HET THREE LINES MODEL VAN HET IIA

Een update van de 'Three Lines of Defense'

The Institute of Internal Auditors | Global

Inhoudsopgave

Inleiding 1

Beginselen van het Three Lines Model 2

- Beginsel 1: Governance 2
- Beginsel 2: Rollen van het bestuursorgaan 2
- Beginsel 3: Management en eerste- en tweedelijnsrollen 3
- Beginsel 4: Derdelijnsrollen 3
- Beginsel 5: Derdelijnsonafhankelijkheid 3
- Beginsel 6: Het creëren en beschermen van waarde 3

Kernrollen in het Three Lines Model 5

- Het bestuursorgaan 5
- Management 5
- Internal audit 6
- Externe auditors 6

Relaties tussen kernrollen 7

- Tussen het bestuursorgaan en het management (zowel eerste- als tweedelijnsrollen) 7
- Tussen het management (zowel eerste- als tweedelijnsrollen) en internal audit 7
- Tussen internal audit en het bestuursorgaan 8
- Tussen alle rollen 8

Het model toepassen 9

- Structuur, rollen en verantwoordelijkheden 9
- Toezicht en assurance 10
- Coördinatie en afstemming 10

INLEIDING

Organisaties zijn ondernemingen van mensen, die actief zijn in een wereld die steeds onzekerder, complexer, meer onderling verbonden en volatiel wordt. Vaak hebben ze meerdere stakeholders met verschillende, veranderende en soms tegengestelde belangen. Stakeholders vertrouwen het toezicht op de organisatie toe aan een bestuursorgaan, dat op zijn beurt middelen en bevoegdheden aan het management delegeert om passende actie te ondernemen, inclusief risicomanagement.

Onder meer om deze redenen hebben organisaties effectieve structuren en processen nodig die het mogelijk maken doelstellingen te realiseren, en die tegelijkertijd een sterke governance en risicomanagement ondersteunen. Aangezien het bestuursorgaan van het management rapportages over activiteiten, resultaten en prognoses ontvangt, rekent zowel het bestuursorgaan als het management erop dat internal audit bij alle vraagstukken onafhankelijke, objectieve assurance en adviezen verstrekt, en innovatie en verbetering bevordert en faciliteert. Het bestuursorgaan is eindverantwoordelijk voor de governance, die door de acties en handelwijzen van het bestuursorgaan, het management en internal audit wordt verwezenlijkt.

Het Three Lines Model helpt organisaties structuren en processen in kaart te brengen die het beste bijdragen aan het realiseren van doelstellingen en die een sterke governance en risicomanagement faciliteren. Het model is op alle organisaties van toepassing en wordt geoptimaliseerd door het volgende:

- Een op beginselen gebaseerde aanpak hanteren en het model aanpassen aan de doelstellingen en omstandigheden van de organisatie.
- Focussen op de bijdrage die risicomanagement levert aan het realiseren van doelstellingen en het creëren van waarde, en ook aan de 'verdediging' en het beschermen van waarde.
- Een helder inzicht in de rollen en verantwoordelijkheden in het model en de onderlinge relaties.
- Maatregelen nemen om ervoor te zorgen dat activiteiten en doelstellingen zijn afgestemd op de voornaamste belangen van stakeholders.

Kernbegrippen

Organisatie – Een georganiseerde groep activiteiten, middelen en mensen die toewerken naar gezamenlijke doelen.

Stakeholders – Groepen en personen wier belangen door de organisatie worden behartigd of beïnvloed.

Bestuurslichaam – Degenen die aan stakeholders verantwoording afleggen voor het succes van de organisatie.

Management – De personen, teams en ondersteunende functies die zijn aangewezen om producten en/of diensten te leveren aan de klanten van de organisatie.

Internal audit – Personen die onafhankelijk van het management opereren om assurance te verschaffen over en inzicht te geven in de toereikendheid en effectiviteit van governance en risicomanagement (inclusief interne beheersing).

Het Three Lines Model – Het model dat eerder bekend stond onder de naam de 'Three Lines of Defense'.

Interne beheersing – Processen die erop gericht zijn redelijke zekerheid te verschaffen over het realiseren van doelstellingen.

