# Internal Audit Monitor 2021

## Ontwikkelingen in Internal Audit

Instituut van
**Internal Auditors**
*Nederland*

ONE
RISK ADVISORY

## OPDRACHTGEVER

IIA Nederland

## AUTEURS

Robert Bogtstra, Inge Garretsen en Remko Renes

# Inhoudsopgave

# 1 Inleiding

In de herziening van de Nederlandse Corporate Governance Code (de Code) in 2016 werd de Internal Audit Functie (IAF) erkend als essentiële schakel in de besturing en beheersing van de organisatie. Het realiseren daarvan is niet echter niet altijd makkelijk, met name voor de kleinere beursfondsen, en zeker geen 'eenheidsworst'. IIA Nederland heeft sinds 2017 de realisatie van dit principe uit de Code gevolgd met de Internal Audit Monitor. Niet alleen om dit in beeld te hebben, maar vooral om bestuurders en commissarissen handvatten te bieden de IAF binnen hun organisatie zo goed mogelijk in te richten, en daarmee de kwaliteit van de governance waar mogelijk te verbeteren.

In deze Internal Audit Monitor schetsen we wederom de belangrijkste ontwikkelingen van IAF's bij in Nederland beursgenoteerde vennootschappen. We staan, evenals afgelopen jaren, stil bij de ontwikkeling in het aantal en de verschillende verschijningsvormen (intern, uitbesteed, gecombineerd) van IAF's over de boekjaren 2016 – 2020 (hoofdstuk 3).

Een belangrijk onderwerp in de editie van dit jaar is de combinatie van risicomanagement en internal audit activiteiten. Een combinatie die we in de praktijk regelmatig zien en waarover vaak discussie is over de voordelen en mogelijkheden. In hoofdstuk 4 schetsen we de dynamiek ervan en beargumenteren dat deze combinatie – met uitsluiting van de onder toezicht vallende financiële instellingen[1] - (1) onder voorwaarden geen taboe hoeft te zijn vanuit principes voor onafhankelijkheid en (2) kan passen bij de status en inrichting van de governance structuur binnen een organisatie.

We beginnen met de achtergrond en aanpak van het onderzoek. Daarna geven een korte toelichting op de Code, de aandacht die de IAF hierin krijgt en het belang van een kwalitatief goede uitleg in geval van afwijken van de Code (hoofdstuk 2).

1 Bij onder toezicht vallende financiële instellingen is deze combinatie niet toegestaan door onder andere de Code Banken, Basel II en Solvency II.

## 1.1 Achtergrond

In 2017 deed IIA Nederland, in samenwerking met ONE Risk Advisory en Nyenrode Business Universiteit, onderzoek naar IAF's bij beursgenoteerde ondernemingen in Nederland: Internal Audit Monitor 2017[2]. Dit onderzoek gaf inzicht in het aantal IAF's bij Euronext Amsterdam beursgenoteerde ondernemingen met statutaire zetel in Nederland en in de aard en samenstelling van deze IAF's.

In 2020 publiceerden de auteurs een artikel in het Maandblad voor Accountancy en Bedrijfseconomie (MAB) dat ingaat op ontwikkelingen van IAF's in de jaren 2016 – 2018 en op argumenten die organisaties geven voor het niet hebben van een IAF in jaarverslagen over boekjaar 2018[3].

Als vervolg hierop verzocht IIA Nederland, ONE Risk Advisory en Nyenrode Business Universiteit onderzoek te doen naar de meest recente status van internal audit bij Nederlandse beursgenoteerde vennootschappen. IIA Nederland wil hiermee inzicht geven aan bestuurders, commissarissen en internal auditors in recente ontwikkelingen op gebied van internal audit en de inrichting van de IAF, om daarmee handvatten te geven de governance te evalueren en mogelijk te verbeteren.

## 1.2 Aanpak

Deze Internal Audit Monitor 2021 is net als de eerdere onderzoeken gebaseerd op publieke informatie waarin wij hebben vastgesteld of beursgenoteerde vennootschappen over een  beschikken en op welke manier deze is ingericht.

De Internal Audit Monitor 2021 is gebaseerd op de beursnotering en de samenstelling van de verschillende indices (AEX, AMX, AScX en lokale fondsen) per 31 december 2021 en de jaarverslagen over 2020.  Vanwege mutaties in de samenstelling van de indices, zoals nieuwe noteringen alsmede bedrijven die van de beurs zijn verdwenen, zijn de vergelijkende cijfers voor de eerdere jaren (2016 tot en met 2019) soms afwijkend. De vergelijkende cijfers voor beursgenoteerde vennootschappen die in eerdere jaren in een andere index waren opgenomen, zijn opgenomen bij de index waar de bedrijven eind van het verslagjaar zijn genoteerd. Voor bedrijven die voor het eerst in 2020 beursgenoteerd zijn, is voor de eerdere jaren geen informatie opgenomen.

2 Bogtstra, R., R. Renes, (2017), Internal Audit Monitor 2017. Goed bestuur en toezicht verdient een goede Internal Audit Functie, IIA Nederland, Onderzoeksrapport in opdracht van de Stichting Vaktechnisch Onderzoek IIA Nederland. Geraadpleegd op www.IIA.nl

3 Bogtstra R, Garretsen I, Renes R (2020) Compliant in principle! and in practice? Internal audit at listed companies in the Netherlands: beyond compliance with the Dutch Corporate Governance Code. Maandblad Voor Accountancy en Bedrijfseconomie 94(3/4): 93-101.

# 2 De internal audit functie in de huidige Corporate Governance Code

De Nederlandse Corporate Governance Code (2016) besteedt uitgebreid aandacht aan de IAF (principe 1.3 IAF). De Code benoemt niet alleen de IAF nadrukkelijk, maar gaat ook specifiek in op de rol en de taken van internal audit. Het instellen van een IAF is volgens de Code gewenst en organisaties die geen IAF inrichten moeten die keuze - geheel volgens het 'pas toe of leg uit'-principe - toelichten.

