IPPF

International Professional Practices Framework

Aanvullende richtlijnen

Praktijkgids

Planning van de opdracht

Beoordeling van frauderisico's

Instituut van Internal Auditors Nederland

Planning van de opdracht
Beoordeling van frauderisico's

Colofon

Titel

Planning van de opdracht
Beoordeling van frauderisico's

Instituut van
Internal Auditors
Nederland

Inhoudsopgave

Samenvatting

Fraude kan de bedrijfsactiviteiten verstoren, zorgen voor compliance risico's, de naam van een organisatie in diskrediet brengen en aanzienlijke kosten voor een organisatie en haar stakeholders opleveren. Al heeft het management, onder toezicht van het bestuur, de primaire verantwoordelijkheid voor het vaststellen en bewaken van effectieve beheersingsmaatregelen om fraude tegen te gaan en op te sporen, het is de plicht van de internal auditfunctie om het risico op fraude te beoordelen volgens de *internationale standaarden voor de beroepsuitoefening van internal auditing*. Daarnaast moet de Chief Audit Executive (CAE) significante kwesties op het gebied van risico- en beheersing, met inbegrip van fraude, rapporteren aan de directie en de Raad van Commissarissen (Standaard 2060 – Rapportering aan senior management en het bestuur).

De *Standaarden* leggen de internal auditfunctie de plicht op de frauderisico's op organisatie en opdrachtniveau te beoordelen. Om voor elke opdracht een adequate beoordeling van de relevante risico's te maken, moeten interne auditors als onderdeel van de planning van de opdracht een frauderisicoanalyse verrichten (Standaard 2210.A1). Na verloop van tijd kan de kennis die de internal auditfunctie tijdens afzonderlijke opdrachten heeft opgedaan, worden verzameld ten behoeve van een grondige en uitgebreide frauderisicoanalyse van de gehele organisatie.

In deze praktijkgids worden de kenmerken van fraude beschreven, evenals het proces van het tijdens de planning van de opdracht vaststellen en beoordelen van frauderisico's. Hoe de frauderisicobeoordeling precies moet worden opgenomen in de planning van de opdracht, kan variëren al naargelang de behoeften van de individuele organisatie, de internal auditfunctie en de opdracht. Over het algemeen omvat het proces echter de volgende stappen:

- het verzamelen van informatie om inzicht te krijgen in het doel en de context van de opdracht, alsook in de governance, het risicomanagement en de beheersingsmaatregelen die van belang zijn voor het te beoordelen domein of proces;
- het brainstormen over fraudescenario's om potentiële frauderisico's te identificeren;
- het beoordelen van de geïdentificeerde frauderisico's om te bepalen welke risico's tijdens de opdracht verder moeten worden geëvalueerd.

Inleiding

De internal auditfunctie is verantwoordelijk voor de beoordeling van de risicomanagement-processen van de organisatie en de effectiviteit daarvan, met inbegrip van de evaluatie van de frauderisico's en hoe deze worden beheerd door de organisatie (2120.A2). Het is echter even belangrijk om bij de planning van elke opdracht de potentiële gevallen van fraude te beoordelen, aangezien nieuwe frauderisico's zich op ieder moment kunnen voordoen. Internal auditors moeten daarom bij het bepalen van de doelstellingen van elke opdracht de waarschijnlijkheid van fraude inschatten (Standaard 2210.A2).

Door aan het begin van elke opdracht een frauderisicoanalyse te verrichten, kunnen internal auditors frauderisico's ontdekken die mogelijk nog niet golden op het moment dat de organisatiebrede risicobeoordeling voor het laatst werd bijgewerkt. Bovendien kunnen bepaalde frauderisico's op organisatorisch niveau onbeduidend zijn, maar aan belang winnen binnen een afzonderlijk domein of proces.

Internal auditors moeten over voldoende kennis beschikken om frauderisico's en de manier waarop die risico's door de organisatie beheerst worden, te beoordelen. Er wordt van hen echter niet verwacht dat zij de expertise bezitten van een persoon wiens voornaamste verantwoordelijkheid het ontdekken en onderzoeken van fraude is (Standaard 1210. A2). Bij de beoordeling van frauderisico's wordt van internal auditors verwacht dat zij beroepsmatige zorgvuldigheid betrachten (Standaard 1220.A1) en dat zij een onpartijdige en onbevooroordeelde houding hebben (Standaard 1120 – Individuele objectiviteit). Ook geven internal auditors blijk van beroepsmatige scepsis, d.w.z. een onderzoekende houding, zonder vooroordelen of aannamen over de inherente eerlijkheid van het management of de medewerkers. Zo wordt een objectieve, kritische beoordeling van het te beoordelen domein of proces gewaarborgd.

Deze praktijkgids biedt een kort overzicht van de kenmerken van fraude, gevolgd door een omschrijving van hoe de frauderisico's, als onderdeel van de planning van de opdracht, moeten worden geëvalueerd. De gids beschrijft hoe informatie moet worden verzameld, hoe over fraudescenario's moet worden gebrainstormd, hoe frauderisico's moeten worden onderkend en hoe hun belang moet worden geclassificeerd teneinde te bepalen welke frauderisico's tijdens de opdracht nader moeten worden geëvalueerd.

Inzicht in fraude

Hoewel er tal van definities bestaan, definieert het Instituut van Internal Auditors (IIA) *fraude* als "elke onwettige handeling die wordt gekenmerkt door bedrog, verduistering of inbreuk op het vertrouwen." Deze definitie omvat een kenmerk dat fraude onderscheidt van overige risico's: intentie. Bij frauduleuze handelingen zijn mensen betrokken die de intentie hebben beheersingsmaatregelen te omzeilen of gebruik te maken van zwakke punten in de organisatie. De definitie van het IIA geeft tevens aan dat "fraude wordt gepleegd om geld, eigendommen of diensten te verkrijgen, om uitgaven of verlies van diensten te voorkomen of om persoonlijke of zakelijke voordelen veilig te stellen."

Omdat wetgeving varieert, kan de rechtmatigheid van een frauduleuze handeling aanvechtbaar zijn. Een multinational waarvan het hoofdkantoor is gevestigd in een bepaald land waar een handeling onwettig is, kan bijvoorbeeld zaken doen in andere landen waar dezelfde handeling geen inbreuk maakt op de lokale wetgeving. Maar ongeacht de wettelijke verschillen is het doel van een frauderisicoanalyse om het potentieel van schendingen van het vertrouwen, misbruik van zwakke punten en ontwijking van beheersingsmaatregelen aan het licht te brengen.

