TOEZICHT RAPPORT

12 bouwstenen voor beheerst gebruik van audit-tooling

In het kort Geavanceerde audit-tools – waaronder (Gen)AI – bieden accountantsorganisaties volop kansen: efficiëntere processen, een hogere kwaliteit van controlewerkzaamheden en aantrekkelijker werk. De AFM moedigt innovatie aan, mits verantwoord en beheerst. Enkele grotere accountantsorganisaties lopen voorop in het voeren van beleid voor tooling in de wettelijke controle. Bij andere is het fundament wankeler. Overal is ruimte voor verbetering. De AFM biedt daarom 12 bouwstenen om te evalueren wat al goed gaat en waar versterking nodig is. De onderste drie lagen van de toren moeten eerst goed op orde zijn, vóór inzet van innovatieve technologie zoals (Gen)AI. Check het fundament, versterk waar nodig en bouw verder aan kwaliteit en vertrouwen.

(Gen)AI-tooling 4
De (Gen)AI-tool wordt beheerst toegepast.

Bouwstenen:
- (Gen)AI-tools worden veilig en beheerst ingezet.
- De uitkomsten uit de (Gen)AI-tool zijn verifieerbaar of reproduceerbaar.
- De externe accountant is eindverantwoordelijk voor de uitkomsten uit de (Gen)AI-tool.

Zorg voor een stevig fundament

Audit-tooling 3
De audit-tool wordt beheerst geïmplementeerd.

Bouwstenen:
- Ontwikkel kennis en vaardigheden mee met innovatie.
- Integreer de toepassing van de audit-tooling in de controlestrategie en het controleplan.
- Volg de uitkomsten van audit-tooling op de juiste manier op.

Input-data 2
De input-data zijn relevant en betrouwbaar voor het verkrijgen van voldoende en geschikte controle-informatie.

Bouwstenen:
- Voer de juiste IT-werkzaamheden uit die toezien op de betrouwbaarheid en bruikbaarheid van de input-data.
- Stel vast dat relevante en betrouwbare input-data worden gebruikt om voldoende en geschikte controle-informatie te verkrijgen.
- Zorg voor een consistent ETL-proces en leg dit vast.

Risicomanagement 1
De accountantsorganisatie heeft haar risicomanagement en -beheersing op orde.
Dit is de basis.

Bouwstenen:
- Gebruik een passend raamwerk voor informatiebeveiliging.
- Formaliseer beleid rondom audit-tooling.
- Monitor het effect van audit-tooling op de kwaliteit van de wettelijke controle.

DECEMBER 2025

AFM

TOEZICHT RAPPORT

Inhoud

AFM

Inleiding

Technologische ontwikkelingen en digitalisering veranderen in hoog tempo de manier waarop accountantsorganisaties hun werkzaamheden uitvoeren, wat het belang van beheerst gebruik van audit-tooling versterkt. Deze ontwikkelingen bieden kansen, zoals verhoogde efficiëntie en kwaliteit van het controlewerk en aantrekkelijker werk.[1] Tegelijkertijd brengen ze risico's met zich mee: een gebrekkige beheersing van de technologie of de onjuiste toepassing kan de kwaliteit van wettelijke controles ondermijnen en kan leiden tot operationele kwetsbaarheden.[2, 3]

Wij signaleren verschillende 'aanjagers' achter de inzet van nieuwe audit-tooling en de vergrote aandacht voor informatiebeveiliging bij accountantsorganisaties. Voorbeelden hiervan zijn de beschikbaarheid van nieuwe technologieën, inspanningen om personeelstekorten op te vangen en druk vanuit private-equity-partijen die sturen op efficiëntie. Deze trends maken audit-tooling steeds meer een integraal onderdeel van de controlepraktijk. Tegelijkertijd nemen risico's op het gebied van informatiebeveiliging toe. Dit komt deels door het toenemende risico op cybercriminaliteit: accountantsorganisaties verwerken vertrouwelijke data en zijn daardoor aantrekkelijke doelwitten. Daarnaast zorgt nieuwe wet- en regelgeving – zoals de Digital Operational Resilience Act (DORA), de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) en de Network and Information Security Directive 2 (NIS2) – voor meer aandacht ten aanzien van digitale weerbaarheid.

We juichen innovatie binnen de sector toe en benadrukken de noodzaak van beheerst gebruik van nieuwe technologie. Accountantsorganisaties beschikken over grote hoeveelheden data van partijen die zij controleren. Het is cruciaal dat deze data veilig worden verwerkt, overgedragen en opgeslagen, en dat de data die als input voor audit-tools dienen relevant en betrouwbaar zijn om voldoende en geschikte controle-informatie te verkrijgen ter onderbouwing van het oordeel van de externe accountant. Daarnaast moeten audit-tools betrouwbare en transparante analyses uitvoeren om de kwaliteit van de wettelijke controles te waarborgen. Dit is essentieel voor het vertrouwen in de accountancysector.

Daarom hebben hebben wij een verkennend onderzoek uitgevoerd naar de inzet en reikwijdte van audit-tooling in wettelijke controles en de impact hiervan op de kwaliteit van deze controles. Dit betreft audit-tooling in de breedste zin van het woord: van dossiersoftware tot data-analysetools[4] en (Gen)AI[5], in alle fasen van het controleproces. Een overzicht van tools die we bij onze verkenning zijn tegengekomen is gepresenteerd op blz. 30 van dit rapport. Het onderzoek is uitgevoerd bij elf accountantsorganisaties met een reguliere vergunning[6] ("RV-accountantsorganisaties") en bij twee accountantsorganisaties met een vergunning voor wettelijke controles bij organisaties van openbaar belang ("OOB-accountantsorganisaties"). Tijdens de onderzoeken ter plaatse hebben wij onderdelen van het stelsel van kwaliteitsbeheersing beoordeeld die toezien op de inzet en implementatie van audit-tools. Ook hebben wij de inzet en reikwijdte van audit-tools bij twee wettelijke controles verkend om inzicht te krijgen in de invloed op de controlekwaliteit. Daarnaast hebben wij verdiepende gesprekken gehad met diverse stakeholders, waaronder leveranciers van acht

1 Committee of European Auditing Oversight Bodies ("CEAOB") - Challenges and applications of advanced technologies in audit firms (gepubliceerd in oktober 2024)

2 AFM – Trendzicht 2026 (gepubliceerd in november 2025)

3 International Forum of Independent Audit Regulators ("IFIAR") - Use of technology in audits – observations, risks and further evolution (gepubliceerd in maart 2025)

4 Conform NBA Handreiking 1141 gebruiken we de volgende definitie voor data-analyse: "Data-analyse is het ontdekken van patronen, afwijkingen, inconsistenties, en het onttrekken van nadere nuttige informatie over het object van het onderzoek door middel van analyse, modellering en visualisatie met het oog op de planning of het uitvoeren van de opdracht".

5 Met (Gen)AI wordt een 'AI-model voor algemene doeleinden' bedoeld als gedefinieerd in Artikel 3 definitie 63 van de Verordening (EU) 2024/1689 van het Europees Parlement en De Raad.

6 Deze accountantsorganisaties zijn geselecteerd vanuit de data die door de RV-accountantsorganisaties aan de AFM zijn aangeleverd over 2024. Deze data zijn weergegeven in figuur 4.3 op pagina 43 van Trendzicht 2026.

verschillende audit-tools en verschillende branche- en beroeps-organisaties. Tot slot hebben wij, naast de reeds voorhanden zijnde data voor RV-accountantsorganisaties, een data-uitvraag gedaan bij de zes OOB-accountantsorganisaties om de organisatie-brede inzet van audit-tooling bij deze populatie in kaart te brengen.

Er valt nog veel te winnen op het gebied van governance en beheersing van audit-tools binnen de sector. Hoewel enkele grotere accountantsorganisaties voorop lijken te lopen voor wat betreft het informatiebeveiligingsbeleid en tool-specifiek beleid op organisatie-niveau, beschikt het merendeel van de organisaties over minder geformaliseerde kaders. Ons onderzoek laat onder andere zien dat meer structurele aandacht nodig is op het gebied van risicobeheersing en het correct toepassen van audit-tooling. Dit geldt in het bijzonder voor de groep accountantsorganisaties met beperkt beleid, maar ook bij organisaties die beleidskaders verder hebben ontwikkeld is nog ruimte voor verbetering.

Om de sector op weg te helpen, bevat ons rapport belangrijke randvoorwaarden voor de beheerste inzet van audit-tooling. De randvoorwaarden zijn gestructureerd in **12 bouwstenen**. Met deze bouwstenen kunnen accountantsorganisaties (verder) werken aan een robuust bouwwerk voor de beheerste implementatie van audit-tooling.

Wat verwacht de AFM?
Een bouwwerk dat niet vroeg of laat aan het wankelen slaat of zelfs omvalt, omdat één of meerdere randvoorwaarden tekort-schieten. De AFM moedigt accountantsorganisaties aan kritisch te beoordelen hoe zij audit-tooling inzetten, zodat deze op een beheerste manier wordt geïmplementeerd in de wettelijke controle.

Beantwoord voor uw organisatie minimaal de volgende drie vragen: *Welke bouwstenen* moet of kan de organisatie inzetten? Heeft de organisatie *alle bouwstenen* nodig voor een robuust bouwwerk? En: Zijn er mogelijk nog *andere bouwstenen* relevant naast de 12 die in dit rapport zijn opgenomen?

Het is aan accountantsorganisaties om deze vragen te beantwoorden, afhankelijk van factoren zoals de aard van de controle en de gebruikte audit-tooling. Organisaties moeten hierin weloverwogen keuzes maken en voldoen aan de toepasselijke wet- en regelgeving.

Onze oproep aan de sector: gebruik de bouwstenen in dit rapport om te evalueren wat al goed gaat en waar verbetering nodig is. Check het fundament, versterk waar nodig én blijf bouwen aan kwaliteit en vertrouwen.

