

Interne audit banken, verzekeraars en financieel dienstverleners: een marktverkenning

In het kort - Interne audit speelt een belangrijke rol in een beheerste en integere bedrijfsvoering. Uit ons onderzoek blijkt dat de volwassenheid van interne auditfuncties binnen de financiële sector verder toeneemt. Banken en verzekeraars beschikken over het algemeen over professioneel ingerichte auditfuncties die bijdragen aan de interne beheersing. Bij grote financieel dienstverleners zien wij verschillende vormen van onafhankelijke toetsing en assurance, met ruimte voor verdere professionalisering. De belangrijkste opgave is het verder versterken van onafhankelijke, deskundige en risicogerichte functies die bijdragen aan het beheersen van risico's voor consumenten en de markt.

1.1 Inleiding

De AFM maakt zich sterk voor eerlijke en transparante financiële markten. Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland. Effectieve interne beheersing bij (financiële) ondernemingen, waaronder een effectieve tone-at-the-top, compliancefuncties en auditfuncties, dragen bij aan deze missie. Interne audit vervult een cruciale rol in de beheersing van risico's van ondernemingen. Als derde lijn verschaft zij onafhankelijke en objectieve zekerheid over de mate waarin risico's worden beheerst, en of governance en controlesystemen effectief functioneren. Daarmee is interne audit binnen ondernemingen een belangrijke schakel voor het signaleren van risico's die raken aan het klantbelang en de integriteit van de markt.

In 2026 hebben wij onderzocht hoe interne audit zich in de praktijk verhoudt tot de AFM-toezichtprioriteiten. Dat hebben wij onderzocht bij banken, verzekeraars en financieel dienstverleners. In 2021 en 2022 hebben wij een vergelijkbaar onderzoek gedaan. Wij constateerden dat de auditfuncties, met name bij banken en verzekeraars, over het algemeen volwassen en professioneel waren ingericht. Tegelijkertijd was hun bijdrage aan thema's die voor de AFM relevant zijn, vaak te beperkt en niet structureel geborgd. Tijdens het huidige onderzoek meten wij de voortgang op de geconstateerde bevindingen uit de voorgaande onderzoeken.

In het eerste halfjaar van 2026 hebben wij ook, samen met De Nederlandsche Bank (DNB), onderzoek gedaan naar de effectiviteit van de interne auditfuncties bij Handelaren op Eigen Rekening (HERs). De resultaten van dit onderzoek zullen besproken worden met betrokken partijen, maar bieden duidelijke parallellen met de resultaten die wij zien bij financieel dienstverleners. Ook hebben wij in deze periode gerapporteerd over interne auditfuncties bij fondsbeheerders ([Aandachtspunten voor compliance- en interne auditfuncties bij beheerders](#)).

Ons onderzoek richt zich op wat interne audit daadwerkelijk doet en waar de focus ligt. De populatie binnen dit onderzoek betreft 5 grote financieel dienstverleners, 6 grote banken en 4 grote verzekeraars. De geselecteerde ondernemingen vertegenwoordigen een substantieel deel van de markt, waardoor wij relevante sectorbrede aanbevelingen kunnen doen. Het onderzoek bestond uit een analyse van auditjaarplannen en uitgevoerde audits over 2025, aangevuld met een gerichte uitvraag op drie kernverwachtingen van de AFM ten aanzien van (I) de bijdrage van de interne auditfunctie bij de naleving van gedragstypische wet- en regelgeving, (II) het toetsen van de organisatiecultuur en om de (III) (toekomstige) risico's voor schendingen van het klantbelang te signaleren. De inzichten uit de aangeleverde informatie hebben wij verder verdiept met sessies op locatie bij de ondernemingen.

Wij vinden het belangrijk om zicht te houden op de effectiviteit van de interne auditfuncties. Periodiek onderzoek heeft een dubbel doel. Het biedt inzicht in de werking van de functie én fungeert als prikkel voor ondernemingen om toezichtthema's, zoals gedrag en klantbelang centraal, explicieter te verankeren in hun auditpraktijk. Daarnaast leiden recente ontwikkelingen, zoals de invoering van DORA, tot aanvullende verwachtingen over de betrokkenheid van interne audit bij de beoordeling van digitale operationele weerbaarheid.