Wanneer mensen fraude plegen, zijn er altijd drie factoren aanwezig: druk of aansporing, waargenomen gelegenheid en rationalisatie.[1]

Druk of drijfveer - een werkelijke of vermeende behoefte die voor een reden of motief zorgt, zoals:

- de behoefte om organisatorische prestatiedoelen of financiële doelen te bereiken;
- persoonlijke problemen of externe druk (bijv. financiële problemen, gezondheidsproblemen of verslavingen);
- de wens om macht, invloed of achting te verwerven in de ogen van familie, vrienden, collega's of management (bijv. computerhackers die fraude begaan met als doel hun capaciteiten aan te tonen in plaats van echt schade aan te richten).

Gelegenheid - een combinatie van omstandigheden of voorwaarden die mogelijk maken dat fraude wordt gepleegd, zoals:

- slechte controle-opzet, gebrek aan beheersingsmaatregelen, ontoereikende beveiliging of functiescheiding, of overige omstandigheden die kunnen leiden tot falende controle;
- een mate van vertrouwen, bevoegdheid, kennis en/of toegang tot beheersprocessen waardoor medewerkers bestaande beheersingsmaatregelen kunnen omzeilen of doorbreken;
- ontoereikend toezicht, training of communicatie van beleidsmaatregelen ten aanzien van professioneel gedrag en de gevolgen van schendingen.

1 Cressey, D.R. "The Criminal Violation of Financial Trust," *American Sociological Review*, 15, nr. 6 (1950): 738-743.

Rationalisatie - een verzonnen, overtuigende en plausibele rechtvaardiging, zoals:

- het gevoel ergens recht op te hebben als gevolg van betrokkenheid bij de organisatie (bijv. grote hoeveelheid onbetaalde overuren of onbeloonde prestaties);
- het geloof dat handelingen acceptabel zijn omdat "anderen het ook wel zullen doen";
- het geloof dat handelingen acceptabel zijn omdat ze binnen de cultuur gangbaar zijn of bij eerdere werkgevers als acceptabel werden beschouwd;
- het geloof dat beleidsmaatregelen en procedures onzinnig en niet gerechtvaardigd zijn;
- de redenatie dat handelingen tijdelijk en/of eenmalig zijn (bijv. "even wat geld lenen; betaal ik later wel terug" of "alleen deze keer");
- het geloof dat de handeling niemand nadeel berokkent of zo onbeduidend is dat niemand iets merkt of zich erover bekommert.

Van deze drie factoren is gelegenheid de enige die door een organisatie direct kan worden beheerst. Management kan proberen de interne beheersingsmaatregelen zodanig te ontwerpen dat gelegenheden voor fraude worden voorkomen en dat frauduleuze handelen worden opgespoord wanneer deze zich voordoen.

Internal auditors moeten beseffen dat medewerkers die frauduleuze handelingen verrichten, fraude niet alleen rationaliseren ten behoeve van zichzelf, maar ook ten behoeve van hun organisatie of van een extern persoon of externe organisatie. Fraude die wordt gepleegd ten behoeve van de organisatie, wordt doorgaans verricht doordat er gebruikgemaakt wordt van een kans om een onrechtvaardig of oneerlijk voordeel te genieten door een externe partij te misleiden. Maar ook als medewerkers de fraude op een dergelijke manier rationaliseren, hebben ze er meestal toch ook indirect personeel voordeel van: bijvoorbeeld het realiseren van een prestatiedoel, een financiële beloning en/of een promotie. Bijlage C bevat een reeks voorbeelden van frauduleuze handelingen en hoe deze worden gerationaliseerd.

Verzamelen van informatie

Om in het te beoordelen domein of proces de frauderisico's vast te stellen, moeten internal auditors inzicht hebben in de organisatie en de bredere context waarin deze opereert (d.w.z. de juridische, politieke, sociale, economische, markttechnische, industriële en culturele omgeving). Daarnaast moeten internal auditors inzicht hebben in de strategische en operationele doelstellingen van de organisatie en hoe deze in lijn zijn met de doelen van het te beoordelen domein of proces (Standaard 2200 – Planning van de opdracht).

Om een dergelijk inzicht te verwerven moeten internal auditors informatie vergaren uit een reeks van bronnen, waaronder:

- eerdere beoordelingen en onderzoeken;
- formele rapportagemechanismen en interviews;
- een voorlopige beoordeling van de beheersomgeving;
- extern onderzoek en specialisten.

Bij het verzamelen van gegevens voor het maken van een frauderisicoanalyse in een opdracht, is het de rol van de internal auditfunctie om de frauderisico's die relevant zijn voor de opdracht te evalueren, en niet om een potentieel fraudegeval te onderzoeken. Internal auditors moeten derhalve discreet communiceren, vertrouwelijkheid bewaren en geen verdenkingen of beschuldigingen van fraude uiten. Onzorgvuldige communicatie kan een potentieel onderzoek verstoren en nodeloos leiden tot ongewilde reputatie en juridische risico's.

Eerdere beoordelingen en onderzoeken

De organisatiebrede risicobeoordeling, waarin de significante risico's op organisatieniveau zijn vastgesteld en die de basis vormt voor het jaarlijkse internal auditplan (Standaard 2010. A1), vormt een goed uitgangspunt om risico's te identificeren die relevant kunnen zijn voor het te beoordelen domein of proces. Beoordelingen die alleen gericht zijn op frauderisico's, ongeacht of deze organisatiebreed zijn of beperkt blijven tot het te beoordelen domein of proces, kunnen eveneens een goede informatiebron zijn. Internal auditors moeten relevante risicobeoordelingen en fraudeonderzoeken beoordelen, die door het management van het te beoordelen domein of door overige (interne of externe) aanbieders van assurance en consulting diensten zijn verricht. Om efficiënt te opereren, nemen internal auditors doorgaans alleen recente beoordelingen in overweging.

Hoewel eerdere beoordelingen en onderzoeken waardevolle inzichten kunnen opleveren, kan het belang van frauderisico's worden beïnvloed door tal van factoren en kan dit dus snel veranderen. Het verrichten van een voorlopige beoordeling van de risico's voor elke afzonderlijke opdracht is dus van cruciaal belang voor een effectieve planning van de opdracht.

Formele rapportagemechanismen en interviews

Het personeel van een organisatie kan nuttige informatie over frauderisico's bieden. Sterker nog, de Association of Certified Fraud Examiners (ACFE) geeft aan dat, ongeacht de omvang of het type organisatie, en ongeacht of er een formeel rapportagemechanisme bestaat, personeel verantwoordelijk is voor meer dan 50% van de fraudetips en dus ook de meest gangbare manier vormt om fraude op te sporen.[2] Opmerkelijk genoeg werd vastgesteld dat de internal auditfunctie de op één na meest voorkomende manier was om fraude op te sporen.