BEGINSELEN VAN HET THREE LINES MODEL

Beginsel 1: Governance

Voor de governance van een organisatie zijn passende structuren en processen nodig die het volgende mogelijk maken:

- **Verantwoording** die een bestuurslichaam aan stakeholders aflegt voor toezicht op de organisatie door integriteit, leiderschap en transparantie.
- **Acties** (inclusief risicomanagement) van het management om de doelstellingen van de organisatie te realiseren door risicogebaseerde besluitvorming en de inzet van middelen.
- **Assurance en adviezen** door een onafhankelijke internal auditfunctie om helderheid en zekerheid te verschaffen, en voortdurende ontwikkeling te bevorderen en te faciliteren door nauwgezet onderzoek en verhelderende communicatie.

Kernbegrippen

Risicogebaseerde besluitvorming – Een weloverwogen proces dat analyse, planning, actie, monitoring en review omvat en rekening houdt met de mogelijke gevolgen van onzekerheid voor de doelstellingen.

Assurance – Onafhankelijke bevestiging en zekerheid.

Beginsel 2: Rollen van het bestuursorgaan

Het bestuursorgaan zorgt voor het volgende:

- Er zijn passende structuren en processen voor een effectieve governance.
- De doelstellingen en activiteiten van de organisatie zijn afgestemd op de voornaamste belangen van stakeholders.

Het bestuursorgaan:

- Delegeert verantwoordelijkheid en stelt het management middelen beschikbaar om de doelstellingen van de organisatie te realiseren en waarborgt tegelijkertijd dat de verwachtingen op het gebied van wet- en regelgeving en ethiek worden ingelost.
- Creëert en houdt toezicht op een onafhankelijke, objectieve en competente internal auditfunctie om helderheid en vertrouwen te verschaffen over de voortgang in het realiseren van doelstellingen.

Beginsel 3: Management en eerste- en tweedelijnsrollen

De verantwoordelijkheid van het management om doelstellingen van de organisatie te realiseren omvat zowel eerste- als tweedelijnsrollen. [1] *Eerstelijnsrollen* zijn het meest direct afgestemd op het leveren van producten en/of diensten aan opdrachtgevers van de organisatie, inclusief ondersteunende functies[2]. *Tweedelijnsrollen* verlenen assistentie bij risicomanagement.

Eerste- en tweedelijnsrollen kunnen worden gemixt of gescheiden blijven. Sommige tweedelijnsrollen kunnen aan specialisten worden toegewezen om aanvullende expertise, ondersteuning, monitoring en een kritische blik te bieden voor degenen met een eerstelijnsrol. Tweedelijnsrollen kunnen zich richten op specifieke doelstellingen van risicomanagement, zoals: naleving van wet- en regelgeving, en aanvaardbaar ethisch gedrag; interne beheersing; beveiliging van informatie en technologie; duurzaamheid; en kwaliteitsborging. Tweedelijnsrollen kunnen ook een bredere verantwoordelijkheid voor risicomanagement omvatten, zoals Enterprise Risk Management (ERM). De verantwoordelijkheid voor het managen van risico's blijft echter onderdeel van de eerstelijnsrollen en onder de scope van het management vallen.

Beginsel 4: Derdelijnsrollen

Internal audit geeft onafhankelijke en objectieve assurance en adviezen over de toereikendheid en effectiviteit van governance en risicomanagement. Dit bereikt zij door het deskundig toepassen van systematische en gedisciplineerde processen, expertise en inzichten. Internal audit rapporteert haar bevindingen aan het management en het bestuursorgaan om continue verbetering te bevorderen en te faciliteren. Daarbij kan internal audit overwegen assurance van andere interne en externe organen te verkrijgen.

Beginsel 5: Derdelijnsonafhankelijkheid

De onafhankelijkheid van internal audit van de verantwoordelijkheden van het management is cruciaal voor haar objectiviteit, autoriteit en geloofwaardigheid. Deze onafhankelijkheid wordt tot stand gebracht door: verantwoording aan het bestuursorgaan; vrije toegang tot mensen, middelen en gegevens die nodig zijn om haar werkzaamheden af te ronden; en het onpartijdig en ongehinderd plannen en leveren van auditdiensten.

Beginsel 6: Het creëren en beschermen van waarde

Alle rollen die samenwerken dragen gezamenlijk bij aan het creëren en beschermen van waarde wanneer zij op elkaar en op de voornaamste belangen van stakeholders zijn afgestemd. Het op elkaar afstemmen van activiteiten wordt gerealiseerd door communicatie, samenwerking en medewerking Dit zorgt ervoor dat de informatie die nodig is voor risicogebaseerde besluitvorming betrouwbaar, samenhangend en transparant is.