In dit rapport leest u twee sectorbeelden: een van banken en verzekeraars, en een van (grote) financieel dienstverleners. In elk sectorbeeld staan de constatering uit de respectievelijke sectoren. Om de sectoren verder op weg te helpen, geven we aanvullend goede praktijkvoorbeelden die we hebben gezien.

2. Sectorbeeld: onze bevindingen

2.1 Banken en verzekeraars

Banken en verzekeraars opereren al lange tijd binnen het Three Lines Model en kennen een duidelijke normstelling voor de inrichting van interne audit. Vanuit wet- en regelgeving (onder andere EBA Guidelines on Internal Governance under CRD) wordt verwacht dat ondernemingen beschikken over een effectieve interne auditfunctie die werkt volgens internationale standaarden, zoals die van het Institute of Internal Auditors (IIA).

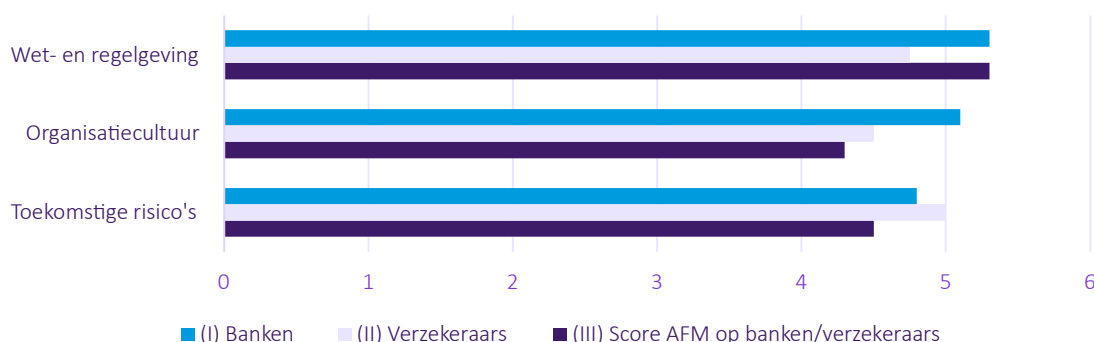
Deze normstelling vertaalt zich zichtbaar naar de praktijk. Interne auditfuncties kennen doorgaans een ingerichte kwaliteitscyclus met interne reviews, periodieke evaluaties en externe validaties. De basis is daarmee op orde en functies opereren over het algemeen op een hoog volwassenheidsniveau.

Die volwassenheid zit vooral in de inrichting en borging van het proces. Auditplanning, uitvoering en rapportage zijn gestructureerd en consistent, en interne auditfuncties zijn goed in staat om hun eigen kwaliteit te bewaken en door te ontwikkelen.

De belangrijkste ontwikkelopgave voor banken en verzekeraars ligt in het expliciet evalueren van de bijdrage van de interne auditfunctie aan organisatiecultuur en in het waarborgen van voldoende kennis en expertise ten aanzien van toekomstige risico's. Functies evalueren vaak op de generieke inrichting van de auditfunctie en de werking daarvan. Het is niet altijd inzichtelijk of de specifieke elementen ten aanzien van organisatiecultuur en de voorbereiding op toekomstige risico's, ook onderdeel zijn van de evaluaties.

In onderstaande figuur staan de gemiddelde volwassenheidsscores van (I) banken en (II) verzekeraars op de drie kernverwachtingen van de AFM. Daarbij is ook weergegeven wat wij, op basis van documentatie en interviews, hebben vastgesteld (III).

Figuur: Gemiddelde volwassenheid per verwachting banken/verzekeraars



Op basis van deze inzichten concluderen wij dat de volwassenheid van interne auditfuncties bij banken en verzekeraars aansluit op de verwachte volwassenheidsniveaus. In lijn met het volwassenheidsmodel scoren banken en verzekeraars gemiddeld ruim boven een 4 (op een schaal van 6) op alle verwachtingen. Dit betekent dat de ondernemingen een degelijke inrichting hebben en deze periodiek op effectiviteit monitoren. Tegelijkertijd ligt de volgende ontwikkelstap in het consistent en explicieter verankeren van toezichtprioriteiten binnen de auditpraktijk. Juist daar kan de functie nog meer impact maken op de verdere bijdrage aan het klantbelang.