Veel organisaties hebben formele mechanismen ingevoerd (bijv. hulplijnen voor klokkenluiders, online formulieren of speciale e-mailadressen) om de melding te bevorderen van mogelijke frauduleuze handelingen en zwakke punten in de interne controle, die de organisatie aan frauderisico's zouden kunnen blootstellen. Veel gemelde zorgen zijn onder meer beschuldigingen van verspilling, misbruik van bevoegdheid, verduistering van activa, samenspanning en overig onethisch of verdacht gedrag. Indien er een formeel fraudemeldingsmechanisme bestaat, kunnen internal auditors de person(o)n(en) die verantwoordelijk zijn voor het beheer ervan, toegang vragen tot alle informatie die van belang is voor het te beoordelen domein of proces, zoals opgenomen telefoongesprekken en vastgelegde verklaringen.

Om inzicht te krijgen in frauduleuze activiteiten die zijn gemeld, ontdekt en/of onderzocht, ondervragen internal auditors doorgaans andere medewerkers uit de organisatie, die verantwoordelijk zijn voor het beheer van frauderisico's, beschuldigingen en gevallen van fraude. Daarbij gaat het onder meer om de Ethics Officer, de Risk and Compliance Officer of medewerkers van de juridische afdeling, HR, beveiliging of frauderisicobeheersing.

Daarnaast kan het ondervragen van personeel op alle niveaus in het te beoordelen domein of proces waardevolle informatie opleveren, die anders niet beschikbaar zou zijn. Medewerkers die de dagelijkse taken en functies van een bepaald domein of proces uitvoeren, komen vaak met de meest precieze en actuele beschrijving van hoe een proces of de bijbehorende beheersingsmaatregelen *in werkelijkheid* functioneren, afgezet tegen hoe ze *zouden moeten* functioneren. Inzicht in de werkelijke activiteiten kan allerlei manieren aan het licht brengen waarop beheersingsmaatregelen kunnen worden omzeild. Om te bepalen wie ze het beste kunnen ondervragen, kunnen internal auditors gebruikmaken van een organigram met de rollen en verantwoordelijkheden

Potentieel rode vlag-woordgebruik

Bepaalde woordkeuzen van ondervraagden kunnen wijzen op potentiële gebreken in de controle en/of frauderisico's:

- "Om even het gedoe te omzeilen..."
- "Alleen voor deze keer..."
- "Ik heb altijd al zo gedaan."
- "Voor een keertje kunnen we best..."
- "Onofficieel…"
- "Er zijn geen beleidsregels of procedures voor dit proces."
- "Iemand zei me dat ik het zo moest doen; ik weet eigenlijk niet zo goed waarom."
- "Dit is zoals we het *echt* doen."
- "Zoals het *eigenlijk zou moeten,* is…"

Bijlage D geeft een overzicht van rode vlag-woordkeuzes..

2 Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2016), 20-25, http://www.acfe.com/rttn2016.aspx (bekeken op 31 oktober 2017).

van medewerkers in het te beoordelen domein, of een proceskaart met een lijst met de voornaamste beheersingsmaatregelen (verstrekt door het management of opgesteld door de internal auditfunctie).

Voorlopige beoordeling van de beheersomgeving

Formele rapportagemechanismen en interviews leggen vaak problemen bloot ten aanzien van de beheersomgeving van de organisatie, die kunnen leiden tot fraude. Er kunnen echter nog meer waarschuwingssignalen worden waargenomen door bepaalde aspecten van de beheersomgeving te evalueren, zoals de structuur en de ethische waarden van de organisatie, en de filosofie en stijl van het management. Een beoordeling van de beheersomgeving moet in ieder geval een evaluatie van de volwassenheid van die beheersomgeving en de doelmatigheid van de desbetreffende beheersingsmaatregelen omvatten. De beoordeling kan potentiële drijfveren en/of vormen van druk blootleggen, die medewerkers ertoe kunnen aanzetten fraude te rationaliseren. Medewerkers kunnen bijvoorbeeld refereren aan een bepaalde prestatiedruk of hun zorgen uiten over onrealistische doelen waar medewerkers gebruik van kunnen maken om hun frauduleuze gedrag te rechtvaardigen. Om inzicht te krijgen in de potentiële druk moeten internal auditors de prestatiedoelen en -metingen (d.w.z. kernprestatie-indicatoren) en bijbehorende prikkels ten aanzien van het te controleren domein vaststellen.

Omdat ze een allesomvattend beeld hebben van de organisatie en haar beheersomgeving, kunnen internal auditors mogelijk na verloop van tijd veranderingen constateren in de cultuur van de organisatie. Culturele veranderingen kunnen de kans vergroten dat fraude plaatsvindt en onopgemerkt blijft. Op opdrachtniveau kunnen internal auditors dichter, dan de directie (en andere medewerkers die de organisatiebrede frauderisico's beheren), komen bij de gedetailleerde operationele activiteiten, systemen en de medewerkers van het te beoordelen domein of proces . Het is voor internal auditors daarom van cruciaal belang alert te zijn op woordkeuzen of handelingen van medewerkers die kunnen wijzen op zwakke punten in de beheersomgeving. In het geval er een vermoeden bestaat van zwakke punten in de beheersomgeving, dient de verantwoordelijke voor de opdracht hiervan melding te doen aan de Chief Audit Executive, aangezien de kwestie groter kan zijn dan de reikwijdte van de opdracht. Dit thema wordt nader gedetailleerd in de praktijkgids van het IIA getiteld "Auditing the Control Environment".

Potentiële rode vlaggen

Managementkwesties:
- gebrek aan materiedeskundigheid
- gebrek aan toezicht
- historie van wetsovertredingen

Personeelskwesties:
- gebrek aan antecedentenonderzoek
- ontevreden medewerkers
- gebrek aan bereidheid om taken te delen

Proceskwesties:
- taken niet gescheiden
- gebrekkige fysieke beveiliging
- gebrekkige toegangscontroles

Extern onderzoek en specialisten

Internal auditors hoeven niet over de expertise van een gespecialiseerde fraudeonderzoeker te beschikken. Zij moeten echter over voldoende kennis beschikken om frauderisico's en de manier waarop die risico's door de organisatie beheerst worden, te beoordelen (Standaard 1210. A2). Internal auditors kunnen dergelijke kennis opdoen door fraudegevallen te onderzoeken die zich hebben voorgedaan bij vergelijkbare organisaties of industrieën en fraudetrends te bestuderen. Daarnaast kunnen internal auditors gebruikmaken van benchmarks om de wijze van frauderisicobeheersing van de organisatie en het te beoordelen domein te vergelijken met die van vergelijkbare en/of meer volwassen organisaties. Kennis kan tevens worden verworven door het lezen van relevante publicaties, het bijhouden van wijzigingen in de regelgeving en het bijwonen van conferenties en trainingen. Professionele organisaties in het vakgebied bieden vaak dergelijke hulpmiddelen en informatie, evenals professionele standaarden.