Naar verwachting zal de AFM de komende jaren meer aandacht besteden aan de beheerste inzet van audit-tooling in verdere (toetsende) onderzoeken.[7]

7 AFM – Trendzicht 2026: Gezien de risico's die door de AFM geïdentificeerd zijn zal dit onderwerp de komende jaren verhoogde aandacht krijgen in (toetsende) onderzoeken. (gepubliceerd in november 2025)

12 Bouwstenen voor beheerst gebruik van audit-tooling – vanuit 4 randvoorwaarden

Randvoorwaarde 1: de accountantsorganisatie heeft haar risicomanagement en -beheersing op orde

Waarom deze randvoorwaarde? Goed risicomanagement en effectieve risicobeheersing zijn essentieel voor verantwoord gebruik van audit-tooling. Het bestuur van de accountantsorganisatie speelt hierin een cruciale rol. Het bestuur is verantwoordelijk voor het opzetten van een robuust raamwerk voor informatiebeveiliging en het ontwikkelen van beleid dat een beheerste toepassing van audit-tooling faciliteert. Daarnaast dient het zorg te dragen voor de effectieve uitrol van audit-tools[8], het tool-specifieke beleid, en de inrichting van monitoringsactiviteiten die de inzet en reikwijdte van audit-tools in de controlepraktijk meetbaar maken.

Wat ziet de AFM in de praktijk bij deze randvoorwaarde? Uit ons onderzoek blijkt dat risicomanagement en -beheersing rondom audit-tooling niet altijd adequaat zijn ingericht. We zien bij verschillende accountantsorganisaties tekortkomingen in het informatiebeveiligingsraamwerk en onvoldoende grip op derde partijen, waardoor cyberrisico's onvoldoende worden beheerst. Daarnaast is tool-specifiek beleid voor inzet en monitoring van audit-tools vaak niet geformaliseerd, wat risico's oplevert voor de uitvoering van de wettelijke controle. Bestuurders zijn zich niet altijd bewust van deze risico's.

Bouwsteen 1: gebruik een passend raamwerk voor informatiebeveiliging. Informatiebeveiliging is essentieel, zeker nu het controleproces steeds meer datagedreven wordt. Toch zien we dat veel accountantsorganisaties kwetsbaar zijn door ad-hoc-beleid, beperkte grip op derde partijen en onvoldoende bewustzijn van risico's bij beleidsbepalers. Een robuust risicomanagementraamwerk biedt houvast om informatiebeveiliging toekomstbestendig in te richten en de "hacker als wekker" te voorkomen.

Bouwsteen 2: formaliseer beleid rondom audit-tooling. Accountantsorganisaties maken steeds vaker gebruik van audit-tooling als onderdeel van hun controleaanpak. Toch ontbreekt bij veel organisaties geformaliseerd beleid over de inzet van audit-tooling. Hierdoor is de toepassing niet altijd effectief of doelmatig voor de controledoelstelling of de algehele controleaanpak. Door beleid te formaliseren krijgt het bestuur grip op de inzet van audit-tooling in de accountantsorganisatie.

Bouwsteen 3: monitor het effect van audit-tooling op de kwaliteit van de wettelijke controle. Audit-tools bieden vaak functionaliteiten voor gebruiksmonitoring waarmee de inzet en reikwijdte meetbaar worden. Door systematisch te monitoren krijgt het bestuur inzicht in het effect van audit-tooling op de wettelijke controle. Bijvoorbeeld door te beoordelen of de juiste functionaliteiten worden gebruikt voor controlewerkzaamheden, of dat men terugvalt op traditionele methodes. Zo kan tijdig worden bijgestuurd en gewenst gedrag worden gestimuleerd. De AFM ziet dat monitoringsfunctionaliteiten van audit-tools vaak niet worden gebruikt, waardoor onjuist gebruik, technische fouten of vaktechnische tekortkomingen onopgemerkt blijven.

8 Financial Reporting Council ("FRC") - Certification of Automated Tools and Techniques (gepubliceerd in juni 2025)

Randvoorwaarde 2: de input-data voor de tool zijn relevant en betrouwbaar voor het verkrijgen van voldoende en geschikte controle-informatie

Waarom deze randvoorwaarde? Audit-tools kunnen helpen bij het verzamelen, sorteren, filteren en analyseren van data van de controlecliënt. De input-data in audit-tooling moeten dan wel relevant en betrouwbaar zijn. De kwaliteit van de uitkomsten is direct afhankelijk van de relevantie en betrouwbaarheid van deze data. Daarom is het noodzakelijk dat de externe accountant de juiste werkzaamheden uitvoert om vast te stellen dat de input-data relevant en betrouwbaar zijn, waaronder de juistheid en volledigheid als dat nodig is voor de onderbouwing van het oordeel.

Wat ziet de AFM in de praktijk bij deze randvoorwaarde? Wij constateren dat externe accountants niet altijd de juiste werkzaamheden uitvoeren om de relevantie en betrouwbaarheid van input-data vast te stellen (waaronder de volledigheid en juistheid van niet-financiële data-elementen). Zo wordt er regelmatig onvoldoende aandacht besteed aan ineffectieve General IT Controls ("GITC's")[9] of de bronverificatie van de door de accountant verkregen data. We zien dat data uit systemen met ineffectieve interne beheersing worden gebruikt, zonder aanvullende waarborgen te treffen. Ook ontbreekt vaak een (in beleid opgenomen) gestandaardiseerd proces om zeker te stellen dat relevante en betrouwbare (volledige en juiste) data van de controlecliënt zijn ontvangen.

Bouwsteen 4: voer de juiste IT-werkzaamheden uit die toezien op de betrouwbaarheid en bruikbaarheid van de input-data. De externe accountant moet inzicht hebben in de invloed van GITC's van de controlecliënt op de betrouwbaarheid en bruikbaarheid van de data. Dit vereist van de externe accountant dat er voldoende diepgaande werkzaamheden worden uitgevoerd waarmee inzicht in de risico's op onbetrouwbare of onbruikbare data wordt verkregen. Ons onderzoek geeft indicaties dat accountants niet altijd voldoende aandacht geven aan GITC's en andere IT-gerelateerde risico's om de conclusie van de betrouwbaarheid en bruikbaarheid van de input-data te kunnen borgen.

Bouwsteen 5: stel vast dat relevante en betrouwbare input-data worden gebruikt om voldoende en geschikte controle-informatie te verkrijgen. Wanneer de externe accountant data van de controlecliënt ontvangt en deze gebruikt als input-data voor audit-tooling is het belangrijk dat de juiste werkzaamheden uitgevoerd worden om vast te stellen dat er relevante en betrouwbare data worden gebruikt om voldoende en geschikte controle-informatie te verkrijgen. In de praktijk zien we dat de externe accountant niet altijd de juiste waarborgen treft om er zeker van te zijn dat de relevantie en betrouwbaarheid van de ontvangen data zijn geborgd ten aanzien van de controledoelstelling. Bijvoorbeeld door de volledigheid en juistheid van de ontvangen data vast te stellen door deze op regelniveau aan te sluiten met onderliggende administratieve vastlegging, en waar relevant, met originele brondocumenten.

Bouwsteen 6: zorg voor een consistent ETL-proces en leg dit vast. Accountantsorganisaties moeten zorgen voor een consistent Extract-Transform-Load (ETL)-proces, bij voorkeur vastgesteld in beleid. De externe accountant dient het ETL-proces met voldoende detail vast te leggen in het controledossier. Een kwalitatief ETL-proces maakt werkzaamheden herleidbaar, ook bij inzet van specialisten of externe partijen. Een zorgvuldig ingericht ETL-proces in de organisatie draagt daarnaast bij aan de consistente evaluatie van de bruikbaarheid, betrouwbaarheid en relevantie van data die in de controle worden gebruikt, wat de controlekwaliteit positief kan beïnvloeden. In de praktijk zien we goede voorbeelden, maar ook ruimte voor verbetering.

9 NV COS 315.12d: Deze paragraaf geeft de definitie van GITC's die gehanteerd wordt in dit rapport.

Randvoorwaarde 3: de audit-tooling wordt beheerst geïmplementeerd

Waarom deze randvoorwaarde? Audit-tooling wordt geïmplementeerd als onderdeel van het controleproces, maar alleen bij juiste inzet draagt het bij aan de kwaliteit van de controle. Voor een beheerste toepassing is het belangrijk dat het opdrachtteam beschikt over de juiste kennis en vaardigheden, dat duidelijk is welk belang de audit-tool inneemt in het algehele controleplan en dat er op de juiste manier wordt omgegaan met de uitkomsten van audit-tooling.

Wat ziet de AFM in de praktijk bij deze randvoorwaarde? In de praktijk zien we dat audit-tooling niet altijd correct wordt toegepast. Een beheerste toepassing vereist dat de externe accountant begrijpt wat de functionaliteiten van de audit-tooling zijn, hoe deze ingezet worden voor een kwalitatieve controle én hoe de uitkomsten bijdragen aan het verkrijgen van voldoende en geschikte controle-informatie. Hierbij zien we dat soms voorbijgegaan wordt aan de controle-doelstelling, en de toepassing van de tool daarmee niet volledig aansluit op de doelstellingen uit het controleplan.

Bouwsteen 7: ontwikkel kennis en vaardigheden mee met innovatie. Accountantsorganisaties hebben vaak een breed scala aan audit-tools met uiteenlopende functionaliteiten. Toch wordt het volledige potentieel niet altijd benut. Dit kan komen doordat opdrachtteams niet op de hoogte zijn van alle mogelijkheden of niet beschikken over de juiste kennis om de tooling goed toe te passen. Wanneer het aan kennis of vaardigheden ontbreekt, kunnen accountantsorganisaties trainingsprogramma's organiseren en praktische handvatten bieden aan medewerkers, of andere vanuit andere specialismes zorgen dat de juiste kennis en competenties in huis worden gehaald.