We zien dat het belang van de IAF voor een goede governance ook terugkomt in de voorgestelde wijzigingen van de Code in het consultatiedocument van de Monitoring Commissie. Belangrijke voorstellen omtrent de IAF zijn:

- Periodieke onafhankelijke externe toetsing
- Positionering bij voorkeur onder verantwoordelijkheid van CEO
- Direct contact met en rapportage aan voorzitter de Audit Commissie

## 2.1 Pas toe of Leg uit

Uitgangspunt van de Code is niet dat deze naar de letter wordt nageleefd, maar *"de mate waarin de intenties van de Code leidend zijn voor het doen en laten van alle betrokkenen"*. Belangrijk hierbij is het beginsel van 'pas toe of leg uit'. De Code biedt ruimte om af te wijken van de principes en best practice bepalingen. Corporate governance is een kwestie van maatwerk en afwijkingen kunnen gerechtvaardigd zijn.

Eventuele afwijkingen dienen te worden voorzien van een inhoudelijke en inzichtelijke uitleg waarbij uitdrukkelijk wordt aangegeven in hoeverre de in de Code opgenomen principes en best practice bepalingen worden opgevolgd. En zo niet, waarom en in hoeverre hiervan wordt afgeweken. De Code benoemt ook de criteria waaraan moet worden voldaan in geval van afwijking:

i. *de wijze waarop de vennootschap is afgeweken van het principe of de best practice bepaling;*
ii. *de redenen voor afwijking;*
iii. *indien de afwijking tijdelijk is en langer dan één boekjaar duurt, wordt aangegeven wanneer de vennootschap voornemens is het principe of de best practice bepaling weer na te leven; en*
iv. *in voorkomend geval, een beschrijving van de alternatieve maatregel die is genomen en een uiteenzetting hoe die maatregel de doelstelling van het principe respectievelijk de best practice bepaling bereikt, of een verduidelijking hoe de maatregel bijdraagt tot een goede corporate governance van de vennootschap.*

De Code heeft dus geen rigide karakter en biedt de optie om af te wijken van best practices mits er (1) wordt gehandeld naar de 'geest' van de bepalingen voor 'good corporate governance' en (2) deze afwijkingen afdoende worden onderbouwd.

## 2.2 Belang van een kwalitatief goede uitleg

De lat komt steeds hoger te liggen voor wat betreft betekenisvolle verslaggeving door vennootschappen mede als gevolg van strengere vereisten op dat vlak, zoals nieuwe wetgeving op het gebied van ESG rapportering.

Ook voor de kwaliteit van uitleg in geval van afwijken van de Code is steeds meer aandacht. Zo heeft de Monitoring Commissie Corporate Governance Code op 15 december 2021 het "Rapport monitoring boekjaar 2020" uitgebracht, waarin – in tegenstelling tot voorgaande nalevingsonderzoeken door de Monitoring Commissie - de nadruk ligt op de *kwaliteit* van rapportage door vennootschappen. De Commissie concludeert dat: "*beursvennootschappen meer betekenisvol kunnen rapporteren over naleving van de Corporate Governance Code*". Vennootschappen rapporteren vaak procesmatig en sluiten daarbij nauw aan bij de letterlijke tekst van de desbetreffende bepaling in plaats van dat zij kiezen voor een meer inhoudelijk relevante en betekenisvolle rapportage aan de hand van de aanknopingspunten die de onderliggende gedragsbepalingen bieden.

Het rapport benadrukt dat naleving van de Code geen afvinkexercitie moet zijn en roept vennootschappen op om de intenties van de Code te omarmen. Het gebruik van standaardteksten in jaarverslagen past daar niet goed bij. De commissie hecht belang aan de kwaliteit van de toelichting in het algemeen en niet alleen in geval van afwijking van de Code.

Wij begrijpen dat in het volgende nalevingsonderzoek (over boekjaar 2021) de Monitoring Commissie ook extra aandacht zal blijven geven aan de kwaliteit van rapportage door vennootschappen, door een 'pas toe èn leg uit'-benadering te hanteren. Dit is toe te juichen en sluit aan bij ons onderzoek[4] uit 2020 naar beursgenoteerde vennootschappen in Nederland en hun kwalitatieve uitleg bij afwijkingen van de Code over het boekjaar 2018. We benadrukten toen al het belang van een kwalitatief goede uitleg, óók in geval van naleving, en sluiten daarbij aan bij de Zuid-Afrikaanse Corporate Governance Code (King IV) die verklaart:

> *"Explanation also helps to encourage organisations to see corporate governance not as an act of mindless compliance, but something that will yield results only if it is approached mindfully, with due consideration of the organisation's circumstances."*

Eén van de bepalingen die kort wordt aangehaald in het onderzoek van de Monitoring Commissie over boekjaar 2020, is die van het ontbreken van een interne audit dienst (best practice bepaling 1.3.6.):

> *"Indien voor de IAF geen interne audit dienst is ingericht, beoordeelt de raad van commissarissen jaarlijks, mede op basis van een advies van de auditcommissie, of adequate alternatieve maatregelen zijn getroffen en beziet of behoefte bestaat om een interne audit dienst in te richten. De raad van commissarissen neemt de conclusies alsmede eventuele aanbevelingen en alternatief getroffen maatregelen die daaruit voortkomen, op in het verslag van de raad van commissarissen."*

4 MAB onderzoek 2020

Daarover zegt de Monitoring Commissie dat 30,1% van de vennootschappen uitlegt waarom zij geen IAF heeft (gemotiveerde afwijking) en 3,6% geen uitleg geeft (niet-naleving). De 'verondersteld'[5] naleving is daarmee 96,4%. Vennootschappen zonder interne auditdienst beargumenteren daarover meestal dat dat te maken heeft met hun kleine omvang (qua aantal werknemers of omzet) en/of de beperkte complexiteit van hun organisatie of bedrijfsvoering. Dit ligt in lijn met het feit dat vooral lokale vennootschappen niet beschikken over een IAF.