2.2 (Grote) financieel dienstverleners

De markt van financieel dienstverleners is zeer divers in omvang, complexiteit en bedrijfsvoering. In dit onderzoek hebben wij ons daarom gericht op een beperkte groep grote financieel dienstverleners die horen tot de bovenkant van de Nederlandse markt. Anders dan banken en verzekeraars zijn financieel dienstverleners veelal niet wettelijk verplicht een onafhankelijke interne auditfunctie in te richten. De inrichting van governance, risicobeheersing en interne controle moet echter wel aansluiten op de aard, omvang en complexiteit van de onderneming. Voor grote financieel dienstverleners betekent dit een passend niveau van onafhankelijke toetsing en assurance, terwijl voor het merendeel van de sector centraal staat dat zij kunnen aantonen voldoende zicht te hebben op risico's, compliance en een beheerste en integere bedrijfsvoering.

Bij de grote financieel dienstverleners zien wij uiteenlopende vormen van onafhankelijke toetsing en assurance. In verschillende gevallen zijn functies als interne auditfunctie aangewezen, maar voldoen zij niet volledig aan de kenmerken die doorgaans worden geassocieerd met een onafhankelijke derde lijn, bijvoorbeeld ten aanzien van positionering, mandaat of onafhankelijkheid. Het ontbreken van een directe wettelijke verplichting tot het inrichten van een interne auditfunctie verklaart een deel van deze verschillen. Tegelijkertijd verwachten wij dat ondernemingen die ervoor kiezen een interne auditfunctie in te richten, deze op een wijze vormgeven die past bij de rol en verantwoordelijkheden van een onafhankelijke derde lijn.

Met name op het gebied van onafhankelijkheid, positionering en professionaliteit constateren wij belangrijke tekortkomingen. In verschillende gevallen worden werkzaamheden uitgevoerd door medewerkers die onvoldoende onafhankelijk zijn van de processen die zij beoordelen, ontbreekt een formeel auditmandaat of wordt slechts beperkt gewerkt volgens algemeen geaccepteerde auditstandaarden. Hoewel de uitgevoerde activiteiten vaak waardevolle inzichten opleveren voor de organisatie, kwalificeren deze functies daarmee niet als volwaardige interne auditfunctie.

Daar waar wel sprake is van een professioneel ingerichte auditfunctie zien wij een ander aandachtspunt. Deze functies voldoen doorgaans aan de basisvereisten van onafhankelijkheid en beschikken over voldoende auditmethodiek en vakbekwaamheid. Tegelijkertijd constateren wij dat het aantal uitgevoerde audits relatief beperkt is en dat onderwerpen die direct raken aan het klantbelang niet altijd voldoende prioriteit krijgen binnen de auditplanning.

De oorzaken hiervan lijken divers te zijn. In een aantal gevallen zien wij dat de omvang van de auditfunctie niet aansluit bij de omvang en complexiteit van de organisatie. Hierdoor moeten keuzes worden gemaakt in de dekking van het audituniversum. Daarnaast zien wij internationaal georganiseerde functies die hun capaciteit voornamelijk inzetten op groepsprioriteiten, waardoor Nederlandse toezichtprioriteiten minder aandacht krijgen. Tot slot constateren wij dat kennis en ervaring op specifieke toezichtrelevante thema's, zoals klantbelang, productgovernance en gedrag, niet altijd in voldoende mate aanwezig zijn binnen de auditfunctie. Daarbij zien wij ook dat kleinere auditfuncties niet altijd beschikken over dezelfde schaalvoordelen als grotere functies, bijvoorbeeld bij kwaliteitsborging, kennisontwikkeling en specialisatie.