De CAE dient ervoor te zorgen dat de internal auditfunctie gezamenlijk de bekwaamheden bezit of verwerft die benodigd zijn om haar taken uit te voeren (Standaard 1210 – Vakbekwaamheid) en moet deskundig advies en bijstand inhuren indien het de internal auditors ontbreekt aan de bekwaamheden die benodigd zijn om de gehele opdracht of een gedeelte daarvan uit te voeren (Standaard 1210.A1). De CAE biedt de medewerkers van internal audit mogelijkheden voor training en begeleiding, maar kan daarnaast ook specialisten aantrekken met kennis van de sector of de specifieke functionele domeinen of processen. Bij het brainstormen over fraudescenario's of het verrichten van een opdracht met frauderisico's kunnen internal auditors waar nodig ruggespraak houden met dergelijke specialisten.

Brainstormen over fraudescenario's

Op basis van de verzamelde informatie kunnen internal auditors fraudescenario's en frauderisico's overwegen die van toepassing kunnen zijn op het te beoordelen domein of proces. Door te brainstormen over fraudescenario's kunnen op effectieve wijze de voor het specifieke domein of proces unieke kenmerken en omstandigheden worden bepaald waardoor gelegenheden of prikkels voor fraude kunnen ontstaan.

De mate waarin brainstormsessies nodig zijn, de complexiteit van de sessies en wie daar allemaal bij aanschuiven, variëren per opdracht, afhankelijk van de behoeften van de internal auditfunctie, de organisatie en de opdracht, evenals de kennis van de internal auditors van het specifieke te beoordelen domein of proces. Om tot een grondige lijst van de fraudescenario's te komen moeten internal auditors van gedachten wisselen met personen met uiteenlopende kennis en gezichtspunten en die in verschillende relaties staan tot het te beoordelen domein of proces.

Potentiële deelnemers brainstormsessies

- Accounting en Finance
- Internal Audit
- Juridisch en Compliance
- Bedrijfsvoering
- Proceseigenaren
- Directie, management
- Overige aanbieders van assurancediensten

Bij het brainstormen over frauderisico's moeten de deelnemers de potentiële druk en gelegenheden om fraude te plegen binnen het te beoordelen domein of proces overwegen. De deelnemers moeten ook oog hebben voor fraudescenario's waarbij interne en externe IT-dreigingen betrokken zijn, bijv. de bevoegdheid om systeemconfiguraties te negeren, waardoor frauduleuze transacties en/of diefstal van gevoelige organisatorische informatie mogelijk worden.

Het brainstormen is bedoeld om een open deelname en een ongeremde uitwisseling van gedachten en ideeën te stimuleren. Daarom moeten internal auditors bij de beoordeling van de voorgestelde fraudescenario's oog hebben voor het feit dat sommige potentiële frauderisico's zeer onwaarschijnlijk kunnen zijn, niet altijd goed op de opdrachtdoelen zijn afgestemd of buiten de reikwijdte van de voor de huidige opdracht toegewezen middelen liggen.

De informatie die tijdens de brainstormsessies wordt verzameld, kan worden gebruikt om voor elk te beoordelen domein of proces een lijst van fraudescenario's en bijbehorende risico's op te stellen. **Figuur 1** bevat bijvoorbeeld de fraudescenario's en bijbehorende risico's die tijdens een brainstormsessie voor een assuranceopdracht inzake crediteuren zouden kunnen worden vastgesteld. Bijlage E bevat een frauderisicoanalyse voor een opdracht inzake het proces van kasuitgaven.

Fraudescenario	Frauderisico
A. Fictieve personeelskosten.	A.1 Zakelijke betaalkaarten worden met opzet ongepast gebruikt, waardoor er frauduleuze kosten ontstaan.
	A.2 Er worden kosten ingediend voor goederen of diensten die in werkelijkheid niet aan de organisatie zijn geleverd.
	A.3 Voor dezelfde kosten worden meerdere kostenvergoedingen ingediend.
B. Frauduleuze uitgaven.	B.1 In het systeem worden fictieve leveranciers aangemaakt, waaraan frauduleuze betalingen worden gedaan.
	B.2 Er worden onjuiste terugbetalingen en/of nietigverklaringen doorgevoerd.
C. Verborgen verplichtingen en onkosten.	C.1 Onkosten in verband met dubieuze debiteuren worden bewust weggelaten.
	C.2 Onkosten worden gekapitaliseerd.
D. Transacties met gerelateerde partijen.	D.1 Een partij ontvangt een bepaald voordeel dat deze bij een zakelijke transactie niet zou hebben ontvangen.
E. Verduistering.	E.1 Personeel betaalt personeelsuitgaven met middelen van de organisatie en vervalst de administratie om dit te verbergen.

Figuur 1: Brainstormen over fraudescenario's

Beoordeling van frauderisico's

De opdracht kan onmogelijk alle risico's afdekken. Daarom moeten internal auditors het belang bepalen van de frauderisico's die tijdens het brainstormen worden vastgesteld. Zo kan worden bepaald welke risico's tijdens de opdracht nader moeten worden geëvalueerd. Een effectieve manier om een frauderisicoanalyse uit te voeren en te documenteren is om een frauderisicomatrix met alle fraudescenario's en bijbehorende risico's op te stellen en in deze matrix vervolgens ook alle maatregelen op te nemen die van belang zijn.

Met behulp van een spreadsheet of een vergelijkbaar document kan, met of zonder een auditsoftwareprogramma, een frauderisicomatrix worden gecreëerd. De indeling van de matrix kan variëren, maar omvat gewoonlijk een rij voor elk risico en een kolom voor elke risicomaatstaf, zoals impact en waarschijnlijkheid.

Figuur 2 laat zien hoe de in figuur 1 gedocumenteerde fraudescenario's kunnen worden uitgebreid met risicoclassificaties voor de impact en de waarschijnlijkheid.