De Code geeft in een toelichting bij deze bepaling aan dat:

> *"Het uitgangspunt is dat vennootschappen voor de uitvoering van de taak van de IAF, een interne audit dienst inrichten. Mocht van dit uitgangspunt worden afgeweken, bijvoorbeeld als de omvang van de vennootschap zich daarvoor niet leent, dan kan uitbesteding een adequaat alternatief zijn."*

De beperkte omvang van de organisatie is volgens deze redenering op zichzelf dus geen gemotiveerde verklaring.

Ons onderzoek uit 2020 laat zien dat een kwalitatief goede uitleg, die voldoet aan de criteria genoemd in de Code, veelal ontbreekt. Slechts drie beursgenoteerde vennootschappen geven een uitleg die voldoet aan de norm zoals uiteengezet in de Code. Zij geven niet alleen een beschrijving van de genomen alternatieve maatregel(en), maar beargumenteren ook hoe deze maatregel(en) de doelstelling van het de best practice bepaling bereikt en/of hoe de maatregelen bijdragen tot goed ondernemingsbestuur van de vennootschap. Er valt dus nog veel te winnen op dit terrein.

5 Veronderstelde naleving: wanneer vennootschappen niet aangeven dat zij afwijken van een bepaling in de Code, moet naleving worden verondersteld.

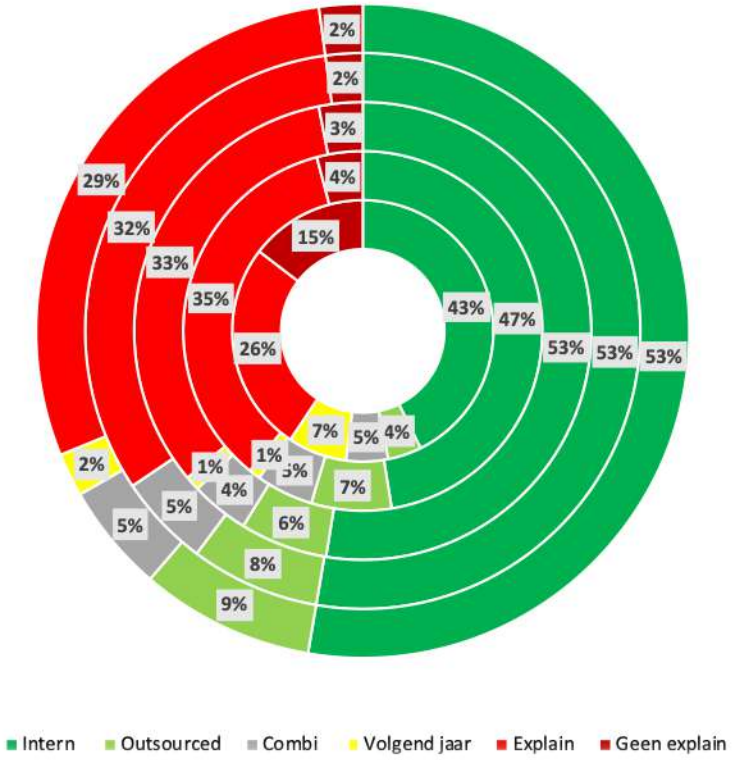
# 3 Ontwikkelingen door de tijd

## 3.1 Ontwikkeling in IAF's afgelopen vijf jaren (2016 – 2020)

Deze paragraaf beschrijft de verschijningsvormen van IAF's. Eerst voor het totaal van de Nederlandse beursfondsen, daarna per type fondsen.

### NEDERLANDSE BEURSFONDSEN TOTAAL

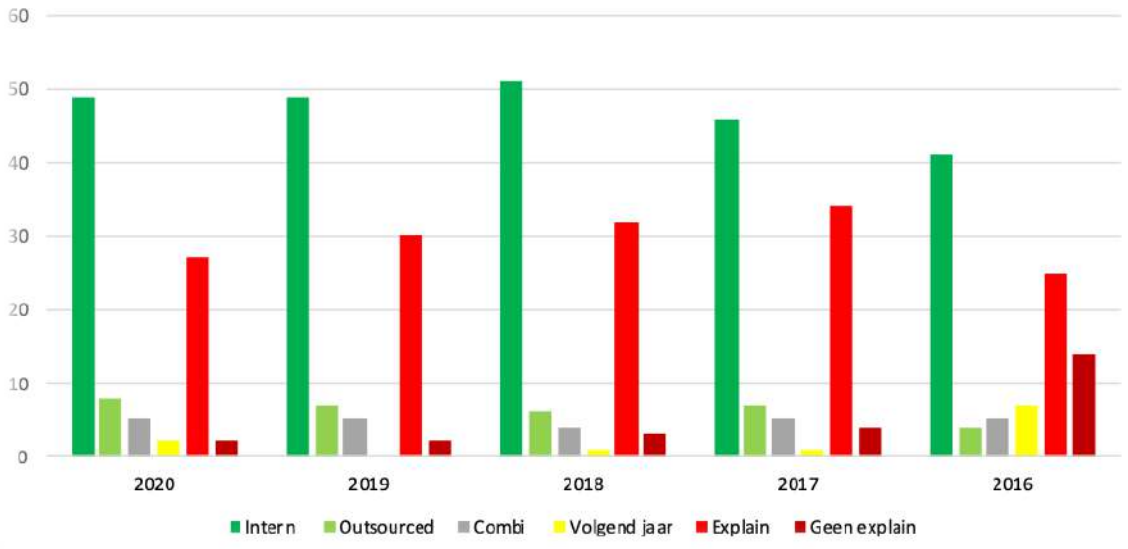
Hieronder zijn drie figuren opgenomen. Figuur 1 beschrijft de verschijningsvormen in percentages van 2016 tot en met 2020. Figuur 2 beschrijft de absolute aantallen in deze periode. Figuur 3 geeft samenvattend inzicht in de percentages met en zonder IAF van 2016 tot en met 2020.