Bouwsteen 8: integreer de toepassing van de audit-tooling in de controlestrategie en het controleplan. Audit-tooling vervult een ondersteunende rol in het controleproces; het is geen doel op zich. In de praktijk zien we dat audit-tooling niet altijd wordt ingezet op basis van de ingeschatte controlerisico's of het algehele controleplan, waardoor de uitkomsten (in sommige gevallen) minder sterk controlebewijs opleveren. Het is belangrijk dat audit-tooling wordt geïntegreerd in de controleaanpak, afgestemd op geïdentificeerde risico's en op de mate van controlebewijs die met de tooling kan worden verkregen.

Bouwsteen 9: volg de uitkomsten van audit-tooling op de juiste manier op. Audit-tooling wordt in wettelijke controles ingezet om controlebewijs of andere uitkomsten te genereren. We zien dat er ruimte voor verbetering is in de manier waarop met deze uitkomsten wordt omgegaan, bijvoorbeeld bij (potentieel significante) uitzonderingen en afwijkingen die kunnen leiden tot controle-verschillen of andere bevindingen. Het is belangrijk dat de gebruiker van een audit-tool op de juiste manier omgaat met de uitkomsten om de controlekwaliteit te borgen.

Randvoorwaarde 4: de (Gen)AI-tool wordt beheerst toegepast

Waarom deze randvoorwaarde? (Gen)AI brengt nieuwe, inherente risicofactoren met zich mee vanwege de aard en complexiteit van de technologie. De voorgaande 9 bouwstenen zijn vanzelfsprekend ook relevant voor het gebruik van (Gen)AI-tooling, maar een beheerste toepassing van (Gen)AI-tooling vraagt om 3 aanvullende bouwstenen.

Wat ziet de AFM in de praktijk bij deze randvoorwaarde? Bij (Gen)AI-tooling zien we vaker dan bij traditionele audit-tools een risico op **overreliance** door de vorm van de gepresenteerde uitkomsten. Uitkomsten van (Gen)AI-tools kunnen overtuigend overkomen door de antropomorfistische eigenschappen van sommige tools. Deze tools bootsen menselijke eigenschappen na, waardoor de gebruiker vaak sneller vertrouwt op de uitkomsten en deze minder kritisch beoordeeld. Dat de resultaten van (Gen)AI-tooling overtuigend kunnen lijken door de structuur en/of vorm, kan voor het 'halo-effect' zorgen. Daarnaast is het niet altijd transparant hoe uitkomsten tot stand

komen – dit vanwege de stochastische techniek waarmee uitkomsten gegenereerd worden. Daarom geeft de AFM **3 extra bouwstenen** ter ondersteuning van een beheerste inzet van (Gen)AI.

Bouwsteen 10: (Gen)AI-tools worden veilig en beheerst ingezet. Traditionele audit-tools zijn over het algemeen eenvoudiger te beheersen dan (Gen)AI-tools, omdat ze minder complex zijn qua ontwerp. Door de aard van (Gen)AI-tools is het lastiger om grip te houden op wat er met ingevoerde data gebeurt en om te waarborgen dat de tool blijft functioneren zoals de accountantsorganisatie heeft beoogd.

Bouwsteen 11: de uitkomsten uit de (Gen)AI-tool zijn verifieerbaar of reproduceerbaar. Bij traditionele audit-tooling is duidelijk welke stappen zijn genomen om tot een uitkomst te komen. Deze tooling is (veelal) gebaseerd op vaste (algoritmische) regels en logica. (Gen)AI-tools, bijvoorbeeld chatbots die zijn gebouwd op Large Language Models (LLM's), presenteren output op basis van statistiek en complexe algoritmes, waardoor de redenatie achter een uitkomst vaak niet transparant is. Daarom is het essentieel dat de uitkomsten van (Gen)AI-tools die gebruikt worden als controlebewijs, verifieerbaar of reproduceerbaar zijn. Dit stelt de externe accountant in staat aantoonbaar verantwoordelijkheid te nemen voor de uitkomsten.

Bouwsteen 12: de externe accountant is eindverantwoordelijk voor de uitkomsten uit de (Gen)AI-tool. Audit-tooling die gebruikmaakt van generatieve AI, kan uitkomsten genereren die lijken op conclusies van mensen. We zien het risico dat deze uitkomsten zonder kritische beoordeling worden overgenomen. Het is daarom essentieel dat de mens de uitkomsten van (Gen)AI zorgvuldig beoordeelt en zelf de relevante beslissingen nemen. De externe accountant moet de AI-output kritisch beoordelen en zelfstandig bepalen wanneer aanvullende menselijke verificatie noodzakelijk is.

Tone at the top essentieel bij alle bouwstenen

Bestuurders van accountantsorganisaties zijn verantwoordelijk voor een beheerste en integere bedrijfsvoering. Dit omvat de regels en procedures rondom audit-tooling die binnen de accountantsorganisatie gelden. De cultuur binnen de accountantsorganisatie is bepalend voor de mate waarin medewerkers deze regels en procedures naleven. Dat vraagt om bestuurders die risico's en ethische implicaties van digitalisering en innovatie begrijpen, doorleven én actief overbrengen aan medewerkers.

Voor effectieve innovatie is het daarnaast ook van belang dat bestuurders technologische kansen herkennen en ruimte creëren voor vernieuwing. Door strategisch richting te geven aan innovatie en medewerkers gecontroleerd te laten experimenteren met nieuwe technologieën, kan het bestuur duurzame en beheerste innovatie stimuleren.

We zien dat accountantsorganisaties onderscheid maken tussen 'running the business' en 'changing the business'. Specifieke verantwoordelijkheden worden toegewezen aan bepaalde medewerkers om innovatie in goede banen te leiden. De uitvoering van dagelijkse werkzaamheden staat hierbij los van de innovatiestrategie. Zo kan het bestuur de stabiliteit van de dagelijkse operatie waarborgen én tegelijkertijd ruimte creëren voor beheerste innovatie.

Het bestuur is verantwoordelijk voor het creëren van een cultuur die duurzame en beheerste innovatie ondersteunt. We hebben goede praktijkvoorbeelden gezien waarin het bestuur van de accountantsorganisatie ruimte biedt voor het bespreken van obstakels, fouten en morele dilemma's bij het gebruik van audit-tooling. Het bestuur gaat actief in gesprek met medewerkers en weegt signalen uit de praktijk mee bij de ontwikkeling van nieuw beleid en procedures voor beheerste innovatie. Dit draagt bij aan een lerende organisatie en een cultuur waarin medewerkers psychologische veiligheid ervaren om met innovatieve audit-tooling aan de slag te gaan.

Bestuurders beslissen over hoe wordt omgegaan met verhoogde efficiëntie door het gebruik van nieuwe technologie. Digitalisering kan leiden tot meer efficiëntie, waardoor tijd vrijkomt voor werkzaamheden die controlekwaliteit verhogen. Dit biedt ruimte voor meer professionele oordeelsvorming en vaktechnische diepgang —aspecten die ook het werkplezier kunnen vergroten. Tegelijkertijd kan dit vragen om aanvullende kennis en vaardigheden bij medewerkers om complexere en technisch uitdagende werkzaamheden uit te voeren. Het bestuur moet deze uitdagingen tijdig onderkennen en medewerkers voorbereiden door gerichte training, het stimuleren van continu leren en het monitoren van voortgang om de kwaliteit van wettelijke controles en professionele standaarden te waarborgen.

Toenemend gebruik van audit-tooling maakt een robuust raamwerk essentieel

Vanuit het uitgevoerde verkennende onderzoek dat tot dit rapport heeft geleid, signaleren wij de volgende drijfveren bij accountantsorganisaties voor de toenemende aandacht en inzet van innovatieve audit-tooling:

1. **Bijblijven met digitalisering van controlecliënten.** Controlecliënten verwerken steeds grotere hoeveelheden data en werken met steeds complexere IT-systemen. Accountantsorganisaties zetten audit-tooling in die datagedreven en systeemgerichte controlewerkzaamheden ondersteunt. Dit stelt hen in staat beter aan te sluiten bij de digitale bedrijfsvoering van hun cliënten.[10]

2. **Voldoen aan verwachtingen van controlecliënten over veiligheid en vertrouwelijkheid van dataverwerking.** Controlecliënten verwachten dat externe accountants hun data veilig, efficiënt en effectief gebruiken tijdens de wettelijke controle. Audit-tools kunnen niet alleen de efficiëntie en kwaliteit van controlewerkzaamheden verbeteren, maar ook diepere inzichten bieden in de bedrijfsvoering van cliënten—inzichten die soms ook met cliënten worden gedeeld.

3. **Benutten van opkomende technologieën.** Innovaties zoals machine learning en generatieve AI bieden functionaliteiten die de kwaliteit en efficiëntie van wettelijke controles kunnen verhogen. Wij zien dat accountantsorganisaties deze technologieën steeds vaker inzetten als kans om hun dienstverlening te verbeteren, met oog op efficiëntie en controlekwaliteit.[11]

4. **Omgaan met personeelstekorten.** Technologie maakt automatisering van repetitieve taken en efficiëntere controleprocessen mogelijk, waardoor tijd vrijkomt voor complexere en inhoudelijk interessante werkzaamheden. Dit vergroot de aantrekkelijkheid van het werk en kan zo bijdragen aan het behoud en de werving van nieuwe medewerkers.

5. **Uitfasering verouderde 'on-premise'-controlepaketten.** De uitfasering van veelgebruikte 'on-premise'-software voor audit-documentatie biedt accountantskantoren de kans om oplossingen te kiezen met geavanceerdere technologie en functionaliteiten, waaronder (Gen)AI en cloud-gebaseerde tools. Deze (noodzakelijke) migratie versnelt innovatie.