Fraudescenario	Frauderisico	Impact (L, M, H)	Waarschijnlijkheid (L, M, H)
A. Fictieve personeelskosten.	A.1 Zakelijke betaalkaarten worden met opzet ongepast gebruikt, waardoor er frauduleuze kosten ontstaan.	L	M
	A.2 Er worden kosten ingediend voor goederen of diensten die in werkelijkheid niet aan de organisatie zijn geleverd.	H	M
	A.3 Voor dezelfde kosten worden meerdere kostenvergoedingen ingediend.	M	H
B. Frauduleuze uitgaven.	B.1 In het systeem worden fictieve leveranciers aangemaakt, waaraan frauduleuze betalingen worden gedaan.	H	H
	B.2 Er worden onjuiste terugbetalingen en/of nietigverklaringen doorgevoerd.	L	H
C. Verborgen verplichtingen en onkosten.	C.1 Onkosten in verband met dubieuze debiteuren worden bewust weggelaten.	H	L
	C.2 Onkosten worden gekapitaliseerd.	H	L
D. Transacties met gerelateerde partijen.	D.1 Een partij ontvangt een bepaald voordeel dat deze bij een zakelijke transactie niet zou hebben ontvangen.	M	M
E. Verduistering.	E.1 Personeel betaalt personeelsuitgaven met middelen van de organisatie en vervalst de administratie om dit te verbergen.	M	M

Figuur 2: Frauderisicomatrix voor crediteuren

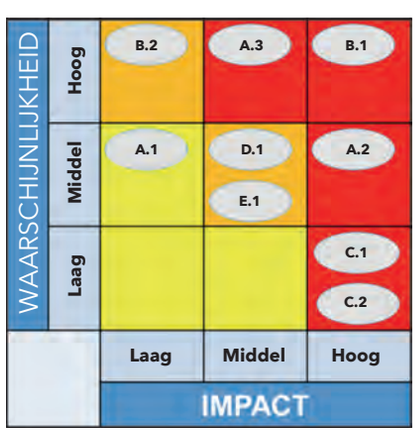
Het beoordelen van de impact is vaak gecompliceerd omdat zowel kwantitatieve als kwalitatieve factoren een rol spelen. Internal auditors dienen niet alleen rekening te houden met de financiële, operationele en wettelijke impact van de potentiële frauderisico's, maar ook met de niet-financiële impact, zoals schade aan de reputatie van de organisatie of relaties met klanten of leveranciers. Bijvoorbeeld, een frauderisico met een niet-wezenlijke directe financiële impact op de organisatie, kan toch een groot effect hebben op de reputatie en daarom worden geclassificeerd als een risico met een hoge impact.

Factoren die moeten worden overwogen bij de beoordeling van de waarschijnlijkheid, zijn onder meer eerdere beschuldigingen of gevallen van fraude, het voorkomen van vergelijkbare fraudegevallen in de sector en de complexiteit en hoeveelheid bij het proces betrokken personen.

De risicoclassificaties uit de frauderisicomatrix kunnen dan worden weergegeven in een basisgrafiek, zoals een heatmap. Door de impact van elk risico op de ene as en de waarschijnlijkheid ervan op de andere as uit te zetten, kunnen internal auditors een duidelijk beeld geven van het totale belang van het risico of de prioriteit. De gecombineerde betekenis van impact en waarschijnlijkheid wordt doorgaans aangegeven met behulp van een kleurensysteem: rood geeft de hoogste prioriteit aan, oranje geeft risico's aan die belangrijk genoeg zijn om in overweging te worden genomen, en geel geeft risico's aan die niet significant zijn.

Figuur 3 bevat een heatmap die is gecreëerd op basis van de informatie in de frauderisicomatrix van figuur 2. De heatmap moet worden opgenomen in de werkdocumenten van de opdracht, omdat deze de beslissingen van internal auditors over de significantie van risico's ondersteunt.

Een beperking van heatmaps is dat impact en waarschijnlijkheid even belangrijk lijken te zijn. Hoewel impact en waarschijnlijkheid in sommige gevallen even belangrijk kunnen zijn, heeft impact gewoonlijk een hoger prioriteit dan waarschijnlijkheid. Zo moet in de meeste gevallen aan een risico met een hoge impact en een lage waarschijnlijkheid (H, L) een hogere prioriteit worden gegeven dan aan een risico met een lage impact, ook al is de waarschijnlijkheid dat het risico zich voordoet groot (L, H).



Figuur 3: Heatmap

Een bijkomende beperking van heatmaps is dat slechts twee maatstaven tegelijk kunnen worden bekeken (in dit geval de impact en de waarschijnlijkheid). Het kan wenselijk of noodzakelijk zijn om bij het bepalen van de significantie van het risico ook rekening te houden met maatstaven als snelheid, kwetsbaarheid, volatiliteit, onderlinge afhankelijkheid en/of correlatie.

Op basis van de volledige heatmap kunnen internal auditors de significante frauderisico's weergeven, die in de opdracht moeten worden opgenomen voor nadere toetsing. **Figuur 4** laat de frauderisicomatrix zien, zoals gecorrigeerd overeenkomstig de geprioriteerde frauderisico's in de voorbeeldopdracht inzake crediteuren.

Frauderisico	Impact (L, M, H)	Waarschijnlijkheid (L, M, H)
B.1 In het systeem worden fictieve leveranciers aangemaakt, waaraan frauduleuze betalingen worden gedaan.	H	H
A.2 Er worden kosten ingediend voor goederen of diensten die in werkelijkheid niet aan de organisatie zijn geleverd.	H	M
A.3 Voor dezelfde kosten worden meerdere kostenvergoedingen ingediend.	M	H
C.1 Onkosten in verband met dubieuze debiteuren worden bewust weggelaten.	H	L
C.2 Onkosten worden gekapitaliseerd.	H	L
D.1 Een partij ontvangt een bepaald voordeel dat deze bij een zakelijke transactie niet zou hebben ontvangen.	M	M
E.1 Personeel betaalt personeelsuitgaven met middelen van de organisatie en vervalst de administratie om dit te verbergen.	M	M

Figuur 4: Significante frauderisico's

Internal auditors kunnen het management het overzicht voorleggen van de geïdentificeerde frauderisico's, om te overwegen of deze moeten worden opgenomen in de organisatiebrede risicoanalyse. De frauderisico's die voor deze opdracht niet nader hoeven worden geëvalueerd, kunnen worden opgenomen in een inventarisatie of controlelijst van frauderisico's van de internal auditfunctie. Deze kunnen dan bij toekomstige opdrachten worden overwogen.