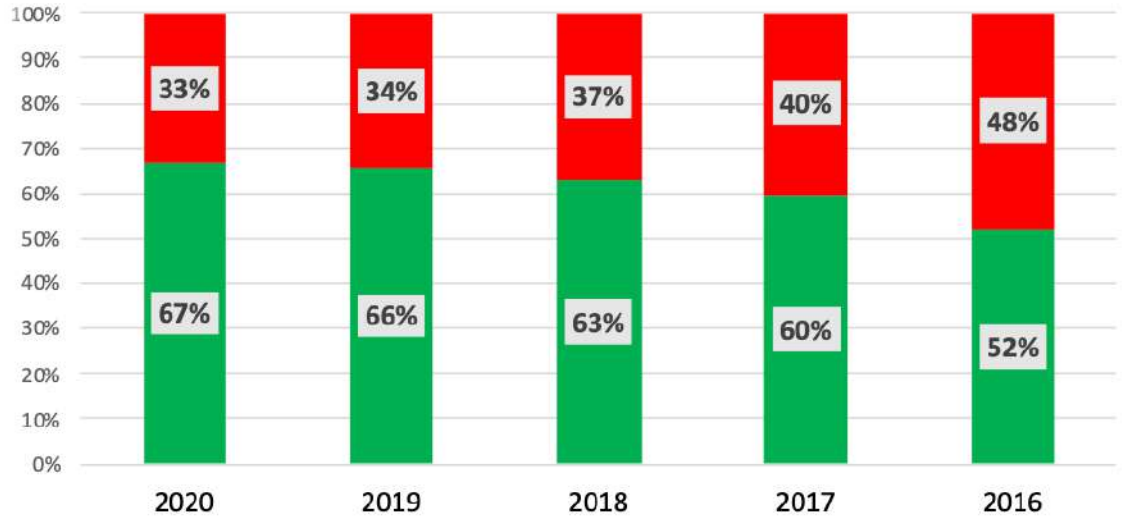

*Figuur 1 -Verschijningsvormen van IAF's in percentages 2016-2020*

Wij stellen vast dat het aantal Nederlandse beursgenoteerde vennootschappen dat een IAF heeft is toegenomen van 2016 tot en met 2020. In de Internal Audit Monitor 2017 constateerden wij al dat dit ook het geval was in de periode 2010 tot en met 2016. Eind 2016 beschikte 52% van de Nederlandse beursgenoteerde vennootschappen over een IAF. Per eind 2020 was dit percentage 67%. Terwijl (vrijwel) alle AEX- en AMX-fonsen een IAF hebben, ontbreekt deze nog vaak bij de AScX- en lokale fondsen.

We zien dat de stijging van het aan IAF's aan het afvlakken is in vergelijking met 2016 - 2017. Het lijkt erop dat de invoering van de herziene Nederlandse Corporate Governance Code in 2016, met veel aandacht voor internal audit, reden was voor de sterkte stijging.

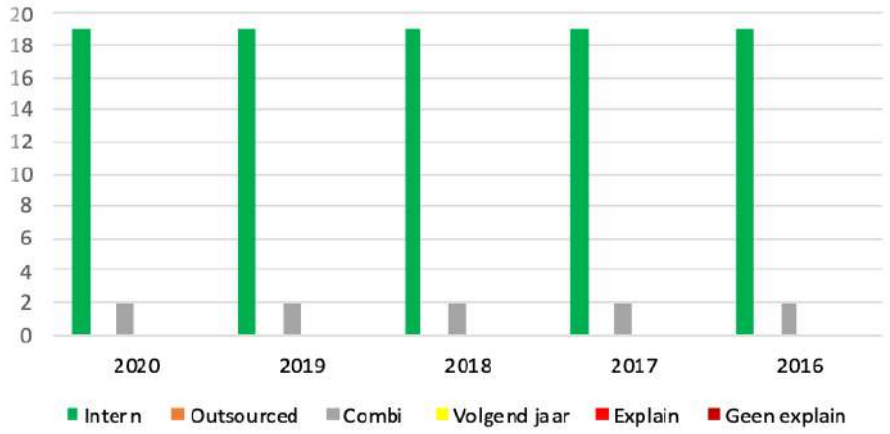



*Figuur 2 - Verschijningsvormen van internal audit functies in aantallen 2016-2020*




*Figuur 3 – Percentages internal audit functies 2016-2020*

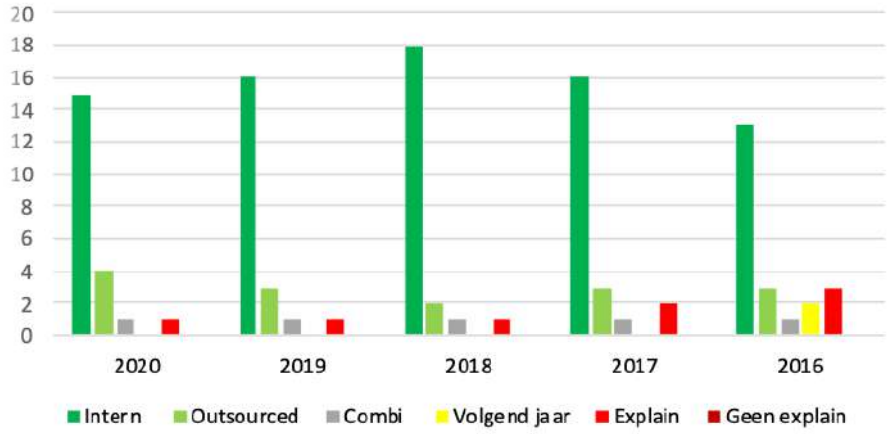
## AEX-FONDSEN




*Figuur 4 - Verschijningsvormen van AEX internal audit functies in aantallen 2016-2020*

- Alle Nederlandse AEX bedrijven hebben eind 2020 een IAF, net als in 2016. In twee gevallen is de betreffende functie tevens verantwoordelijk voor tweedelijnsactiviteiten rond (Enterprise) Risk Management. Het gaat om Randstad Holding en RELX.
- Prosus en Adyen waren in 2016 nog niet beursgenoteerd. Beide organisaties hebben eind 2020 een IAF.
- IMCD en Just Eat Takeaway waren in 2016 wel beursgenoteerd maar geen onderdeel van de AEX-index. In 2016 hadden beide organisaties geen IAF. Inmiddels wel.