6. **Efficiëntie gedreven door private equity.** Private-equity-investeerders sturen vaak aan op efficiëntie via digitalisering om schaalvoordelen te realiseren en processen te stroomlijnen. Nieuwe audit-tooling kan bijdragen aan snelheid, inzicht en kostenbeheersing. Hoewel dit op de korte termijn voordelen biedt, ziet de AFM ook potentiële langetermijnrisico's.[12]

10 Burgerlijk Wetboek ("BW") - Artikel 393 lid 4 van Boek 2: Dit artikel bepaalt dat de accountant als onderdeel van zijn onderzoek van de jaarrekening verslag moet uitbrengen aan de raad van commissarissen en het bestuur. Dit verslag moet ten minste melding maken van de bevindingen van de accountant met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

11 AFM – Trendzicht 2026 p. 42: Een incidentele uitvraag in 2024 laat zien dat 49% van de RV-accountantsorganisaties innovatieve tooling toepast, waarbij de meeste organisaties meerdere typen tools combineren. OOB-accountantsorganisaties gebruiken audit-tools al langer, maar zetten die nu steeds vaker in voor risicoanalyses en andere niet-routinematige controlewerkzaamheden. Ook experimenteren zij steeds meer met nieuwe technologieën zoals (Gen)AI. (gepubliceerd in november 2025)

12 AFM - Private equity in accountancy: publiek belang onder druk (gepubliceerd in april 2025)

Wij zien daarnaast groeiende aandacht voor informatiebeveiliging binnen de sector:

1. **Toegenomen cyberrisico's**. Toenemende digitalisering vergroot de blootstelling aan cybercriminaliteit. Accountantsorganisaties zijn aantrekkelijke doelwitten vanwege de grote hoeveelheden vertrouwelijke data die zij verwerken in het kader van controle-opdrachten. Incidenten zoals datalekken en ransomware-aanvallen, kunnen aanzienlijke reputatie- en financiële schade veroorzaken, wat de noodzaak van structurele digitale weerbaarheid benadrukt.[13] Accountantsorganisaties moeten alert blijven, omdat de gevolgen van een incident groot kunnen zijn.[14]

2. **Ontwikkelingen in wet- en regelgeving.** Wetgeving zoals de Digital Operational Resilience Act (DORA), de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) en de Network and Information Security Directive 2 (NIS2) stelt strengere eisen aan digitale weerbaarheid. Hoewel accountantsorganisaties niet zozeer direct onder deze wetgeving vallen, moeten zij bij dienstverlening aan gereguleerde instellingen aantonen dat de eigen IT-processen veilig en robuust zijn. Deze ketenverplichting stimuleert versterking van informatiebeveiligingsmaatregelen, en daarmee de keuze voor veilige audit-tools.

13 Algemene Inlichtingen- en veiligheidsdienst ("AIVD") - Verdedigbaar Netwerk Hoe doe je dat? (gepubliceerd in augustus 2024)

14 AFM – Trendzicht 2026 p. 43. Accountantsorganisaties rapporteren weinig cyberincidenten en RV-accountantsorganisaties lijken hun eigen cyber-risico's te onderschatten. (gepubliceerd in november 2025)

1. Randvoorwaarde 1: de accountantsorganisatie heeft haar risicomanagement en -beheersing op orde

1.1 Bouwsteen 1: gebruik een passend raamwerk voor informatiebeveiliging

We zien dat dat het controleproces meer datagedreven wordt; daardoor groeien bepaalde risico's. Incidenten zoals datalekken, ransomware- en/of ketenaanvallen, ongeautoriseerde toegang of verlies van controle-informatie, kunnen direct impact hebben op vertrouwen, de betrouwbaarheid en de integriteit van de controlepraktijk. Accountantsorganisaties zijn kwetsbare partijen, omdat zij met grote hoeveelheden vertrouwelijke data werken en veelal (extern toegankelijke) interfaces hebben met derde partijen, waaronder ook controlecliënten.

Ons onderzoek resulteert in aandachtspunten ten aanzien van informatiebeveiliging voor bijna alle onderzochte accountantsorganisaties. Accountantsorganisaties regelen de informatiebeveiliging bijvoorbeeld organisch in, of hebben beperkt zicht op de kwetsbaarheden die voor hun organisatie relevant zijn omdat deze nooit formeel zijn geëvalueerd. Wat opvalt, is dat beleidsbepalers zich niet altijd bewust lijken te zijn van opkomende risico's, bijvoorbeeld ten aanzien van cyber-risico's wanneer quantumcomputers kunnen worden ingezet door cybercriminelen.[15] Ook zien we dat de cloud-strategie en het risico op digitale afhankelijkheid (van softwareleveranciers) vaak geen onderwerpen zijn die bij accountantsorganisaties structureel aandacht krijgen.[16, 17]

Informatiebeveiliging is ook nadrukkelijk van belang voor de derde partijen die data verwerken van de controlecliënt, zoals leveranciers van audit-tooling. Leveranciers zijn een belangrijke schakel in de sector. Dit komt omdat ze van meerdere accountantsorganisaties data opslaan en verwerken, veelal in een centrale Cloud-omgeving. Hierdoor kan één kwetsbaarheid in de IT-omgeving van de leverancier potentieel impact hebben op meerdere accountantsorganisaties. Het is aan het bestuur van de accountantsorganisatie om hier kritisch mee om te gaan en oog te hebben voor de risico's. Bijvoorbeeld door duidelijke afspraken te maken over veilige en betrouwbare dataverwerking, retentie, encryptie en deze periodiek te evalueren en waar nodig te herzien. Daarnaast kan het verstandig zijn om een jaarlijkse penetratietest ("pen-test"), ISO 27001- of SOC2-certificering of een 'right to audit' op te nemen in de contractvoorwaarden.

Een gestructureerd risicomanagement-raamwerk voor informatiebeveiliging geeft accountantsorganisaties handvatten om cyberrisico's te beheersen. Een risicomanagement-raamwerk voor informatiebeveiliging maakt risico's inzichtelijk, definieert rollen en een systematische aanpak van beheersmaatregelen, zoals periodieke pentesten en andere interne controles. Daarnaast geeft het ondersteuning wanneer een cyberrisico zich manifesteert. Door een goed georganiseerd raamwerk te implementeren, kunnen accountantsorganisaties ook aan de buitenwereld laten zien dat informatiebeveiliging voor hen de hoogste prioriteit krijgt en dat de juiste stappen genomen worden om risico's te mitigeren. Dit kan financiële en reputatieschade voor de accountantsorganisatie en in het verlengde de sector beperken.

15 AIVD – Bereid je voor op de dreiging van quantumcomputers (gepubliceerd in september 2021)

16 Prof. Moerel, L. et al. - Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default (gepubliceerd in februari 2024). Voor concrete cloud-beveiliging, simulatie en implementatie denk bijvoorbeeld voor Azure aan: Ignite'25 Spotlight: Announcing Microsoft Baseline security mode | Microsoft Community Hub

17 DNB - Digitale afhankelijkheid in de financiële sector (gepubliceerd in oktober 2025)

Een goed voorbeeld van een risicomanagement-raamwerk is de Good Practice Informatiebeveiliging van De Nederlandsche Bank ("DNB").[18] De beheersmaatregelen in dit raamwerk zijn proportioneel ten opzichte van de aard, omvang en complexiteit van accountantsorganisaties. De maatregelen gaan verder dan technologische oplossingen en omvatten ook menselijk gedrag, procesinrichting en benodigde faciliteiten.

Een robuust risicomanagementraamwerk voor informatiebeveiliging bevat preventieve, detecterende, corrigerende en repressieve beheersmaatregelen, zoals: netwerkbeveiliging, encryptie, logische toegangsbeveiliging, change-managementbeleid en beleid voor logging, monitoring en pentesten.

Daarnaast is het belangrijk dat het bestuur periodiek de informatiebeveiligingsvereisten bij derde partijen, zoals softwareleveranciers, toetst aan het eigen raamwerk om afstemming te waarborgen en risico's te mitigeren.

Good practice
Een accountantsorganisatie laat alle deelnemende en overgenomen kantoren gebruik maken van een uniforme technische infrastructuur en beheert deze centraal. Deze infrastructuur omvat onder andere goedgekeurde netwerkapparatuur en IT-assets, maar ook vastgesteld beleid en procedures voor de installatie van softwareoplossingen, waarmee consistentie in de gehele organisatie wordt gewaarborgd.

Toelichting
Een gestandaardiseerde, centraal beheerde infrastructuur vermindert complexiteit en fragmentatie, waardoor het aantal potentiële toegangspunten voor aanvallers wordt beperkt. Dit vergroot het inzicht en de controle, maakt consistente handhaving van beleid mogelijk en vereenvoudigt de respons bij incidenten. Voor accountantsorganisaties – waar teams vaak op afstand en bij meerdere cliënten werken – is dergelijke uniformiteit essentieel om verkeerde configuraties te voorkomen, het aanvalsoppervlak te verkleinen en het algehele risicomanagement voor informatiebeveiliging te versterken.

18 DNB - Good Practice Informatiebeveiliging 2023: Deze publicatie geeft instellingen handvatten om de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de (geautomatiseerde) gegevensverwerking te waarborgen. (gepubliceerd in december 2023)

Good practice
We zien al goede voorbeelden van accountants-organisaties die externe (volwassenheids) assessments of testen uitvoeren bij derde partijen die een risico vormen in de keten. In sommige gevallen betreft dit een gedetailleerde beoordeling van de ISO27001-certificering, SOC2- en/of ISAE3402-rapportages van de derde partij. Bepaalde accountants-organisaties beoordelen ook pentest-resultaten van deze partijen om potentiële kwetsbaarheden te identificeren en te waarborgen dat deze in lijn zijn met het interne informatiebeveiligingsbeleid, de overeengekomen service level agreements (SLA's) met deze partijen, en de vastgestelde risicobereidheid van de organisatie.

Toelichting
Het evalueren van derde partijen is een belangrijke manier om het informatiebeveiligingsbeleid van de accountantsorganisatie door de gehele keten toe te passen. Dit stelt het bestuur in staat om waar nodig corrigerende maatregelen te nemen en, indien vereist, diensten bij derde partijen aan te passen of te beëindigen om informatiebeveiliging in de keten te waarborgen.

