelen effectief zijn.
- Organisatorische informatie of gegevens in bewaring bij een third party zijn geretourneerd of vernietigd.
- De toegang van de third party tot de gegevens, systemen of faciliteiten van de organisatie is ingetrokken.
- De activa van de primaire organisatie, zoals apparaten, softwarelicenties, intellectueel eigendom en documentatie, zijn teruggegeven.
- Wanneer een third party wordt ontslagen vanwege een dringende reden, worden de verzachtende omstandigheden of risico's geïdentificeerd en doorgegeven aan het senior management en/of de raad van bestuur.
- Wanneer het contract van een geprioriteerde third party wordt beëindigd, wordt de partij vervangen op basis van dezelfde risicobeoordeling, tenzij het contract is voltooid of niet langer nodig is.

Bijlage A. Voorbeelden van praktische toepassingen

De volgende voorbeelden beschrijven scenario's waarin de Third-Party Topical Requirement van toepassing zou zijn:

Voorbeeld 1: Een internal auditopdracht in het internal auditplan omvat een dienst of output die momenteel wordt geleverd door een third party.

Wanneer de internal auditfunctie haar risicogebaseerde planningsproces voltooit en een of meer opdrachten in het internal auditplan opneemt van diensten of output die momenteel door third parties worden geleverd in het kader van een contract of overeenkomst, is de Topical Requirement verplicht.

Niet elke eis in de actuele eis is van toepassing op elke opdracht. Wanneer internal auditors professionele oordeelsvorming toepassen en bepalen dat een of meer vereisten van de Third-Party Topical Requirement niet van toepassing zijn en daarom moeten worden uitgesloten van een opdracht, moeten internal auditors de reden voor het uitsluiten van deze vereisten documenteren en bewaren. De reden voor het uitsluiten van bepaalde vereisten kan bijvoorbeeld zijn dat de internal auditfunctie heeft vastgesteld dat de organisatie weinig vertrouwt op third parties voor missiekritieke diensten, of dat het een gevestigde relatie is met een lage financiële impact.

Voorbeeld 2: Third party-risico's worden geïdentificeerd tijdens een assurance-opdracht over een ander onderwerp dan third parties of contractbeheer.

Internal auditors kunnen een significant third party-risico identificeren tijdens het beoordelen van een proces waarvan in eerste instantie niet was vastgesteld dat het betrekking had op third parties of contractbeheer. Bij het plannen van een opdracht om gegevensopslag te beoordelen, komen internal auditors er bijvoorbeeld achter dat cloud-diensten worden gehost door een third party. Tijdens gesprekken met het management van de diensten van third parties identificeren interne controleurs 'cybersecurity risico's met betrekking tot de third party.

Zodra de relevante risico's zijn geïdentificeerd, moeten internal auditors zowel de Third-Partyals Cybersecurity Topical Requirement doornemen en bepalen welke vereisten van toepassing zijn. Auditors kunnen het bestuur van third parties of het risicomanagementproces van third parties uitsluiten van de reikwijdte van de opdracht en zich richten op de controles van third parties op de diensten die worden gecontroleerd. Ditzelfde professionele oordeel is van toepassing op de toepassing van de Cybersecurity Topical Requirement. Auditors moeten in de werkdocumenten de reden voor het uitsluiten van vereisten van de Third-Party of Cybersecurity Topical Requirements documenteren en de documentatie bewaren.

Voorbeeld 3: Een opdracht van een third party die oorspronkelijk niet in het internal auditplan was opgenomen, is nodig.

Er doet zich binnen de organisatie een probleem voor met een geprioriteerde third party dat onmiddellijke aandacht vereist van de internal auditfunctie. Er was sprake van een fout in de beheersing De chief audit executive moet met het bestuur communiceren over het herprioriteren van het auditplan en de middelen van de internal auditfunctie om aan de behoefte te voldoen. De auditor moet samen met het getroffen management doelstellingen ontwikkelen om de situatie te evalueren en aanbevelingen te doen om herhaling te voorkomen. De chief audit executive moet de Topical Requirement doornemen om de reikwijdte van de opdracht te bepalen, vaststellen welke vereisten van toepassing zijn en eventuele uitsluitingen dienovereenkomstig documenteren.

Bijlage B. Optioneel hulpmiddel voor documentatie

Van internal auditors wordt verwacht dat zij hun professionele oordeel gebruiken bij het bepalen van de toepasbaarheid van de vereisten op basis van de risicobeoordeling en dat zij de uitsluiting van bepaalde vereisten op passende wijze documenteren. De Topical Requirement kan worden gedocumenteerd in het internal auditplan of in de werkdocumenten van de betreffende opdracht, op basis van de professionele oordeelsvorming van de auditor. Eén of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kan het zijn dat niet alle vereisten van toepassing zijn. Het afdrukbare formulier hieronder biedt één optie voor het documenteren van conformiteit met de Third-Party Topical Requirement, maar het gebruik ervan is niet verplicht.

Governance van third parties

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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 de 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.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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 zijn onder andere het bestuur, senior management, inkoop, operations, risicomanagement, compliance, juridische zaken, informatietechnologie, informatiebeveiliging en personeelszaken.		

Risicomanagement van third parties

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
A. Processen voor risicomanagement van third parties 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.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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 van third parties

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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 beheersprocessen om te beoordelen of third parties gedurende de hele levenscyclus presteren in overeenstemming met de voorwaarden van het contract of de overeenkomst en of de third parties 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.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
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 vanhet beheer en retourneren of vernietigen van de gevoelige gegevens van de organisatie die bij de third party zijn opgeslagen. • Ontzeggen van de third party's toegang 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.

Disclaimer

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