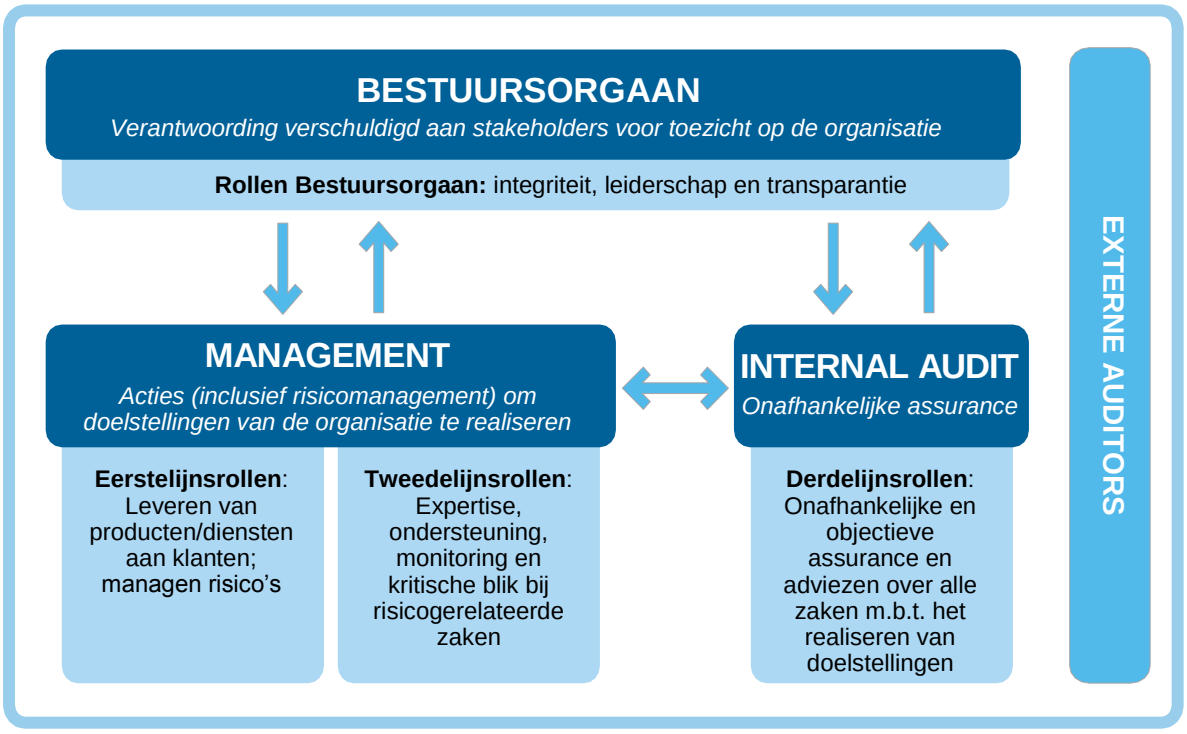
---

1. In verband met de herkenbaarheid zijn de termen 'eerste lijn, 'tweede lijn' en 'derde lijn' uit het oorspronkelijke model behouden. De 'lijnen' verwijzen echter niet naar structuur elementen, maar dienen om rollen op een zinvolle manier van elkaar te onderscheiden. Logischerwijs vormen bestuursorganen ook een 'lijn', maar om verwarring te voorkomen is van dit gebruik afgezien. De nummering (eerste, tweede, derde) moet niet worden opgevat als een opeenvolging van activiteiten. In plaats daarvan worden alle rollen gelijktijdig vervuld.

2. Sommigen zien ondersteunende functies (zoals HR, administratie en gebouwendiensten) als tweedelijnsrollen. Voor alle duidelijkheid: in het Three Lines Model omvatten *eerstelijnsrollen* activiteiten aan zowel de 'voor-' als 'achterkant' (front- en back-office), en onder *tweedelijnsrollen* vallen aanvullende activiteiten die gericht zijn op risicogerelateerde zaken.

3. In sommige organisaties worden andere derdelijnsrollen geïdentificeerd, zoals toezicht, inspectie, onderzoek, evaluatie en herstel, die deel uitmaken van de internal auditfunctie of afzonderlijk worden vervuld.