1.2 Bouwsteen 2: formaliseer beleid rondom audit-tooling

Beleid voor de uitrol van nieuwe tooling beperkt de risico's rondom informatiebeveiliging en de werking. Dit start bij een risico-inschatting op verschillende expertisegebieden. Bijvoorbeeld vaktechnisch, cyber-security[19], IT, juridisch (inclusief data-privacy en independence) en learning & development. Is de kennis niet in huis, dan is het verstandig om externe expertise in te winnen voordat nieuwe tools worden geïmplementeerd.

Bij de inkoop en implementatie van nieuwe tooling is een gestructureerd en beheerst inkoopproces belangrijk. Inkoopcriteria, risicobeoordelingen en contractuele afspraken - zoals informatie-beveiliging, dataretentie- en minimalisatie en change management - bepalen waaraan de tool-leverancier wordt gehouden. Daarnaast is het aan bestuurders om het risico op digitale afhankelijkheid te beheersen (denk hierbij aan vendor-lock-in en datasoevereiniteit).[20]

Procedures voor het testen en valideren van intern ontwikkelde audit-tools beperken de risico's rondom informatiebeveiliging en de werking van de tools. Wanneer de accountantsorganisatie tools zelf ontwikkelt, gelden over het algemeen dezelfde risico's als bij ingekochte tools, maar ontstaan er ook nieuwe risico's die aanvullende maatregelen vereisen. Bijvoorbeeld rondom de vaktechnische en methodologische borging of de OTAP-straat ('Ontwikkeling, Test, Acceptatie en Productie'-straat).

Ook bij veranderingen en updates van tooling is er beleid nodig om de kwaliteit- en beveiligingsvereisten te waarborgen. Beleid dat bepaalt *hoe* veranderingen en updates van audit-tools bij de accountantsorganisatie worden doorgevoerd en getest. Daarbij speelt onder andere mee het type technologie waarop de audit-tool is gebouwd (bijvoorbeeld: on-premise of in de cloud) en hoe frequent er updates zijn. Bij significante veranderingen is het van belang dat het bestuur tijdig en adequaat de impact van deze veranderingen beoordeelt en hier opvolging aan geeft.

Centraal in tool-specifiek organisatiebeleid staat de methodologische inbedding in de controleaanpak, waarbij de audit-tool niet als losstaande activiteit, maar als een geïntegreerd onderdeel van de controlemethodologie wordt gezien. In beleid dient vastgelegd te worden in welke fase van de controle de tool kan worden ingezet, is beschreven welke richtlijnen of criteria relevant zijn bij de selectie van de tool, welke beweringen of concrete risico's de tool kan afdekken en onder welke voorwaarden de tool gebruikt kan worden voor een controledoelstelling (of niet). Waar de tool werkzaamheden die in de

19 CEAOB - Information security & Cybersecurity Inspection Work Program (gepubliceerd in november 2021)
20 DNB - Digitale afhankelijkheid in de financiële sector (gepubliceerd in oktober 2025)

controle worden uitgevoerd kan ondersteunen of voorbereiden, blijft de externe accountant eindverantwoordelijk voor de aansluiting van die werkzaamheden op de controlemethodologie.

Leg in het beleid ook de *methodologie* vast voor het gebruik van audit-tooling. Beschrijf bijvoorbeeld welke werkzaamheden de externe accountant in verschillende situaties kan of moet uitvoeren. Het is belangrijk dat het beleid beschrijft ***welke*** informatie met de audit-tool mag worden gebruikt; ***hoe*** deze informatie moet worden getoetst op bruikbaarheid, relevantie en betrouwbaarheid; en ***hoe*** de externe accountant bijzonderheden die voortkomen uit de controle-werkzaamheden moet interpreteren en opvolgen, ook wanneer deze samenhangen met andere controlewerkzaamheden.

Daarbij kan het beleid documentatievereisten voorschrijven om consistentie te waarborgen binnen de controledossiers van de accountantsorganisatie. Dit draagt bij aan de verifieerbaarheid en reproduceerbaarheid van de werkzaamheden. We zien in ons onderzoek al goede voorbeelden van standaardtemplates voor documentatie bij het gebruik van audit-tooling die in de gehele organisatie worden voorgeschreven.

In beleid kan worden vastgelegd wanneer en hoe specialisten – zoals data-analisten en IT-auditors – worden betrokken, wat hun verantwoordelijkheden zijn en hoe het werk van de specialisten past in het controleproces. De inzet van specialisten, zoals data-analisten en IT-auditors, is vaak noodzakelijk bij de toepassing van meer complexe audit-tooling of bij complexere IT-systemen van controlecliënten. Denk hierbij ook aan de relevante vereisten vanuit de controle-standaarden voor de inzet van een specialist als onderdeel van het opdrachtteam of als (externe) deskundige.[21]

Wanneer (Gen)AI-tools worden ingezet bij procedures in de wettelijke controle, verwachten wij dat de accountantsorganisatie specifiek beleid vaststelt om de implementatie van deze technologie te beheersen. Dit beleid ziet ten minste toe op drie onderwerpen.

1. Informatiebeveiliging: waarborgen voor de veilige verwerking van vertrouwelijke (klant)data en voor de correcte toepassing van de technologie.
2. Verifieerbaarheid of reproduceerbaarheid: de mogelijkheid om uitkomsten die als controle-informatie worden gebruikt, volledig te traceren of reproduceren.
3. Eindverantwoordelijkheid: de externe accountant blijft verantwoordelijk voor alle door de tool gegenereerde uitkomsten.

Daarnaast moeten relevante compliance vereisten, zoals die uit de AI Act, in het beleid worden opgenomen.[22]

Wanneer AI-agents een actieve rol hebben in de wettelijke controle, is aanvullend beleid voor het treffen van passende beheersmaatregelen essentieel.[23] AI-agents kunnen zelfstandig taken uitvoeren en toegang krijgen tot IT-systemen. Dit biedt kansen, maar brengt ook risico's voor accountantsorganisaties. Heldere governance en robuuste waarborgen zijn daarom van groot belang om verantwoord en veilig gebruik van deze technieken te kunnen garanderen.

Om te borgen dat audit-tools op de juiste wijze worden ingezet, is het verstandig om in beleid op te nemen hoe de toepassing van audit-tools systematisch wordt gemonitord en geëvalueerd. Dit omvat definities van de reikwijdte en frequentie van monitorings-activiteiten. Effectieve monitoring maakt het mogelijk om gewenst gebruik te bevorderen, terwijl ongewenst gebruik tijdig kan worden gedetecteerd en waar nodig, gecorrigeerd.

21 NV COS 220.12 of NV COS 620

22 Europese Unie ("EU") - Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence: De EU AI Act is een Europese verordening over het veilige en verantwoorde gebruik van kunstmatige intelligentie.

23 NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

Good practice
Uit ons onderzoek blijkt dat meerdere accountantsorganisaties geformaliseerd beleid en procedures hebben opgesteld voor de verwerving, ontwikkeling en uitrol van audit-tooling. In dit beleid en deze procedures is expliciet aandacht voor risicobeheersing, door de eerdergenoemde thema's te adresseren. Na de uitrol worden deze thema's opnieuw geëvalueerd, rekening houdend met de risico's, reikwijdte en inzet van de tooling.

Toelichting
Wij moedigen accountantsorganisaties aan om een gestructureerd proces in te richten voor zowel de implementatie als de periodieke review van audit-tooling, binnen een robuust kader voor risicobeheersing.

1.3 Bouwsteen 3: monitor het effect van audit-tooling op de kwaliteit van de wettelijke controle

Het monitoren van de impact van audit-tooling is een evaluatie onderdeel van de bestuurlijke informatievoorziening voor de accountantsorganisatie; de inzichten bieden handvatten voor strategische en operationele beslissingen. Hoe de accountantsorganisatie het effect van audit-tooling op de kwaliteit van de wettelijke controle meetbaar maakt, hangt af van de inzet en reikwijdte van de audit-tooling. Wij vinden het belangrijk dat het bestuur een monitoringsraamwerk vaststelt op basis van de kwaliteitsdoelstellingen en relevante risico's. Het bestuur kan hiervoor KPI's bepalen en monitoringswerkzaamheden inrichten. De verkregen inzichten kunnen vervolgens strategische en operationele keuzes ondersteunen.

Good practice
Een accountantsorganisatie gebruikt een dashboard om inzicht te krijgen in de inzet en reikwijdte van een audit-tool bij controlewerkzaamheden. Met dit dashboard kan de beleidsbepaler voor iedere toepassing van de audit-tool exact vaststellen welke uitzonderingen en afwijkingen uit analyses volgen en hoe de accountant deze heeft opgevolgd.

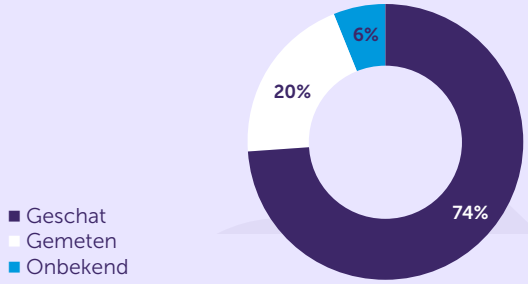
Toelichting
Door deze systematische monitoring krijgt het bestuur inzicht in het effect van de audit-tooling op de kwaliteit van de wettelijke controle en kan het bestuur tijdig bijsturen waar nodig. Daarnaast kan hiermee gewenst gedrag worden herkend en aangemoedigd binnen de organisatie.

Voor het monitoren kunnen verschillende bronnen en methodes worden toegepast. Bijvoorbeeld data uit audit-tools die automatisch gebruikspatronen en afwijkingen logt. Deze informatie kan helpen om trends en knelpunten te identificeren in het gebruik van deze audit-tools. Daarnaast kunnen periodieke dossierreviews door vaktechnische experts waardevolle input bieden. Deze reviews kunnen onjuist gebruik, inconsistenties of interpretatiefouten signaleren die anders onder de radar blijven. Ook is het gebruikersperspectief van belang. Gebruikersenquêtes en support-tickets voor vragen en incidentmeldingen zijn methodes om subjectieve ervaringen te verzamelen en risico's te identificeren. Opgehaalde resultaten kunnen inzicht geven in de ervaringen van professionals in de praktijk waarmee de kwaliteit en bruikbaarheid van de tools voor uitgevoerde controlewerkzaamheden duidelijker wordt. Wanneer functionaliteiten van audit-tools worden aangepast, kunnen A/B-testen een manier zijn om de veranderingen te toetsen aan verwachte uitkomsten.[24] Tot slot biedt het verzamelen van meta-data –bijvoorbeeld binnen welke dossiers en voor welke controleprocessen de tooling gebruikt is– een robuuste basis voor (risico-)gerichte analyses.