Het gevolg is dat belangrijke risico's voor consumenten niet altijd zichtbaar terugkomen in de auditpraktijk. Hoewel onderwerpen zoals operationele risico's, IT en governance veelvuldig worden geaudit, zien wij minder expliciete aandacht voor de vraag in hoeverre producten, processen en besluitvorming daadwerkelijk bijdragen aan goede klantuitkomsten. Daarmee blijft een belangrijk deel van het potentieel van de interne auditfunctie onbenut.

De wijze waarop grote financieel dienstverleners onafhankelijke toetsing en assurance hebben ingericht, loopt sterk uiteen. De AFM ziet ruimte voor verdere professionalisering van deze functies, met name op het gebied van onafhankelijkheid, deskundigheid en risicogerichte prioritering. Daarbij geldt dat

de inrichting passend moet zijn bij de aard, omvang en complexiteit van de onderneming en moet bijdragen aan een beheerste bedrijfsvoering, naleving van wet- en regelgeving en het klantbelang.

3. Goede praktijkvoorbeelden

3.1 Aansluiting op IIA-standaarden en inrichting van de functie

Sterke interne auditfuncties kenmerken zich door een duidelijke aansluiting op internationale standaarden. In de praktijk zien wij functies die werken conform de IIA Global Internal Audit Standards (GIAS) en gebruikmaken van topical standards voor specifieke risicogebieden. Deze functies hebben hun audituniversum, risk assessment en planning goed gestructureerd en zorgen voor een consistente uitvoering en kwaliteitsmonitoring.

Daarbij valt op dat deze functies beschikken over voldoende capaciteit en duidelijke governance. Veelal zien wij een bezetting die aansluit bij een verhouding van circa 1 auditor op 150 medewerkers, onder aansturing van een onafhankelijke chieft audit executive (CAE). Deze CAE vervult een centrale rol in het borgen van kwaliteit en het monitoren van effectiviteit over de gehele auditcyclus. Aanvullend is de CAE juist gepositioneerd om (in)formeel op de hoogte te zijn van belangrijke ontwikkelingen in de onderneming. Juist deze combinatie van standaarden, capaciteit en duidelijke verantwoordelijkheden maakt dat de functie stabiel presteert en zich gericht kan doorontwikkelen.

Internationale of groepsgestuurde auditfuncties besteden expliciet aandacht aan Nederlandse risico's en toezichtthema's. Hoewel deze functies vaak werken met centrale standaarden, methodieken en specialistische expertise, zorgen zij ervoor dat lokale risico's, relevante wet- en regelgeving en klantbelangthema's zichtbaar worden meegenomen in de risicoanalyse, auditplanning en uitvoering van audits.

3.2 Expliciete continue verbetering

Interne auditfuncties die het hoogst scoren in de benchmark van dit onderzoek zijn zich expliciet bewust van de verbeterpunten die worden nagestreefd. Deze functies kijken niet alleen naar de organisatie waarop zij toezicht houden, maar ook naar zichzelf. Er worden jaarlijkse SWOT-analyses gemaakt, strategische personeelsanalyses uitgevoerd, strategiesessies gehouden en/of vergelijkingen gemaakt met andere functies. De geïdentificeerde acties uit deze inzichten worden vervolgens vertaald naar het jaarplan en er wordt effectief gemonitord op de voortgang van deze acties. Op deze manier waarborgen deze functies expliciet de continue verbetering van de functie.

3.3 Specifieke analyse vanuit het klantbelang

Vooruitstrevende functies maken expliciet ruimte voor een analyse vanuit het klantbelangperspectief. In plaats van dit thema impliciet mee te nemen in de risico-identificatie of auditplanning, wordt het onderwerp apart geanalyseerd, bijvoorbeeld via werkgroepen binnen de auditfunctie. Daarmee wordt structureel gekeken naar risico's rond klantbelang/zorgplicht en de wijze waarop deze risico's zich ontwikkelen.

Deze analyse leidt tot scherpere keuzes in de auditpraktijk. Functies stellen expliciet de vraag of zij voldoende doen op dit domein, of het onderwerp zichtbaar terugkomt in de audituniversum en of de geplande dekking aansluit bij de risico's. Ook wordt vooruitgekeken naar nieuwe of opkomende risico's. Dit helpt om het klantbelang niet alleen retrospectief te toetsen, maar ook onderdeel te maken van de auditplanning.