Als de informatie die is blootgelegd tijdens de frauderisicoanalyse, wijst op een potentiële frauduleuze handeling, dienen internal auditors het vaste protocol voor de interne rapportage en onderzoek naar fraudebeschuldigingen te volgen. Doorgaans rapporteren internal auditors hun zorgen en de voorlopige bewijsstukken aan de CAE. Deze bepaalt vervolgens of de zaak moet worden geëscaleerd naar het senior management en/of het bestuur.

Vaststellen van beheersingsmaatregelen

Nadat internal auditors de fraudescenario's hebben overwogen en de frauderisico's hebben vastgesteld en geprioriteerd, moeten zij bepalen welke beheersingsmaatregelen, voor zover aanwezig, reeds zijn ingevoerd om deze risico's te beperken.

Frauderisico	Impact (L, M, H)	Waarschijnlijkheid (L, M, H)	Maatregel
B.1 In het systeem worden fictieve leveranciers aangemaakt, waaraan frauduleuze betalingen worden gedaan	H	H	Functiescheiding binnen leveranciersbeheer.
A.2 Er worden kosten ingediend voor goederen of diensten die in werkelijkheid niet aan de organisatie zijn geleverd.	H	M	Ontvangstbevestiging van goederen en diensten.
A.3 Voor dezelfde kosten worden meerdere kostenvergoedingen ingediend.	M	H	Automatische controles om dubbel ingediende onkosten op te sporen.
C.1 Onkosten in verband met dubieuze debiteuren worden bewust weggelaten.	H	L	Regelmatig toezicht op en goedkeuring van berekeningen van onkosten in verband met dubieuze debiteuren.
C.2 Onkosten worden gekapitaliseerd.	H	L	Controle en goedkeuring door management van alle kapitalisatieboekingen.
D.1 Een partij ontvangt een bepaald voordeel dat deze bij een zakelijke transactie niet zou hebben ontvangen.	M	M	Due diligence voor transacties met gerelateerde partijen.
E.1 Personeel betaalt personeelsuitgaven met middelen van de organisatie en vervalst de administratie om dit te verbergen.	M	M	Functiescheiding binnen crediteuren en goedkeuring management vereist voor personeelsuitgaven.

Figuur 5: Frauderisico- en controlematrix voor crediteuren

Figuur 5 laat zien hoe de matrix van figuur 4 kan worden uitgebreid met de bestaande beheersingsmaatregelen.

De frauderisico- en controlematrix dient, net als de heatmap, te worden opgenomen in de werkdocumenten van de opdracht. De informatie uit de matrix wordt vervolgens verwerkt in de voorlopige risicobeoordeling die wordt gebruikt om de doelstellingen en reikwijdte van de opdracht vast te stellen. De IIA-praktijkgids "Engagement Planning: Establishing Objectives and Scope" biedt gedetailleerde informatie over het voortbouwen op de risicobeoordeling om de doelstellingen en reikwijdte van de opdracht te ontwikkelen. Daarnaast ondersteunen de heatmap en de risico- en controlematrix voor frauderisico's de resultaten en conclusies van de opdracht, in overeenstemming met Standaard 2330 – Documenteren van de informatie.

Bijlage A. Standaarden en richtlijnen van het IIA

Relevante standaarden van het IIA

De volgende selecties uit de *Internationale standaarden voor de beroepsuitoefening van internal auditing* van het IIA zijn relevant voor controles van planning van de opdracht: beoordeling van frauderisico's. Zie de *Standaarden* voor de volledige verklaring. Om u te helpen bij de implementatie van de *Standaarden*, beveelt het IIA aan dat internal auditors de respectieve Implementatierichtlijnen van elke standaard raadplegen.

1210 – Vakbekwaamheid
1210.A1
1210.A2
1220 – Beroepsmatige zorgvuldigheid
1220.A1
2120 – Risicomanagement
2120.A2
2200 – Planning van de opdracht
2210 – Doelstellingen van de opdracht
2210.A1
2210.A2

Gerelateerde richtlijnen van het IIA

Practice Guide "Auduiting the Control Environment"
Practice Guide "Engagement Planning: Establishing Objectives and Scope"
Practice Guide "Internal auditing and Fraud."

Bijlage B. Woordenlijst

De met een sterretje (*) aangeduide termen zijn ontleend aan de "Woordenlijst" van de *International Professional Practices Framework* van het IIA, uitgave van 2017.

Controlemaatregel*- Elke actie van het management, het bestuur en andere partijen om risico's te beheersen en de waarschijnlijkheid te verhogen dat de beoogde doelstellingen en doelen gerealiseerd worden. De directie plant, organiseert en leidt de uitvoering van voldoende maatregelen om een redelijke zekerheid te bieden dat de doelstellingen en doelen zullen worden gerealiseerd.

Beheersomgeving* - De houding en acties van het bestuur en het management met betrekking tot het belang van de beheersing binnen de organisatie. De beheersomgeving bepaalt de discipline en de structuur om de voornaamste doelstellingen van het systeem van interne beheersing te realiseren. De beheersomgeving omvat de volgende aspecten:

- de integriteit en de ethische waarden;
- de filosofie en de operationele stijl van het management;
- de structuur van de organisatie;
- het toewijzen van bevoegdheden en verantwoordelijkheden;
- personeelsbeleid en procedures;
- de competentie van het personeel.

Fraude* - Elke onwettige handeling die wordt gekenmerkt door bedrog, verduistering of inbreuk op het vertrouwen. Daarbij gaat het niet om handelingen die worden verricht onder dreiging met geweld of fysieke dwang. Fraude wordt gepleegd door partijen en organisaties om geld, eigendommen of diensten te verkrijgen, ter voorkoming van uitgaven of verlies van diensten of om persoonlijke of zakelijke voordelen veilig te stellen.

Risico* - De mogelijkheid van het optreden van een gebeurtenis die een impact heeft op het behalen van de doelstellingen. Risico wordt gemeten in termen van impact en waarschijnlijkheid.

Bijlage C. Voorbeelden van frauduleuze handelingen

De hiernavolgende voorbeelden van frauduleuze handelingen vormen geen uitputtende of geprioriteerde lijst. De voorbeelden worden slechts geboden om het bewustzijn van potentiële frauderisico's te stimuleren. De frauderisico's zijn gecategoriseerd naar type rationalisatie.