24 Een A/B-test (ook wel split test genoemd) is een methode waarmee twee versies van een audit-tool worden vergeleken om te zien welke beter presteert.

Monitoring – observaties uit het verkennend onderzoek
Tijdens ons onderzoek zien wij dat er (nog) niet altijd aandacht wordt besteed aan monitoring van audit-tool-gebruik en de invloed hiervan op de kwaliteit van de wettelijke controle. Vaak monitoren organisaties het gebruik achteraf met steekproefsgewijze interne kwaliteitsbeoordelingen of met vragenlijsten aan gebruikers. Accountantsorganisaties geven aan dat zij aan het beoordelen zijn hoe er betere managementinformatie verkregen kan worden door structurele monitoringsactiviteiten in te richten.

Methode van monitoring in % audit-tooling



Het beeld dat wij zien is mede gebaseerd op data die wij hebben verzameld. Vanuit de data zien wij dat gemiddeld genomen voor 74% van de audit-tools het gebruik op het niveau van de controleopdracht wordt geschat. Het gebruik van 20% van de audit-tools wordt daadwerkelijk gemeten (gedetailleerde gebruikersdata). Bij 6% van de audit-tools is het niet duidelijk hoe deze gebruikt worden omdat hiervoor geen informatie beschikbaar is. Onze observaties zijn in lijn met vergelijkbare publicaties.[25, 26]

25 FRC - Certification of Automated Tools and Techniques (gepubliceerd in juni 2025)

26 IFIAR - Use of technology in audits – observations, risks and further evolution: Dit betreft het rapport van de Technology Task Force ("TTF") van IFIAR over het gebruik van technologie in de audit. (gepubliceerd in maart 2025)

2. Randvoorwaarde 2: de input-data zijn relevant en betrouwbaar voor het verkrijgen van voldoende en geschikte controle-informatie

2.1 Bouwsteen 4: voer de juiste IT-werkzaamheden uit die toezien op de betrouwbaarheid en bruikbaarheid van de input-data

We zien dat externe accountants niet altijd voldoende werkzaamheden verrichten voor de beoordeling van GITC's in IT-systemen van controlecliënten voordat ze deze data gebruiken als input-data in een audit-tool.[27] Om een beeld te krijgen van de risico's die binnen (vaak) complexe IT-systemen van de controlecliënt zorgen voor de administratieve verwerking en/of de bron zijn van informatie die in de jaarrekening wordt gepresenteerd, moeten relevante GITC's binnen deze systemen worden beoordeeld. [28, 29, 30] Controlewerkzaamheden omvatten bijvoorbeeld de beoordeling van logische toegangsbeveiliging, rollen en rechten binnen de IT-systemen, change management, informatiebeveiligingsmaatregelen en onveranderlijke logregistratie.

De mate en diepgang van de werkzaamheden die de externe accountant uitvoert voor het toetsen van GITC's, zijn afhankelijk van verschillende factoren.[31] Als de IT-systemen van de controlecliënt complex zijn of de IT-afhankelijkheid van de administratieve organisatie hoog is, wordt het vanwege potentiële significante risico's nog belangrijker om GITC's te toetsen. Daarnaast neemt het belang om GITC's te toetsen toe bij het gebruik van audit-tools, omdat er binnen deze tools vaak grotere hoeveelheden informatie worden verwerkt als basis voor de evaluatie van (significante) controlerisico's of relevante beweringen voor de controle.

Als interne beheersingsrisico's worden vastgesteld, moet de externe accountant een inschatting maken van de mogelijke beperkingen op de betrouwbaarheid en bruikbaarheid van informatie als deze informatie het oordeel van de externe accountant ondersteunt. Wanneer er twijfel bestaat over de betrouwbaarheid of bruikbaarheid van relevante informatie, moet de accountant aanvullende werkzaamheden plannen.[32] De uitkomsten van GITC-evaluatie kunnen effect hebben op de geplande controlewerkzaamheden en de algehele controlestrategie wanneer deze leiden tot betrouwbaarheids- of bruikbaarheidsrisico's van relevante informatie. Bij effectieve GITC's in de IT-omgeving van de controlecliënt kan er gekozen worden voor een efficiëntere controleaanpak door systeemgerichte werkzaamheden uit te voeren. Zijn GITC's niet effectief, dan kan de externe accountant in sommige gevallen aanvullende gegevensgerichte werkzaamheden uitvoeren ter compensatie. Bijvoorbeeld met een 'can-do/did-do-analyse', om aan de hand van de rechten die aan gebruikers zijn toegekend te toetsen of deze gebruikers significante wijzigingen in systemen hebben aangebracht of handelingen hebben verricht die zouden leiden tot controlerisico's. Als hier geen bijzonderheden worden vastgesteld, kan er soms alsnog gesteund worden op de betrouwbaarheid en bruikbaarheid van gegevens, ondanks dat er ineffectieve GITC's zijn

27 NV COS 200.13b

28 Burgerlijk Wetboek ("BW") - Artikel 393 lid 4 van Boek 2

29 CEAOB - IT Audit Inspection Work Program (gepubliceerd in november 2020)

30 NV COS 315.25 en 315.26 in combinatie met Bijlage 5: overwegingen voor het verwerven van inzicht in informatietechnologie en Bijlage 6: overwegingen voor het verwerven van inzicht in de general IT controls

31 NV COS 200.13n

32 NV COS 315.27-28 en NV COS 500.7

vastgesteld.[33] Wanneer er wél significante tekortkomingen worden vastgesteld in de interne beheersing van de controlecliënt, dan moet de accountant een beoordeling maken van de invloed die de risico's hebben op relevante beweringen en gegevensgerichte controlewerkzaamheden. Hierbij is het van belang dat de accountant nagaat of er meer overtuigende controle-informatie nodig is om de geïdentificeerde (materiële) risico's op fouten of fraude in de financiële overzichten te mitigeren. Hierop past de accountant het controleplan aan. Als de externe accountant niet de benodigde expertise heeft voor de beoordeling van risico's binnen IT-systemen, zien we al goede voorbeelden waarbij de accountant een IT-auditor inschakelt.[34]

Bad practice
De externe accountant voert onvoldoende werkzaamheden uit voor de opvolging van de geïdentificeerde risico's en bevindingen van de IT-auditor. Wat ook hierbij ontbreekt, is de evaluatie van de bruikbaarheid en betrouwbaarheid van de input-data voor de audit-tool in relatie tot de risico's en bevindingen die de IT-auditor signaleert. De audit-tooling is gebruikt zonder deze afwegingen mee te nemen.

Toelichting
Bij twijfel over de bruikbaarheid en betrouwbaarheid van input-data voor audit-tools, bijvoorbeeld bij ineffectieve GITC's, moet de accountant werkzaamheden verrichten om deze twijfel weg te nemen. Dit moet gebeuren voordat de tool wordt gebruikt om controlebewijs te vergaren. Ook wanneer een externe accountant vaststelt dat een ERP-systeem veel gebruikersaccounts met verhoogde rechten bevat, moeten er werkzaamheden worden verricht om twijfel weg te nemen voordat de tool gebruikt kan worden om controlebewijs te vergaren. De externe accountant moet hierbij vaststellen welke wijzigingen deze gebruikersaccounts gemaakt hebben en welke gevolgen dit heeft voor het gebruik van de audit-tooling.

Good practice
Wij hebben gezien dat externe accountants tools gebruiken voor het inzichtelijk maken (en zo nodig evalueren) van rollen, rechten en gebruikers- en beheersingsactiviteiten binnen het IT-systeem van de controlecliënt. Dat leverde een integraal beeld op van de verwachte gebruikersactiviteit (bijvoorbeeld bij superuser-accounts of visualisatie van 'happy-flows') en van ongewenste activiteiten, wat inzicht gaf in de risico's op een afwijking van materieel belang binnen deze systemen. Dit complete risicobeeld bood kansen om verdere controlewerkzaamheden efficiënt in te richten.

Toelichting
Door gebruik te maken van tools die GITC's (en application controls) integraal analyseren binnen de IT-omgeving van de entiteit, kan de accountant een beter inzicht krijgen in de relevante risico's op een materiële afwijking die voortkomen uit deze IT-systemen. De integrale beoordeling van alle relevante IT-activiteiten kan daarmee een solide basis vormen voor de verdere controleaanpak en de planning van gegevensgerichte werkzaamheden.

Bij het toetsen van de betrouwbaarheid en bruikbaarheid van de input-data is het van belang dat deze data worden aangesloten op onderliggende administratieve vastlegging en waar nodig op brondocumenten.[35] De data-elementen die de externe accountant gebruikt voor het verkrijgen van controle-informatie, kunnen financieel en niet-financieel van aard zijn. Voorbeelden van niet-financiële data-elementen zijn: gebruikers, dagboeken, datums, tijdseenheden of andere niet-financiële variabelen die gebruikt worden om filteringen of analyses te ondersteunen. Deze data-elementen worden toegekend binnen IT-systemen op basis van bepaalde procedures bij de controlecliënt, en zijn vaak ook relevant voor de informatievoorziening richting het management of voor aspecten van de interne beheersing bij de organisatie. Deze informatie is veelal belangrijk voor systeemgegene-

33 NV COS 315 Bijlage 6: overwegingen voor het verwerven van inzicht in de general IT controls
34 NV COS 315.25 en 315.26 in combinatie met Bijlage 5: overwegingen voor het verwerven van inzicht in informatietechnologie en Bijlage 6: overwegingen voor het verwerven van inzicht in de general IT controls
35 NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

reerd lijstwerk wat door de controlecliënt wordt gebruikt. De externe accountant moet overwegen welke werkzaamheden passend zijn voor de validatie van de betrouwbaarheid en bruikbaarheid van deze informatie, bijvoorbeeld met gegevensgerichte werkzaamheden of door de effectiviteit van relevante 'application controls' en GITC's te toetsen. Om te bepalen welke systeemconfiguraties, 'application controls' en GITC's relevant zijn, moet de accountant overwegen welke informatie relevant is voor de audit-tool, eventueel in samenspraak met specialisten. De overwegingen voor, en evaluatie van, deze werkzaamheden moeten duidelijk worden opgenomen in het controledossier, zodat blijkt hoe de externe accountant heeft vastgesteld dat de data bruikbaar en betrouwbaar zijn voor verdere controlewerkzaamheden.