## AMX-FONDSEN



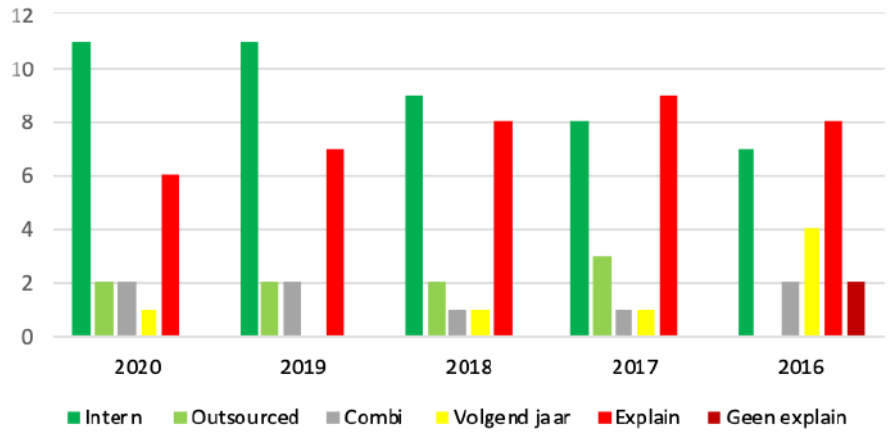

*Figuur 5 - Verschijningsvormen van AMX internal audit functies in aantallen 2016-2020*

- Van de Nederlandse AMX-bedrijven heeft 95% eind 2020 een IAF (2016: 77%). Vanaf 2018 blijft het aantal IAF stabiel (95%).
- Risicomanagement en Internal audit zijn een gecombineerde verantwoordelijkheid bij OCI N.V.
- Eén organisatie heeft eind 2020 geen IAF. Het gaat om Pharming Group. In hun jaarverslag geven zij als uitleg:

*"Due to the size of the company, Pharming has not created a specific position for an internal auditor, but it has provided for the assessment and testing of the risk management and control systems to be supported by the finance manager. As a result of the company operating in the highly regulated field of development and worldwide commercialization of human medicines, the company has a fully-staffed quality assurance department which is responsible, inter alia, for maintaining an extensive system of standard operating procedures throughout the company and for the execution of audits on all (major) suppliers, subcontractors, licensees and internal departments of the company including the finance department, although this is not the same as an internal auditor [...] the audit committee concluded that due to the controls in place and the size of the company, no internal auditor was needed at that point in time. The audit committee reconsiders this position at least annually. The fast rate of growth of the Company at present may cause a different determination at some point in the foreseeable future."*

- Eurocommercial Properties, GrandVision, Basic-Fit en NSI hebben hun IAF uitbesteed aan een externe dienstverlener.

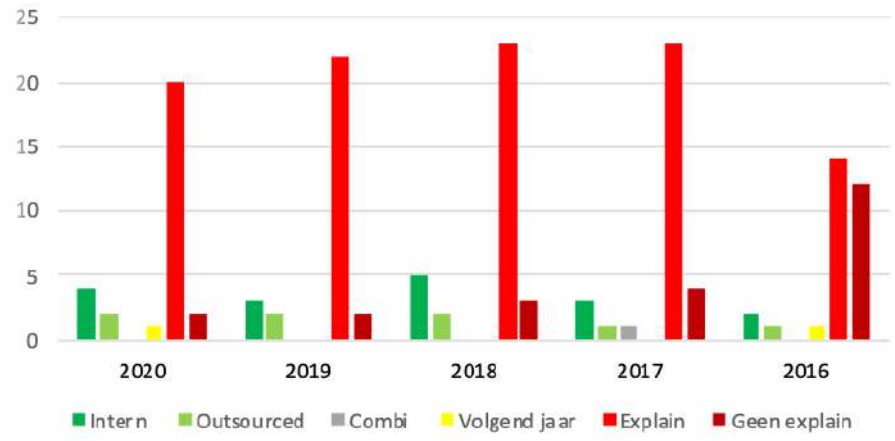
## ASCX-FONDSEN




*Figuur 6 - Verschijningsvormen van AScX internal audit functies in aantallen 2016-2020*

- Van de Nederlandse AScX-bedrijven heeft 68% eind 2020 een IAF; dat is een flinke stijging ten opzichte van 2016 (39%).
- Risicomanagement en internal audit zijn een gecombineerde verantwoordelijkheid bij Heijmans en Kendrion.
- Wereldhave en Vastned Retail hebben hun IAF uitbesteed aan een externe partij.
- Voor één van de zeven (was veertien eind 2016) bedrijven zonder IAF (Sligro) betreft dit een tijdelijke situatie. Aangegeven wordt dat in 2021 de IAF bij deze organisatie zal terugkeren. We zien dat dit ook is gebeurd.
- De meest genoemde reden bij SmallCap ondernemingen om geen IAF in te richten is de beperkte omvang van de onderneming.

### LOKALE FONDSEN




*Figuur7 - Verschijningsvormen van lokale internal audit functies in aantallen 2016-2020*

- Onder de lokale fondsen is het aantal IAF beperkt tot zes van de in totaal 29[6] (21%) bedrijven (was drie per eind 2016: 10%): Beter Bed, Core Laboratories, Euronext, Kardan, Neways Electronics en CM.com. Waarvan Beter Bed en Kardan hun IAF hebben uitbesteed aan een externe partij.
- Fastned geeft aan in 2021 "*een internal control en internal audit functie*" op te gaan zetten.
- In jaarverslagen van lokale vennootschappen wordt vaak niet of onvoldoende uitgelegd of en waarom een IAF ontbreekt. Men beperkt zich – evenals bij de AScX-fondsen - eenvoudig tot de vaststelling dat de omvang van de organisatie beperkt is.