Het Three Lines Model van het IIA



LEGENDA: ↑ Verantwoording, rapporteren | ↓ Delegeren, richting, middelen, toezicht | ↔ Afstemming, communicatie, coördinatie, samenwerking

KERNROLLEN IN HET THREE LINES MODEL

Organisaties verschillen sterk van elkaar wat betreft de verdeling van verantwoordelijkheden. Onderstaande rollen op hoog niveau dragen echter bij het aan versterken van de beginselen van het Three Lines Model.

Het bestuursorgaan

- Legt aan stakeholders verantwoording af voor het toezicht op organisatie.
- Gaat de dialoog aan met stakeholders om hun belangen te behartigen en transparant te communiceren over het realiseren van doelstellingen.
- Stimuleert een cultuur die ethisch gedrag en verantwoording bevordert.
- Ontwikkelt structuren en processen voor governance, waar nodig inclusief ondersteunende commissies.
- Delegeert verantwoordelijkheid en stelt het management middelen beschikbaar om de doelstellingen van de organisatie te realiseren.
- Bepaalt de risicobereidheid van de organisatie en oefent toezicht uit op risicomanagement (inclusief interne beheersing).
- Ziet erop toe dat de verwachtingen op het gebied van wet- en regelgeving en ethiek worden ingelost.
- Richt een onafhankelijke, objectieve en competente internal auditfunctie in en houdt daarop toezicht.

Management

Eerstelijnsrollen

- Geeft leiding en sturing aan acties (inclusief risicomanagement) en de inzet van middelen om de doelstellingen van de organisatie te realiseren.
- Blijft voortdurend in dialoog met het bestuursorgaan en rapporteert over: geplande, werkelijke en verwachte resultaten die gekoppeld zijn aan de doelstellingen van de organisatie; en risico.
- Ontwikkelt en onderhoudt passende structuren en processen voor het beheer van activiteiten en risico (inclusief interne beheersing).
- Zorgt dat de verwachtingen op het gebied van wet- en regelgeving en ethiek worden ingelost.

Tweedelijnsrollen

- Voorziet in aanvullende expertise, ondersteuning, monitoring en een kritische blik met betrekking tot risicomanagement, waaronder:
    - De ontwikkeling, implementatie en voortdurende verbetering van risicomanagementpraktijken (inclusief interne beheersing) op het niveau van processen, systemen en entiteiten.
    - Het realiseren van doelstellingen voor risicomanagement, zoals: naleving van wet- en regelgeving, en aanvaardbaar ethisch gedrag; interne beheersing; beveiliging van informatie en technologie; duurzaamheid; en kwaliteitsborging.
- Verstrekt analyses en rapporteert over de toereikendheid en effectiviteit van risicomanagement (inclusief interne beheersing).

Internal audit

- Legt primair verantwoording af aan het bestuursorgaan en blijft onafhankelijk van de verantwoordelijkheden van het management.
- Communiceert onafhankelijke en objectieve assurance en adviezen aan het management en het bestuursorgaan met betrekking tot de toereikendheid en effectiviteit van governance en risicomanagement (inclusief interne beheersing) om het realiseren van doelstellingen van de organisatie te ondersteunen en continue verbetering te bevorderen en te faciliteren.
- Rapporteert aantasting van de onafhankelijkheid en objectiviteit aan het bestuursorgaan en voert waar nodig waarborgen in.

Externe auditors

- Bieden aanvullende assurance om:
    - Verwachtingen op het gebied van wet- en regelgeving in te lossen ter bescherming van de belangen van stakeholders.
    - Verzoeken van het management en het bestuursorgaan in te willigen om interne bronnen van assurance aan te vullen.

RELATIES TUSSEN KERNROLLEN

Tussen het bestuursorgaan en het management (zowel eerste- als tweedelijnsrollen)

Het bestuursorgaan bepaalt doorgaans de koers van de organisatie door de visie, missie, waarden en risicobereidheid van de organisatie vast te stellen. Vervolgens delegeert het bestuursorgaan de verantwoordelijkheid voor het realiseren van de doelstellingen van de organisatie aan het management, samen met de benodigde middelen. Van het management ontvangt het bestuursorgaan rapportages over geplande, werkelijke en verwachte resultaten, alsmede rapportages over risico's en risicomanagement.

Kernbegrip

Chief Executive Officer (CEO) – De hoogst verantwoordelijke voor de operationele activiteiten binnen de organisatie.