Good practice

We zien bij meerdere accountantsorganisaties dat er stroomschema's beschikbaar gesteld worden aan externe accountants om hen met een vast proces te helpen de juiste afwegingen te maken voor de evaluatie van de bruikbaarheid en betrouwbaarheid van informatie die door de entiteit is gegenereerd. Onderdeel van dat proces is de vraag om te reflecteren op de effectiviteit van de GITC's in IT-systemen van de controlecliënt. Ook worden er voorbeelden gegeven van mogelijke alternatieve werkzaamheden die risico's naar een aanvaardbaar laag niveau kunnen terugbrengen wanneer er tekortkomingen in de interne beheersing zijn geconstateerd.

Toelichting

De externe accountant kiest op een gesystematiseerde wijze passende werkzaamheden voor de validatie van de betrouwbaarheid en bruikbaarheid van informatie. Zo houdt de accountantsorganisatie grip op de relevantie en betrouwbaarheid van de uitkomsten uit audit-tooling die relevant zijn voor het oordeel van de externe accountant.

2.2 Bouwsteen 5: stel vast dat relevante en betrouwbare input-data worden gebruikt om voldoende en geschikte controle-informatie te verkrijgen

De externe accountant is verantwoordelijk voor de validatie van de input-data die een audit-tool verwerkt. Vaak is het mogelijk om een inschatting te maken van de inherente risico's die samenhangen met de informatie die de controlecliënt verstrekt.[36] De externe accountant kan van tevoren werkzaamheden bepalen ter validatie van de relevantie en betrouwbaarheid van informatie als deze wordt gebruikt voor het verkrijgen van controlebewijs. Als de externe accountant moeite heeft om deze evaluatie zelfstandig te verrichten, bijvoorbeeld bij complexe IT-systemen of -koppelingen, zijn er soms deskundigen nodig die werkzaamheden voor de externe accountant uitvoeren. Deze deskundigen kunnen bijvoorbeeld helpen bij het beoordelen van systeemarchitectuur, 'application controls', datastromen en koppelingen tussen verschillende IT-applicaties, om zo de volledigheid en juistheid van de data te waarborgen. Ook bij inzet van specialisten blijft het van belang dat de externe accountant begrijpt hoe de relevantie en betrouwbaarheid van de data gewaarborgd wordt. Hiervoor is het nodig dat de externe accountant de deskundige duidelijke instructies meegeeft. En dat de relevante vereisten vanuit de NV COS 620 in acht worden genomen. Deze gaan onder meer over de beoordeling van de onafhankelijkheid, vaardigheden en capaciteiten van de deskundige, maar ook over de evaluatie van de relevante beroepsregels of andere vereisten. Uiteindelijk blijft de externe accountant verantwoordelijk voor alle uitgevoerde werkzaamheden, ook wanneer deskundigen worden ingeschakeld.

36 NV COS 315 Bijlage 5: overwegingen voor het verwerven van inzicht in informatietechnologie

Good practice
Een accountantsorganisatie stelt in beleid dat een derde-partij-softwareleverancier die tijdens de wettelijke controle ondersteuning biedt bij data-analyse-werkzaamheden, geclassificeerd wordt als een ingeschakelde deskundige, in lijn met NV COS 620. Het beleid specificeert welke aspecten de externe accountant moet beoordelen en vastleggen in het controledossier. De externe accountant formuleert een opdracht, toetst de kennis, onafhankelijkheid en competenties van de deskundige én evalueert zichtbaar in het controledossier of de uitkomsten van de werkzaamheden van de deskundige adequaat zijn voor het behalen van de controledoelstelling.

Toelichting
Door in beleid te stellen dat de relevante waarborgen voor het inzetten van ingeschakelde deskundigen moeten worden geëvalueerd, kan de accountantsorganisatie de consistentie, onafhankelijkheid en kwaliteit van de inzet van die deskundigen in wettelijke controles bevorderen.

Het is aan de externe accountant om de extractiemethode te bepalen die voldoende zekerheid geeft over de relevantie en betrouwbaarheid van de data.[37] De externe accountant kan data op verschillende manieren verkrijgen - manieren die verschillende risico's met zich meebrengen. De kans op fouten bij de data-extractie kan door de externe accountant worden verkleind. Dat kan bijvoorbeeld door tijdens de extractie aanwezig te zijn of zelf de extractie uit te voeren via een interface of API-koppeling met de bronsystemen. Tijdens ons onderzoek hebben wij gezien dat externe accountants banktransacties rechtstreeks bij de bank van de controlecliënt extraheren met behulp van een API-koppeling of een audit-tool. Een Application Programming Interface (API) fungeert als een 'brug' of 'stekker' die standaardcommunicatie tussen verschillende soorten software mogelijk maakt. Met een API-koppeling kunnen automatisch gegevens kunnen worden uitgewisseld en gesynchroniseerd zonder handmatige tussenkomst van de externe accountant. Wanneer de externe accountant zelf beschikking heeft over de API-koppeling, en hiermee zelf data uit het systeem van de controleclient kan onttrekken, kan de externe accountant de parameters van de te onttrekken data vanuit de eigen wensen bepalen. Hierdoor blijft de externe accountant in control over de extractie van de juiste en volledige informatie die relevant is voor de controle. Neem hierbij wel de juiste maatregelen om informatiebeveiligingsrisico's naar een aanvaardbaar laag niveau te brengen, aangezien er bij API-koppeling andere cyber-risico's gelden dan bij traditionele systemen voor bestandsuitwisseling. Bijvoorbeeld door het inregelen van (minimaal) TLS 1.2 encryptie waarbij de verbinding uitsluitend via HTTPS tot stand kan komen.

37 NV COS 520.a12

Good practice
Meerdere accountantsorganisaties hebben beleid opgesteld voor het vaststellen van de betrouwbaarheid en bruikbaarheid van controle-informatie die wordt verkregen van de entiteit. Het beleid specificeert welke controlewerkzaamheden moeten worden uitgevoerd op basis van het type data en de bron van de data, in lijn met de controlestandaarden (NV COS 500.A35). In het beleid is ook opgenomen wanneer en hoe deze werkzaamhedenheden gedocumenteerd moeten worden in het controledossier.

Toelichting
De herkomst van de input-data die in een tool worden gebruikt kan van invloed zijn op de door de externe accountant uit te voeren werkzaamheden om de betrouwbaarheid en bruikbaarheid van deze data vast te stellen. Het opnemen van procedures hiervoor in beleid dat binnen de gehele organisatie wordt toegepast, helpt potentiële controle- en andere risico's te beheersen.

2.3 Bouwsteen 6: zorg voor een consistent ETL-proces en leg dit vast

Het 'Extract- Transform- and Load' proces ("ETL-proces") helpt de externe accountant om de betrouwbaarheid en bruikbaarheid van de verwerkte data te beheersen, en om de kwaliteit van verdere controlewerkzaamheden te waarborgen.[38] Het ETL-proces is het proces waarbij de externe accountant relevante input-data extraheert uit bronsystemen (Extract), deze transformeert naar een geschikt bestandsformaat en structuur (Transform), om het vervolgens in de audit-tool in te laden (Load). In dit proces kan de externe accountant bewust stilstaan bij data-minimalisatie - door alleen relevante input-data voor de tools op te halen en te verwerken. Bijvoorbeeld door rekening te houden met mogelijke exclusie van bijzondere persoonsgegevens. Bij het plannen van het ETL-proces kan de externe accountant al beoordelen in hoeverre de informatie relevant is om voldoende en geschikte controle-informatie te verkrijgen.

De externe accountant moet vaststellen dat de data afkomstig zijn uit de juiste bron (bijvoorbeeld de productieomgeving of het data-warehouse), dat de juiste query is gebruikt en dat de data juist en volledig zijn. Het extractieproces brengt specifieke risico's met zich mee voor de juistheid en volledigheid van gegevens, wat weer van invloed is op de relevantie en betrouwbaarheid bij het verkrijgen van voldoende en geschikte controle-informatie. Als onderdeel van ons onderzoek hebben we procedures gezien die auditors gebruiken bij data-extracties om betrouwbaarheid van de gegevens te waarborgen. Dit kan onder andere door aanwezig te zijn bij de extractie (fysiek of tijdens een online-meeting) en door verificatie van de query en parameters die voor de extractie zijn gebruikt, en door het aansluiten van de aangeleverde data op (financiële) overzichten of andere bron-documenten, zowel voor financiële als niet-financiële elementen. Denk hierbij aan de aansluiting van totaalbedragen uit verschillende kolommen, de vergelijking van het totaal aantal rijen in de database met die van de brondata, of door de aansluiting van controletotalen (hash-totalen) die door het systeem gegenereerd worden met het geprinte controletotaal op de data-extractie.