## 3.2 Nieuwe en aankomende Internal Audit functies

### NIEUW

In 2020 zijn er drie nieuwe IAF's bijgekomen bij Nederlandse beursgenoteerde ondernemingen. Het gaat om:
- Eurocommercial Properties N.V.
- JDE Peet's
- CM.com

JDE Peet's en CM.com zijn nieuwkomers op Euronext Amsterdam, die reeds beschikten over een IAF. CM.com geeft aan de IAF in 2020 anders te hebben ingericht, onder meer met directe rapportagelijn aan de CEO en audit commissie, waarmee organisatorische onafhankelijkheid is geborgd. Bij beide organisaties is er in 2020 een (nieuw) Hoofd Internal Audit aangesteld.

6 Van de volgende drie vennootschappen was op het moment van het uitvoeren van het onderzoek nog geen jaarverslag 2020 beschikbaar: Esperite, New Sources Energy en Dutch Star Comp. 2. Genoemde organisaties hebben wij dan ook niet mee kunnen nemen in de statistieken.

Eurocommercial Properties N.V. heeft aangegeven hun IAF in 2020 te hebben uitbesteed. De Audit Commissie had de behoefte voor een IAF geëvalueerd en aan het bestuur geadviseerd om outsourcing te overwegen. In het jaarverslag wordt helaas niet ingegaan op de beweegredenen hiervoor. Een gemiste kans!

### VOORNEMENS

Ook hebben twee organisaties aangekondigd in 2021 een IAF te (her)introduceren binnen hun bedrijf:
- Sligro
- Fastned

Sligro had in 2019 een IAF. Deze is begin 2020 vacant komen te staan. Vanwege COVID heeft Sligro besloten een aantal vacatures niet direct in te vullen, waaronder de internal audit positie. Hierdoor zijn er in 2020 geen internal audits uitgevoerd. Het bedrijf geeft geen uitleg over hoe zij het tijdelijke 'gemis' van een internal audit functie hebben opgevangen. Ook hier is sprake van een gemiste kans.

De raad van Commissarissen van Fastned is van mening dat een afdeling internal audit, gezien de omvang en personele bezetting van Fastned tot nu toe, mogelijk niet proportioneel is geweest. Met de versnelde groei van de vennootschap is echter besloten om een IAF op te richten. Het bestuur van Fastned heeft daarop besloten om - gezien de uitbreidingsplannen voor de onderneming binnen Fastned - een internal control en IAF op te zetten. Het is vanuit het jaarverslag onduidelijk wat nu precies het omslagpunt is geweest voor de raad van commissarissen en bestuur van Fastned. Ook is onduidelijk of er nu een aparte internal control èn IAF gaat komen of een gecombineerde functie.

## 3.3 Ontwikkeling in kwaliteit van uitleg

In paragraaf 2.2 beschreven we de eisen aan een goede uitleg van het ontbreken van een IAF, en de status daarvan zoals bleek uit ons onderzoek in 2020. Wij stellen in dit onderzoek vast dat de kwaliteit van de uitleg sindsdien nauwelijks is verbeterd. Het merendeel van de Nederlandse beursgenoteerde vennootschappen beperkt zich nog steeds tot de uitleg dat vanwege 'de beperkte omvang' van de organisatie er geen reden is tot het inrichten van een internal audit functie. Onduidelijk is wat er bedoeld wordt met 'omvang'. Wordt omzet, aantal medewerkers of fte, aantal locaties, geografische spreiding of aantal klanten bedoeld?

Er zijn in 2020 zelfs twee organisaties die helemaal geen uitleg geven voor het ontbreken van een IAF:
- DGB Group N.V.
- TIE Kinetix N.V.

DGB Group geeft bij de bepalingen best practice bepaling 1.3.1 - 1.3.6 van de Code aan: *"Deze rol is tot 10 september verzorgd door de niet-uitvoerend bestuurders"*. Deze bijzondere verklaring roept vooral veel vragen op. Immers, de niet-uitvoerend bestuurders hebben vooral een toezichthoudende rol, die ook het toezicht op de governance, inclusief de IAF omvat.

TIE Kinetix doet het af met de verklaring:

> *"It is the opinion of the Supervisory Board that, at present, there is no need for an internal audit function in the Company".*

Er is dus geen inhoudelijke toelichting en het bedrijf heeft wellicht ook zelf geconcludeerd dat dat erg summier was. In het jaarverslag over 2021 staat een uitgebreidere verklaring en valt te lezen:

> *"It is the opinion of the Supervisory Board that, at present, there is no need for an internal audit function in the Company. Due to the company's limited size, the internal controls including the accounting and governance processes, are of limited complexity. As such, this allows for the Executive Board to closely monitor the internal control system and report to the Supervisory Board. The company stimulates its employees to identify areas for improvement in risk management and control systems. The employees are in direct contact with the executive board so that suggestions are assessed at the appropriate level and an improvement plan rolled out as appropriate. Furthermore, the absence of an internal audit function has not been identified as a principal risk that would require mitigation. In this respect, reference is made to the section Risk Management and Control, starting on page 43."*

# 4 De combinatie internal audit en risicomanagement

## 4.1 Achtergrond

Het combineren van de internal audit en de risicomanagement functie wordt vaak als onwenselijk gezien. Het doet immers afbreuk aan het gedegen 'three lines model', waarin risicomanagement een belangrijke tweedelijnsfunctie is en de IAF de onafhankelijke derde lijn. Een van de prominente vraagstukken daarbij is dan ook hoe het dan zit met de onafhankelijkheid en objectiviteit als lijnen worden samengevoegd. In sommige sectoren, zoals de onder toezicht vallende financiële instellingen, is dan ook sprake van wet- en regelgeving die een aparte functie voor risicobeheer vereist. Uit resultaten van uitgevoerde kwaliteitstoetsingen van IAF's blijkt dat dat in andere sectoren niet het geval is en daar lijkt er minder dan vroeger een taboe op de combinatie te rusten.