Organisaties verschillen in de mate van overlap en scheiding tussen de rollen van het bestuursorgaan en het management. Het bestuursorgaan kan meer of minder 'hands-on' te werk gaan bij strategische en operationele aangelegenheden. Het bestuursorgaan of het management kan het voortouw nemen bij de ontwikkeling van het strategisch plan, maar het kan ook een gezamenlijke onderneming zijn. In sommige rechtsgebieden kan de Chief Executive Officer (CEO) lid zijn van het bestuursorgaan en zelfs het bestuursorgaan voorzitten. In alle gevallen moet er tussen het management en het bestuursorgaan een sterke communicatie zijn. Gebruikelijk is de CEO het aanspreekpunt voor deze communicatie, maar andere senior managers kunnen ook veelvuldig overleg plegen met het bestuursorgaan. Soms willen organisaties, en stellen toezichthouders dit verplicht, dat leidinggevenden van tweedelijnsrollen, zoals een Chief Risk Officer (CRO) en een Chief Compliance Officer (CCO) een directe rapportagelijn naar het bestuursorgaan hebben. Dit is volledig in overeenstemming met de beginselen van het Three Lines Model.

Tussen het management (zowel eerste- als tweedelijnsrollen) en internal audit

De onafhankelijkheid van het management zorgt ervoor dat internal audit haar werkzaamheden vrij en ongehinderd kan verrichten, en vrij toegang heeft tot de vereiste mensen, middelen en gegevens. Internal audit is verantwoording schuldig aan het bestuursorgaan. Onafhankelijkheid bekent echter niet afzondering. Er moet tussen internal audit en het management regelmatig contact zijn om ervoor te zorgen dat het werk van internal audit relevant is en aansluit op de strategische en operationele behoeften van de organisatie. Door al haar activiteiten bouwt internal audit kennis en begrip van de organisatie op, wat bijdraagt aan de assurance en adviezen die internal audit biedt als vertrouwde adviseur en strategische partner. Tussen zowel de eerste- als tweedelijnsrollen van het management en internal audit bestaat er behoefte aan samenwerking en communicatie om onnodig dubbel werk, overlapping of lacunes te voorkomen.

Tussen internal audit en het bestuursorgaan

Internal audit is verantwoording schuldig aan, en wordt soms omschreven als de 'ogen en oren' van, het bestuursorgaan.

Het bestuursorgaan is verantwoordelijk voor het toezicht op internal audit en dit houdt in: zorgen voor de inrichting van een onafhankelijke internal auditfunctie, inclusief het benoemen en ontslaan van het hoofd van de internal auditfunctie (Chief Audit Executive, CAE); fungeren als primaire rapportagelijn voor de CAE[4]; het auditplan goedkeuren en daarvoor middelen beschikbaar stellen; rapportages van de CAE ontvangen en bestuderen; en ervoor zorgen dat de CAE vrij toegang heeft tot het bestuursorgaan, inclusief vertrouwelijke sessies zonder de aanwezigheid van het management.

Kernbegrip

Chief Audit Executive (CAE) – De hoogst verantwoordelijke voor de internal audit diensten binnen de organisatie, vaak onder de titel Hoofd Internal Audfit of een vergelijkbare titel.

Tussen alle rollen

Het bestuursorgaan, het management en internal audit hebben duidelijk verschillende verantwoordelijkheden. Alle activiteiten moeten echter worden afgestemd op de doelstellingen van de organisatie. De basis voor een geslaagde samenhang is regelmatige en effectieve coördinatie, samenwerking en communicatie.

4. Voor bestuurlijke doeleinden kan de CAE ook rapporteren aan een managementlaag van voldoende hoog niveau.

HET MODEL TOEPASSEN

Structuur, rollen en verantwoordelijkheden

Het Three Lines Model is het meest effectief wanneer het wordt afgestemd op de doelstellingen en omstandigheden van de organisatie. Hoe een organisatie wordt gestructureerd en hoe rollen worden toegewezen zijn zaken die het management en het bestuursorgaan moeten bepalen. Het bestuursorgaan kan commissies instellen om extra toezicht te houden op bepaalde aspecten die onder de verantwoordelijkheid van het bestuursorgaan vallen, zoals audit, risico, financiën, planning en beloning. Binnen het management zijn er waarschijnlijk functionele en hiërarchische structuren en is er vaak sprake van specialisatie naarmate organisaties groter en complexer worden.