Voorbeelden van fraude die wordt gepleegd in het directe voordeel van de pleger, zijn onder meer:

- bewuste verschuiving van omzet naar een medewerker, stakeholder of externe partij, terwijl deze normaal gesproken winst zou genereren voor de organisatie;
- malversatie (bijv. verduistering van gelden of bezittingen, en vervalsing van de financiële administratie om de handeling te verdoezelen);
- spionage, met inbegrip van onderzoek en ontwikkeling;
- bewuste versluiering of verkeerde voorstelling van gebeurtenissen, transacties of gegevens;
- vorderingen die worden ingediend voor goederen of diensten die in werkelijkheid niet aan de organisatie zijn geleverd;
- bewust verzuim om te handelen wanneer actie vereist is door de organisatie of van rechtswege;
- onbevoegd of onwettelijk gebruik van vertrouwelijke of bedrijfseigen informatie;
- onbevoegde of onwettelijke manipulatie van IT-netwerken of besturingssystemen;
- diefstal;
- acceptatie van steekpenningen of smeergelden.

Voorbeelden van fraude die direct ten goede komt aan de organisatie, zijn onder meer:

- onjuiste voorstelling van financiële of niet-financiële gegevens, met inbegrip van de waardering van transacties, activa, passiva, inkomsten of statistische gegevens (met name bij fusies en acquisities);
- verrekenprijzen (d.w.z. de waardering van goederen die worden uitgewisseld tussen gelieerde ondernemingen) waardoor management de resultaten kan verbeteren in het nadeel van concurrerende organisaties;
- activiteiten tussen gerelateerde partijen waarbij de ene partij een voordeel ontvangt dat bij een zakelijke transactie niet zou zijn ontvangen;
- verzuim om belangrijke informatie nauwkeurig of volledig vast te leggen of bekend te maken, waardoor een verbeterde, maar verkeerde voorstelling van de organisatie naar externe partijen ontstaat;
- verkoop of toewijzing van niet-bestaande of verkeerde voorgestelde activa;
- bewust verzuim om te handelen wanneer actie vereist is door de organisatie of van rechtswege;
- wezenlijke verdraaiing van financiële gegevens of andere nalevingsactiviteiten om de aandelenkoers omhoog te stuwen, concurrentievoordeel te behalen of de belastingdruk te reduceren of boetes te omzeilen;
- bedrijfsactiviteiten die inbreuk maken op de wet- en regelgeving of op contracten;
- illegale politieke bijdragen, smeergelden en steekpenningen die worden geboden aan klanten of leveranciers, of betalingen aan overheidsfunctionarissen of hun tussenpersonen.

Bijlage D. Potentiële woordkeuzen waarbij men extra alert moet zijn

De volgende tabel bevat voorbeelden van woordkeuzen van ondervraagden die in bepaalde omstandigheden of in een bepaalde context scepsis kunnen oproepen bij een internal auditor, en zo moeten leiden tot aanvullend onderzoek.

🚩 Potentiële woordkeuzen waarbij men extra alert moet zijn		
Agressief	Dwang	Opnieuw toewijzen
Anticiperen	Gefragmenteerd	Reserves
Veronderstellen	Freelance	Herzien
Uitdagend	Interpretatie	Riskant
Complex	Kwestie	Situatiegebonden
Zorg	Maskeren	Gladstrijken
Creatief	Non-conformistisch	Soms
Opvangen	Aanpassen	Subjectief
Hangt ervan af	Nieuwe manier	Toegespitst
Andere aanpak	Niet zeker	Tijdelijk
Moeilijk	Onofficieel	Overgang
Loskoppelen	Negeren	Onzeker
In ontwikkeling	Mogelijk	Onconventioneel

Bijlage E. Casestudy: Assuranceopdracht inzake kasuitgaven

De volgende casestudy illustreert hoe frauderisico's kunnen worden vastgesteld en gedocumenteerd tijdens de planning van een assuranceopdracht van het kasuitgavenproces. De casestudy behandelt niet alle frauderisico's bij het feitelijke kasuitgavenproces en is evenmin bedoeld als sjabloon of programma voor een risicobeoordeling. Aangezien de kenmerken van elke organisatie anders zijn, werken ook de frauderisico's anders.

Verzamelen informatie

Bij het plannen van een assuranceopdracht inzake kasuitgaven verzamelden de internal auditors de volgende informatie:

- Er bestaat geen verslag van eerdere interne of externe beoordelingen of onderzoeken.
- Medewerkers die bevoegd zijn om de leveranciersgegevens in het leveranciersbestand bij te werken, kunnen ook betalingen doorvoeren in het systeem.
- Er zijn diverse medewerkers met superuser-toegang tot crediteurenfuncties: beheren van het leveranciersbestand, aanmaken van facturen, algemene goedkeuring van facturen en bijwerken van betalingsgegevens.
- De procedure van goedkeuring wordt niet consequent toegepast en vaak in het systeem overschreven.
- Beoordelingen en goedkeuringen van kasuitgaven worden niet consequent toegepast.
- De inkomsten zijn aanzienlijk afgenomen ten opzichte van het voorgaande jaar, terwijl in dezelfde periode de bedrijfsuitgaven onverwacht zijn toegenomen.
- Bonussen worden alleen toegekend als de financiële doelen worden behaald.
- Uit gesprekken met het HR-personeel bleek dat de supervisor van de crediteuren beschuldigd is van ongepast familiaire omgang met de medewerkers die aan hem moeten rapporteren.
- De supervisor is behoorlijk vriendschappelijk en vertrouwensvol ten aanzien van het personeel bij de crediteurenafdeling.

Brainstormen over fraudescenario's

Internal auditors hebben tijdens de brainstormsessies inzake de fraudescenario's de volgende informatie gedocumenteerd:

Fraudefactoren	Fraudescenario's
Druk	Er worden substantiële bonussen toegekend als de financiële doelen worden behaald.
	Sommige medewerkers maken zich zorgen over de beperkte opwaartse doorstroom en/of zijn bang hun baan te verliezen.
	Dit jaar worden mogelijk geen bonussen uitgekeerd.
	Een van de medewerkers was onlangs aan het opscheppen tegen zijn collega's over haar luxueuze levensstijl.
Gelegenheid	De taken zijn niet naar behoren gescheiden.
	De relaties tussen medewerkers en het management zijn mogelijk ongepast. Een medewerker heeft een wel erg hechte relatie met haar manager.
	Diverse medewerkers delen dezelfde inlogtoegang als beheerder en de betalingsverwerkingsgegevens en bankgegevens kunnen worden gewijzigd door medewerkers met beheerderstoegang.
	Het leveranciersbestand kan worden bijgewerkt door alle medewerkers en het systeem houdt de veranderingshistorie niet bij.
Rationalisatie	Medewerkers ervaren soms vriendjespolitiek en voelen zich soms overgeslagen of zijn soms rancuneus.
	Medewerkers constateren mogelijk dat het management blijk geeft van een negatieve "toon aan de top" (voorbeeldfunctie).
	Ongepast gedrag lijkt gangbaar.