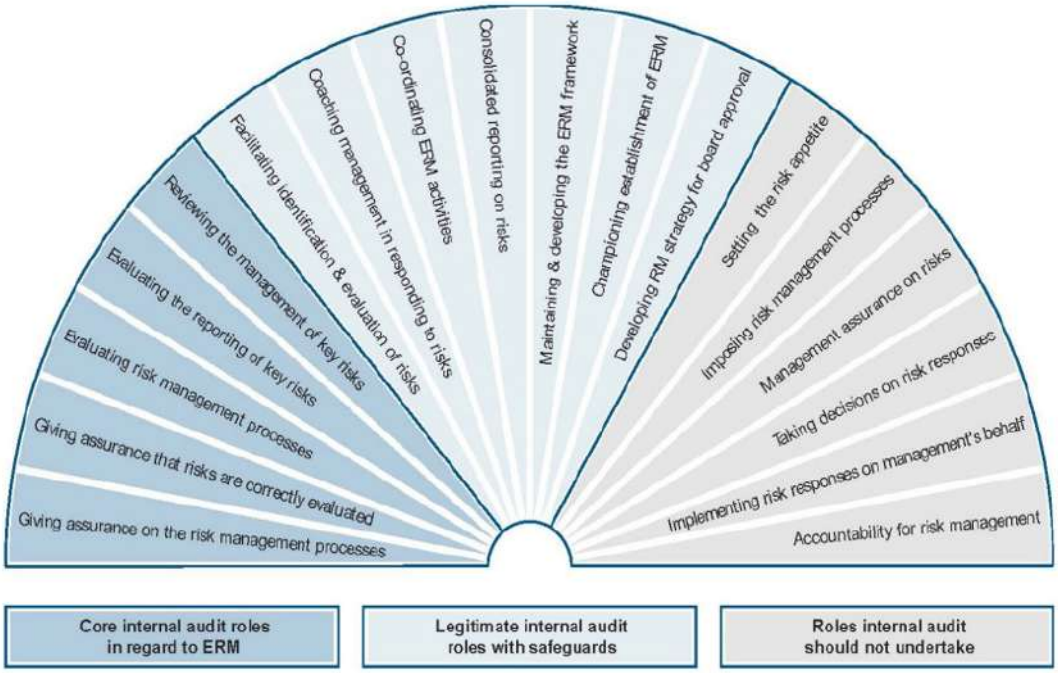
## 4.2 Gecombineerde functies in jaarverslagen

De volgende Nederlandse beursgenoteerde vennootschappen geven (in publiekelijk beschikbare informatie) aan dat risicomanagement en internal audit activiteiten zijn samengevoegd onder één verantwoordelijke persoon:

- Randstad (AEX)
- RELX (AEX)
- OCI N.V. (AMX)
- Heijmans N.V. (AScX)
- Kendrion N.V. (AscX)

In alle gevallen wordt, conform het three lines model, in de jaarverslagen benadrukt dat de verantwoordelijkheid voor goed risicomanagement in de business (de eerste lijn) ligt. Daarbij geeft men aan dat het bij de risicomanagement activiteiten van de IAF in deze gevallen om ondersteunende activiteiten gaat. Daarmee lijken de risicomanagement werkzaamheden die de IAF uitvoert binnen de kernfunctie van internal audit te liggen, of in ieder geval te zijn toegestaan volgens de waaier van mogelijke activiteiten die de IAF wel, niet danwel onder voorwaarden zou kunnen uitvoeren gegeven haar onafhankelijke rol in de governance van de organisatie (zie figuur 8)[7].

7 IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management, januari 2009




*Figuur 8 - Roles of Internal Auditing in Enterprise Risk Management* [8]

Uit jaarverslagen is echter niet altijd op te maken wat de risicomanagement activiteiten precies omhelzen, en wat het onderscheid is met eventueel andere tweedelijns risicomanagementfuncties. Ook is niet altijd duidelijk waarom men voor een gecombineerde functie heeft gekozen.

## VOORBEELDEN

**Randstad**: *"The Group-wide Business Risk & Audit function provides a platform for sharing good practices, and is a sounding board for emerging opportunities, risks, and possible internal control gaps. The function consists of a cross-disciplinary team with Business Risk & Audit staff from the operating companies. Where needed, experts are involved in audits. For additional reassurance, BDO has been engaged to perform financial audits in multiple countries."*

**Heijmans**: *"Heijmans has an internal risk and audit manager, whose primary task is to initiate and conduct sufficient operationally focused audits, including clear feedback reporting to the management in question. In 2020, in addition to the norm audits and external audits, the risk and audit manager oversaw around 100 risk audits. The key findings of these audits were shared with the Group Board and the Supervisory Board's Audit committee on a quarterly basis. Any suggested improvements as a result of these audits are recorded in improvement registers. These registers are used to monitor the follow-up on the improvement measures. In 2020, we once again tightened the improvement process and the monitoring of the follow-up on improvement measures."*

**Kendrion**: *"Kendrion's risk management function, headed by the Internal Audit and Risk Manager, provides guidance and support to the Executive Board. This includes driving risk awareness across the Kendrion organisation and leading reviews of operational processes and effectiveness of the risk management and control system. In 2020, the risk management function has increased its contribution to the organisation significantly by playing a particularly important role in redesigning the approach to risk management and by proactively supporting the identification, evaluation and mitigation of risks."*

8 IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management, januari 2019.

## 4.3 Combi functies in de praktijk

Afgaande op de informatie uit de jaarverslagen lijkt het combineren van risicomanagement en internal audit maar zelden (vijf keer) voor te komen. Dat beeld is strijdig met onze eigen waarneming in de praktijk. Tijdens het uitvoeren van externe quality assessments op IAF zien we dat het combineren van internal audit met andere risicomanagement- en controlefuncties, zoals Enterprise Risk Management en specifieke ISAE3402 of ISO controle teams vaker voorkomt. Ook laat de praktijk zien dat veel IAF's - in meer of mindere mate - risicomanagement activiteiten uitvoeren, zoals faciliterende en coördinerende taken op het gebied van risico assessment en workshops.