Functies, teams en ook personen hebben verantwoordelijkheden die eerste- en tweedelijnsrollen omvatten. De inrichting van de tweedelijnsrollen en het toezicht daarop kunnen zodanig worden ontworpen dat ze een bepaalde mate van onafhankelijkheid waarborgen ten opzichte van die van de eerstelijnsrollen – en ook van de hoogste managementniveaus – door de primaire verantwoording aan en rapportagelijnen naar het bestuursorgaan. In het Three Lines Model zijn zoveel rapportagelijnen tussen het management en het bestuursorgaan mogelijk als er nodig zijn. In sommige organisaties, met name onder toezicht vallende financiële instellingen, is er een wettelijke verplichting om voldoende onafhankelijkheid te waarborgen. Ook in deze situaties blijven degenen in het management met eerstelijnsrollen verantwoordelijk voor risicomanagement.

Tweedelijnsrollen omvatten het monitoren, adviseren, begeleiden, toetsen, analyseren en rapporteren van zaken die verband houden met het managen van risico's. Voor zover ze ondersteuning en een kritische blik bieden voor degenen met eerstelijnsrollen en integraal onderdeel zijn van besluiten en acties van het management, maken tweedelijnsrollen deel uit van de verantwoordelijkheden van het management en zijn ze nooit volledig onafhankelijk van het management, ongeacht rapportagelijnen en verantwoordelijkheden.

Kenmerkend voor derdelijnsrollen is de onafhankelijkheid van het management. De beginselen van het Three Lines Model beschrijven het belang en de aard van de onafhankelijkheid van internal audit, waardoor internal audit zich onderscheidt van andere functies, en assurance en adviezen van bijzondere waarde kan geven. De onafhankelijkheid van internal audit wordt gewaarborgd door geen besluiten te nemen of acties te ondernemen die deel uitmaken van de verantwoordelijkheden van het management (inclusief risicomanagement) en door af te zien van het bieden van assurance bij activiteiten waarvoor internal audit momenteel of recentelijk verantwoordelijk is of was. Zo wordt in sommige organisaties de CAE gevraagd aanvullende besluitvormingsverantwoordelijkheden op zich te nemen voor activiteiten die gebruikmaken van soortgelijke competenties, zoals aspecten van nakoming van wettelijke verplichtingen of Enterprise Risk Management (ERM). In deze omstandigheden is internal audit niet onafhankelijk van deze activiteiten of de resultaten daarvan. Wanneer het bestuursorgaan onafhankelijke en objectieve assurance en adviezen op deze gebieden wenst, moet dit daarom door een gekwalificeerde derde gebeuren.

Toezicht en assurance

Het bestuursorgaan gaat af op rapportages van het management (degenen met eerste- en tweedelijnsrollen), internal audit en anderen om toezicht uit te oefenen en doelstellingen te realiseren, waarvoor het bestuursorgaan verantwoording aflegt aan stakeholders. Het management verschaft waardevolle assurance (ook wel verklaringen genoemd) over geplande, werkelijke en verwachte resultaten, over risico's en over risicomanagement door te putten uit directe ervaring en deskundigheid. Degenen met tweedelijnsrollen verschaffen aanvullende assurance over risicogerelateerde zaken. Omdat internal audit onafhankelijk is van het management, verschaft de assurance van internal audit de grootste mate van objectiviteit en zekerheid die verder gaat dan wat degenen met eerste- en tweedelijnsrollen het bestuursorgaan kunnen bieden, ongeacht de rapportagelijnen. Verdere assurance kan ook worden verkregen van externe auditors.

Coördinatie en afstemming

Voor een effectieve governance is een juiste toewijzing van verantwoordelijkheden nodig, net als een goede afstemming van activiteiten door samenwerking, medewerking en communicatie. Via internal audit verkrijgt het bestuursorgaan bevestiging dat de governancestructuren- en processen goed zijn opgezet en naar behoren functioneren.

Over het IIA

The Institute of Internal Auditors (IIA) is de meest erkende pleitbezorger, opleider en leverancier van standaarden en richtlijnen voor en certificeringen van interne accountants. Het IIA, opgericht in 1941, bedient op dit moment meer dan 200.000 leden uit meer dan 170 landen en regio's. Het wereldwijde hoofdkantoor van de vereniging bevindt zich in Lake Mary, Fla. USA. Ga voor meer informatie naar www.globaliia.org.

Disclaimer

Copyright

Juli 2020

The Institute of Internal Auditors | Global

Wereldwijd hoofdkantoor
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Telefoon: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org