3.4 Inzet van AI en data-analyse

Binnen interne audit is een duidelijke beweging zichtbaar richting het gebruik van AI en data-analyse.

Steeds meer functies maken gebruik van geavanceerde analysetools om risico's te identificeren, afwijkingen te signaleren en audits efficiënter in te richten. Dit draagt zichtbaar bij aan de slagkracht en diepgang van de functie.

Tegelijkertijd blijft het borgen van auditkwaliteit leidend. Het gebruik van technologie vraagt om blijvende aandacht voor traditionele auditprincipes zoals integriteit, volledigheid en juistheid van informatie. Ook moet de onafhankelijkheid van de derde lijn gewaarborgd blijven. Effectieve functies weten deze balans te vinden: zij benutten technologie waar dit waarde toevoegt, zonder concessies te doen aan de betrouwbaarheid en/of verwatering van hun assurance-functie. Zie hiervoor ook onze publicatie [12 bouwstenen voor veiliger inzet geavanceerde \(GenAI\)-audittools](#).

Een effectieve manier om meer datagedreven te werken, is het goed beheersen en monitoren van de eigen auditprocessen.

Steeds meer functies hebben via sterke dashboarding inzicht in de eigen performance en de status van de diverse audits die uitgevoerd worden. Ook zien we dat er functies zijn die op een effectieve manier eigen inzichten en risicobeelden van de eerste/tweede lijn combineren en gebruiken als basis voor de jaarlijkse risicoanalyse. Hierbij valt op dat het niet altijd de meest complexe/AI-gedreven analyses zijn die de meeste waarde opleveren.

3.5 Gedragselementen in de audit

We zien dat steeds meer functies een sterke basis hebben staan om gedragsspecifieke elementen in de audits mee te nemen.

Effectieve functies combineren inzichten op gedrag vanuit root-cause analyses, specifieke gedragsaudits en andere indicatoren tot een periodiek overkoepelend inzicht voor de primaire stakeholders. Functies die verder zijn dan de rest maken de inzichten expliciet inzichtelijk voor het bestuur en weten hier ook acties aan te koppelen. Op 15 december 2026 zal de *IIA Topical Requirement Organizational Behavior* effectief worden. Wij verwachten dat deze leidraad richting zal geven in audits op het gebied van gedrag.

3.6 Doorvertaling naar klantwaarde

Effectieve interne auditfuncties maken expliciet de koppeling tussen hun werkzaamheden en de waarde voor de eindklant.

Dit vraagt om een positionering dicht op de bedrijfsvoering en in verbinding met het bestuur. Audits worden niet alleen uitgevoerd vanuit proces- of complianceperspectief, maar ook beoordeeld op hun relevantie voor het klantbelang. In de praktijk zien wij dat deze functies hun werk expliciet vertalen naar impact voor de consument. Zij stellen bij audits de vraag waarom een bepaald onderwerp ertoe doet voor de eindklant en hoe bevindingen bijdragen aan betere uitkomsten voor consumenten. Deze benadering helpt om prioriteiten scherper te stellen en vergroot de zichtbaarheid en relevantie van de auditfunctie binnen de organisatie.

3.7 Periodiek oordeel over de interne beheersing

Een aantal functies gaat verder dan het rapporteren over individuele bevindingen en geeft periodiek een integraal oordeel over de interne beheersing.

Dit gebeurt bijvoorbeeld op kwartaalbasis, waarbij Interne Audit een duidelijke uitspraak doet over de effectiviteit van de beheersing als geheel.

Dit zien wij als een waardevolle ontwikkeling. Waar veel functies rapporteren over openstaande issues en opvolging, ontbreekt regelmatig een overkoepelend oordeel. Juist dit integrale perspectief biedt bestuur en toezichthouders beter inzicht in de staat van de organisatie. Het dwingt de auditfunctie

bovendien om bevindingen in samenhang te beoordelen en expliciet te wegen wat deze betekenen voor de effectiviteit van de complete interne beheersing.