Beoordeling van frauderisico's en vaststelling van beheersingsmaatregelen

Internal auditors stelden de volgende frauderisico- en controlematrix op om in het opdrachtplan op te nemen.

Fraudescenario	Frauderisico	Impact (L, M, H)	Waarschijnlijkheid (L, M, H)	Maatregel
A. Niet-goedgekeurde leveranciers.	A.1 Er worden fictieve leveranciers ingevoerd in het systeem, wat kan resulteren in frauduleuze betalingen.	H	H	• Functiescheiding. • Periodieke beoordeling van het leveranciersbestand.
	A.2 Adressen van leveranciers worden vervangen met die van medewerkers of de betalingsgegevens worden gewijzigd in de bankgegevens van de medewerker.	M	M	• Goedkeuring management vereist voor het bijwerken van adressen van leveranciers en gegevens voor elektronische overboekingen.
B. Onjuiste betalingen.	B.1 Er worden fictieve terugbetalingen verwerkt voor een betaling.	M	M	• Goedkeuring management vereist voor vergoedingen.
	B.2 In het systeem worden fictieve of dubbele goedkeuringen van facturen genegeerd.	H	H	• Goedkeuring management vereist voordat betaling kan worden verwerkt.
C. Samenspanning.	C.1 Supervisor spant samen met medewerker om bestaande controles te negeren.	H	M	• Geen

Opnemen van de resultaten in het opdrachtplan

Nadat de frauderisico- en controlematrix is opgesteld, nemen de internal auditors de frauderisicoanalyse en de voorlopige bevindingen in het assuranceopdrachtplan voor de kasuitgaven op. Daarbij worden de volgende opmerkingen opgenomen:

- Houd het leveranciersbestand met namen en adressen tegen het licht om te kijken of er dubbele leveranciers in voorkomen.
- Onderzoek of er leveranciersnamen zijn met verschillende adressen en/of betalingsgegevens.
- Controleer de adressen en bankgegevens van leveranciers op matches met gegevens van medewerkers.
- Controleer of er leveranciersadressen voorkomen, die een particulier adres of een postbus zijn.
- Controleer de historie van facturen en bijbehorende betalingen op dubbele factuurnummers of zich herhalende betalingsbedragen.
- Doorloop het betalingsproces en controleer op problemen met functiescheiding in verband met goedkeuringen.

Dankwoord

Guidance Development Team
Glenn Ho, CIA, CRMA, Zuid-Afrika (Voorzitter)
Doug Hileman, CRMA, CPEA, Verenigde Staten (Project Lead)
Caroline Glynn, CIA, Verenigde Staten
John Mickevice, CIA, CRMA, Verenigde Staten
Daniel Samson, CIA, Verenigde Staten

Global Guidance Contributors
Awad Elkarim Mohamed Ahmed, CIA, CCSA, CFSA, CGAP, CRMA, Verenigde Arabische Emiraten
Elastos Chimwanda, CIA, Zimbabwe
Dana Lawrence, CIA, CFSA, CRMA, Verenigde Staten
Barry Smit, CIA, Zuid-Afrika
Dr. Gokhan Sungun, CIA, CCSA, CRMA, Verenigde Staten
Oliver Sznitkies, Frankrijk

IIA Global Standards and Guidance
Christine Hovious, CIA, CRMA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, vicepresident
Debi Roth, CIA, Managing Director
Lauressa Nelson, technisch schrijver
Christina Brune, technisch schrijver

Het IIA wil de volgende toezichthoudende instanties bedanken voor hun steun: Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, en International Professional Practices Framework Oversight Council.

Over het IIA

Het Instituut van Internal Auditors (IIA) is de meest erkende pleitbezorger, opleider en leverancier van standaarden en richtlijnen voor en certificeringen van interne auditors. Het IIA is opgericht in 1941 en bedient op dit moment meer dan 195.000 leden uit meer dan 170 landen en regio's. Het wereldwijde hoofdkantoor van de vereniging bevindt zich in Lake Mary, Florida, VS. Ga voor meer informatie naar www.globaliia.org of www.theiia.org.

Over aanvullende richtlijnen

Aanvullende richtlijnen maken deel uit van het International Professional Practices Framework (IPPF) van het IIA en bieden aanvullende aanbevolen (niet-verplichte) richtlijnen voor het uitvoeren van internal auditactiviteiten. Hoewel ze de internationale standaarden voor de beroepsuitoefening van internal auditing ondersteunen, zijn de aanvullende richtlijnen niet bedoeld om rechtstreeks te verwijzen naar het bereiken van naleving van de Standaarden. Ze zijn in plaats daarvan bedoeld om actuele onderwerpen aan te pakken, evenals sectorspecifieke kwesties, en ze bevatten gedetailleerde processen en procedures. Deze richtlijnen worden door middel van formele beoordelings- en goedkeuringsprocessen onderschreven door het IIA.

Praktijkgidsen
Praktijkgidsen zijn een soort aanvullende richtlijnen die gedetailleerde sturing bieden voor het verrichten van internal auditactiviteiten. Ze bevatten gedetailleerde processen en procedures, zoals hulpmiddelen en technieken, programma's en stapsgewijze benaderingen, evenals voorbeelden van te leveren producten. Als onderdeel van de richtlijnen van het IPPF wordt het aanhouden van de praktijkgidsen aanbevolen (niet-verplicht). De praktijkgidsen worden door middel van formele beoordelings- en goedkeuringsprocessen onderschreven door het IIA.

Een "Global Technologies Audit Guide" (GTAG) is een soort praktijkgids die is geschreven in directe bedrijfstaal en waarin een actuele kwestie met betrekking tot het beheer, de controle en de beveiliging van informatietechnologie wordt behandeld.

Voor andere gezaghebbende richtlijnen die door het IIA worden geleverd, verwijzen we u naar onze website op www.globaliia.org/standards-guidance of www.theiia.org/guidance.

Disclaimer

Het IIA publiceert dit document voor informatieve en educatieve doeleinden. De praktijkgids bevat geen definitieve antwoorden op specifieke individuele omstandigheden en is als zodanig slechts bedoeld om te worden gebruikt als leidraad. Het IIA adviseert om altijd onafhankelijk deskundig advies in te winnen dat rechtstreeks betrekking heeft op een specifieke situatie. Het IIA accepteert geen verantwoordelijkheid wanneer iemand alleen op deze richtlijnen afgaat.

Copyright

Oktober 2017

Instituut van
Internal Auditors
Nederland

Burgemeester Stramanweg 102a
1101 AA Amsterdam
www.iia.nl
iia@iia.nl
Tel.: 088 00 37 100