Het combineren van de rollen komt het meest voor in kleinere organisaties en in organisaties met onvolwassen tweedelijnsrollen, maar ook in organisaties die juist zeer volwassen zijn op het gebied van interne beheersing. Dit beeld wordt bevestigd door een onderzoek van IIA Global, waarin deze trend ook is te zien bij IAF's in Noord Amerika.[9]

Wij zien in de praktijk combi-functies waar derdelijns- (internal audit) en tweedelijns- (o.a. risicomanagement) activiteiten worden uitgevoerd onder de verantwoordelijkheid van één persoon, een 'hoofd internal audit en risicomanagement'. Deze combi-functies komen veelal in twee verschillende vormen voor:

- Internal audit en risicomanagement activiteiten worden door dezelfde personen uitgevoerd. Waarbij het bij risicomanagement activiteiten alleen om coördinerende en faciliterende taken gaat.
- Internal audit en risicomanagement activiteiten worden door verschillende personen, in subteams uitgevoerd. Waarbij veelal in geval van risicomanagement ook adviserende taken worden uitgevoerd.

In de financiële sector is, zoals gezegd, sprake van een ander beeld. Het combineren is daar door externe toezichthouders expliciet verboden voor onder toezicht vallende financiële instellingen.

## 4.4 Een genuanceerde visie op de combinatie

Van oudsher is het zoals gezegd niet gebruikelijk om internal audit en risicomanagement binnen een organisatie te combineren en wordt in de modellen van good governance, zoals het three lines model, aangegeven dat de derde lijn geheel onafhankelijk moet zijn van de andere lijnen. De vraag komt dan ook op of de combinatie van risicomanagement en internal audit mogelijk en wenselijk is. Het antwoord op deze vraag is genuanceerd.

Belangrijke observaties hierbij zijn de volgende:

- Allereerst is het goed om vast te stellen dat beide functies bestaan ten dienste van de raad van bestuur en de raad van commissarissen. Hun werk ligt in elkaars verlengde en draagt bij aan het 'in control' zijn en daarmee aan de continuïteit van de organisatie en het bereiken van haar doelen.

9 North American Pulse of Internal Audit 2022 | Benchmarks for Internal Audit Leaders (iia.nl), p. 38.

- Bestuurders nemen beslissingen over het (bij)sturen van organisaties mede op basis van informatie die beide functies verschaffen over onder meer risico's en risico mitigerende maatregelen. Dat kunnen ze alleen goed doen als deze informatie naadloos aansluit op het perspectief waarmee een bestuurder kijkt naar de organisatie. Het gaat dan ook om het bieden van inzichten in de interne beheersing van de organisatie.
- Bestuurders hebben steeds vaker behoefte aan een geïntegreerd rapport op het gebied van de interne beheersing van de organisatie, waarin de tweede- en derdelijns functies samen optrekken om een gedegen beeld te geven van de in control status van de organisatie.
- Dat vereist een eenheid van taal (en/of onderliggende methodologie) over risico's, temeer daar het bij risico's en interne beheersing vaak gaat om een lastig te communiceren onderwerp. Als risicomanagement en IAF's eigen kaders en begrippen hanteren in de communicatie maakt dat het lastiger voor bestuurders om goed te doorgronden of en hoe de organisatie in control is.
- Tegen die achtergrond is het ook logisch dat bestuurders hechten aan één aanspreekpunt voor internal audit en risicomanagement.
- Een combinatie van internal audit en risicomanagement kan met name voor wat kleinere organisaties ook de nodige efficiencyvoordelen bieden, doordat er sprake is van één hoofd en er minder afstemming nodig is om onnodig dubbel werk, overlapping of lacunes te voorkomen en te kunnen steunen op elkaars uitgevoerde werkzaamheden.
- Vanuit het vak is er geen taboe op dit punt. In het nieuwe three lines model van het IIA blijft het belangrijk om onderscheid te maken tussen de verschillende eerste- tweede- en derdelijns-rollen, maar dit hoeft niet te betekenen dat daarvoor een splitsing in verschillende functies of organisatieonderdelen nodig is. Belangrijk daarbij is aan te sluiten bij de behoeften en omstandigheden van de organisatie; 'fit for purpose'. In de meest recente publicatie over dit onderwerp[10] wordt expliciet aangegeven:

  > *"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".*

- Zowel het nieuwe three lines model alsook de IIA Standaarden staan het combineren van internal audit met risicomanagement toe, mits voldoende waarborgen worden getroffen. Het geven van onafhankelijke en objectieve assurance en adviezen bij activiteiten waarvoor internal audit momenteel of recentelijk verantwoordelijk is of was, is taboe. Daarbij wordt – als voorbeeld – verwezen naar verantwoordelijkheden op het gebied van risicomanagement. Als waarborg wordt geboden om hiervoor een onafhankelijke derde partij in te schakelen, mocht de wens hiertoe bij het bestuursorgaan ontstaan.

Alles overziend is duidelijk dat het combineren van de genoemde functies in bepaalde gevallen een goed alternatief kan zijn. Volgens het three lines model is het ideaalplaatje vanuit governance-perspectief nog steeds een inrichting met separate functies voor risicomanagement en internal audit. Maar er kunnen omstandigheden zijn die een samenvoeging van rollen meer passend maken voor de organisatie: gedurende een bepaalde ontwikkelperiode, of meer structureel, maar wel onder een aantal voorwaarden om de goede corporate governance, en dan met name de onafhankelijkheid van de derde lijn, te waarborgen. Ditbetreffen vooral voorwaarden omtrent het vermijden

10 Het three lines model van het IIA. Een update van de Three Lines of Defense, juli 2022, The Institute of Internal Auditors

van het nemen van verantwoordelijkheid voor beheersingsmaatregelen en “risk appetite”; ze zijn meer uitgebreid beschreven in de IIA-notitie Combining Internal Audit en Second Line of Defense Functions[11].

Concluderend: combinaties van internal audit en risicomanagement (1) zijn geen taboe vanuit principes voor onafhankelijkheid en (2) sluiten in sommige situaties uitstekend aan op de wensen van bestuurders voor goede en eenduidige inzichten in de interne beheersing van hun organisatie, maar (3) vereisen wel een aantal compenserende maatregelen om het geheel van governance-rollen te waarborgen.

11

Instituut van
Internal Auditors
Nederland

ONE
RISK ADVISORY