38 NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

De transformatiefase start zodra de data uit het geautomatiseerde informatiesysteem van de controlecliënt zijn geëxtraheerd. In deze fase worden de data klaargemaakt voor gebruik in een audit-tool. De externe accountant beoordeelt daarbij of de transformatietool (bijvoorbeeld een script) of de uitgevoerde werkzaamheden (bijvoorbeeld handmatige transformaties) de betrouwbaarheid van de data waarborgen. Bijvoorbeeld door te bepalen of de overdracht van de data juist en volledig heeft plaatsgevonden en door bepaalde data-kwaliteitscontroles uit te voeren. De transformatiefase kan werkzaamheden omvatten zoals het opschonen van data, het converteren van datatypes (bijvoorbeeld van *.XAF naar *.csv), het filteren en sorteren van data, berekeningen en andere transformaties die nodig zijn om de data in een bruikbaar formaat voor de audit-tool aan te leveren. De externe accountant moet voor de getransformeerde gegevens vaststellen dat het transformatieproces op de juiste wijze is opgezet. In het transformatieproces moeten relevante beheersingsmaatregelen zijn opgenomen die de betrouwbaarheid van de data waarborgen.

De externe accountant stelt vast dat de volledige dataset vanuit de transformatie-omgeving is geïmporteerd in de data-analyse tool voordat data-analyse plaatsvindt. Ook hierbij is het van belang dat de juistheid en volledigheid van de import-data gevalideerd is. Vervolgens kan de externe accountant algemene consistentiechecks uitvoeren, zoals*:

- Journaalposten die niet in balans zijn;
- Normalisatie van numerieke waarden en een aansluiting op andere administratieve vastleggingen (inclusief de juiste bepaling van decimalen in financiële data);
- Records met 'lege' velden (bijvoorbeeld een leeg datumveld, het ontbreken van de naam van de persoon die de boeking gemaakt heeft of journaalposten waarvan de waarde '0' is);
- Toetsen van controletotalen ('hashtotals') of andere meta-data. Dit om vast te stellen dat de informatie vanuit het transformatieproces volledig is ingeladen in de audit-tool.

*Deze lijst geeft veelvoorkomende procedures weer en is niet limitatief. Casusafhankelijk kunnen andere procedures relevant zijn.

Het documenteren van het ETL-proces is van belang om de traceerbaarheid en reproduceerbaarheid van het proces te waarborgen.[39] Sommige accountantsorganisaties geven aanzienlijke vrijheid aan hun opdrachtteams om de vastlegging in het controledossier zelf in te richten. Dit kan leiden tot inconsistenties en gebrekkige documentatie. De goede voorbeelden in dit onderzoek laten de volledige reis van de data zien - van de extractie tot aan het inladen van de data in de audit-tool. Bij deze goede voorbeelden documenteert de externe accountant alle relevante transformaties en configuraties die helpen de gebruikte informatie voor audit-tooling te verzorgen. De ETL-documentatie moet het spoor van controle-informatie (extractie, transformatie en laden) bevatten. Dit moet voldoende detail geven, zodat een ervaren accountant die niet eerder bij de controle betrokken was, onder andere in staat is om dezelfde conclusies te vormen met de gedocumenteerde informatie. Omdat bij het gebruik van audit-tooling vaak grote hoeveelheden data worden ingeladen en het ETL-proces daardoor in omvang en complexiteit toeneemt, is het essentieel dat de documentatie alle relevante kenmerken en configuraties bevat. Dit moet zodanig gedetailleerd zijn dat een ervaren accountant, die niet eerder bij de controle betrokken was, het proces volledig kan volgen en dezelfde conclusies kan trekken op basis van de vastgelegde informatie.

Good practice
Verschillende accountantsorganisaties stellen in beleid dat een gestandaardiseerd ETL-memo in het controledossier moet worden opgenomen bij het gebruik van data-analyse. Hierin wordt het ETL-proces volledig gedocumenteerd en zijn alle relevante afwegingen - waaronder data-validatie - traceerbaar en verifieerbaar.

Toelichting
Het vastleggen van het ETL-proces in een gestandaardiseerd template draagt bij aan consistentie tussen verschillende controleopdrachten. Het gebruik van uniforme formats en procedures — bijvoorbeeld voor veelvoorkomende ERP-systemen — verlaagt het risico op interpretatieverschillen en inconsistenties. Dit maakt de aanpak reproduceerbaar en controleerbaar, en faciliteert de review van het controledossier.

39 NV COS 230.8

3. Randvoorwaarde 3: de audit-tool wordt beheerst geïmplementeerd

3.1 Bouwsteen 7: ontwikkel kennis en vaardigheden mee met innovatie

Good practice
Verschillende accountantsorganisaties registreren wanneer een opdrachtteam een audit-tool voor de eerste keer inzet. Na de aanvraag krijgt het opdrachtteam begeleiding van een technisch specialist of een medewerker met meer kennis over de tool. Dit om de efficiënte en kwalitatieve toepassing van de tool te waarborgen.

Toelichting
Door de inzet van specialisten die met hun kennis en vaardigheden het opdrachtteam ondersteunen, wanneer een tool voor het eerst wordt gebruikt, kunnen tools effectiever en meer verantwoord worden ingezet in de controle. Hierdoor kan de kwaliteit van de tool-inzet wordt geborgd.

We zien dat audit-tooling bepaalde eenvoudige taken kan overnemen die eerder uitgevoerd werden door assistent-accountants.[40] **Dat geeft meer ruimte voor inhoudelijke werkzaamheden voor assistent-accountants.** Ruimte die kan worden ingezet voor complexere werkzaamheden waar oordeelsvorming voor nodig is, zoals bijvoorbeeld het uitzoeken van verdachte geldstromen. Ook is er meer ruimte om dilemma's door te spreken met het opdrachtteam en de controlecliënt. Hierdoor verandert het benodigde competentieprofiel van de assistent-accountant en wordt de leercurve voor hen steiler.

Om de kwalitatieve inzet van assistent-accountants te waarborgen, zal in de beginfase van hun carrière meer training nodig zijn. Dit is in het bijzonder relevant als deze assistent-accountants gaan werken met audit-tools die hen helpen met de voorbereiding van complexe werkzaamheden. Omdat audit-tools steeds vaker geïmplementeerd worden om eenvoudige en repetitieve controlewerkzaamheden voor te bereiden, moeten accountantsorganisaties voldoende kennis en middelen beschikbaar stellen om de beheerste toepassing van deze tools door assistent-accountants te borgen. Accountantsorganisaties moeten goed voorbereid zijn op veranderende verantwoordelijkheden van medewerkers als gevolg van de implementatie van audit-tools.

Good practice
Bij meerdere accountantsorganisaties is tijdens de planningsmeeting een ervaren toolgebruiker (tool-ambassadeur) of specialist aanwezig geweest. Deze ervaren toolgebruiker adviseert het opdrachtteam over de risico's en kansen die relevant zijn voor de effectieve inzet van audit-tools voor de controleopdracht.

Toelichting
Door een ervaren toolgebruiker mee te laten denken in de beginfase van de controle, krijgt deze de kans om nuances van de controlecliënt te begrijpen. Dat biedt niet alleen kansen voor een beheerste inzet van audit-tools; de ervaren toolgebruiker kan het opdrachtteam ook vernieuwende inzichten geven in de potentie van audit-tools, doordat het controleplan en specifieke risico's in deze fase worden besproken.

40 AFM – Trendzicht 2026 p. 42-43 (gepubliceerd in november 2025)

Beheerst gebruik van audit-tools vereist een combinatie van traditionele vaardigheden en nieuwe vaardigheden.[41] De traditionele vaardigheden zijn ook van belang bij de selectie van de juiste audit-tool voor specifieke controlewerkzaamheden. Echter, voor de correcte toepassing van audit-tooling is vaak specifieke kennis nodig. Niet alleen technische kennis is van belang voor de beheerste inzet, maar ook kennis van de wijze waarop het opdrachtteam moet omgaan met de uitkomsten van de tool. Dit geldt niet alleen voor de medewerker die de tool gebruikt, maar ook voor de beoordelaar van de controlewerkzaamheden waarvoor een audit-tool is ingezet. Accountantsorganisaties moeten waarborgen dat medewerkers de juiste vaardigheden bezitten om te beoordelen hoe met tool-uitkomsten voldoende en geschikte controle-informatie is verkregen.

Good practice

Verschillende accountantsorganisaties hebben voor veelgebruikte audit-tools videomateriaal beschikbaar gesteld. Daarin wordt de tool-functionaliteit stap-voor-stap toegelicht met praktische voorbeelden. Voor onervaren medewerkers wordt aanbevolen om een e-learning te volgen voordat ze de tool daadwerkelijk inzetten. In de e-learning leren medewerkers met videomateriaal op een interactieve manier de werking van relevante functionaliteiten van de tool kennen, en kunnen ze dit gemakkelijk toepassen bij de eigen controle-opdrachten.

Toelichting

Door medewerkers op te leiden voordat zij de audit-tooling gebruiken, zorgt de accountantsorganisatie voor beheerst en verantwoord gebruik in wettelijke controles. Tool-specifieke trainingen waarin relevante functionaliteiten worden uitgelegd, bevordert de juiste en consistente toepassing van de tool. Daarnaast kunnen demo-video's handig materiaal zijn voor gebruikers die twijfels hebben over bepaalde functionaliteiten van audit-tools. Visuele weergave kan hierbij praktische ondersteuning bieden tijdens de uitvoering van werkzaamheden.

Omdat externe accountants ongedeeld verantwoordelijk zijn, moeten ook zij de toepassing van audit-tooling snappen. Daarom is er in het geval van (zeer) complexe audit-tooling of bij specifieke controlewerkzaamheden meer kennis nodig vanuit andere expertisegebieden (statistiek, data-science, enzovoort). Als de accountantsorganisatie deze kennis niet in huis heeft, zien we al goede voorbeelden waarbij deze kennis (extern) wordt ingehuurd, of waarbij er medewerkers met een andere achtergrond dan de accountancy worden aangenomen.

We zien kennisdeling als een kritische succesfactor, waarbij ervaringen met het audit-tool-gebruik systematisch worden gedeeld en vervolgens worden geïntegreerd in de organisatie. Dit omvat zowel kennisdeling over technische aspecten, als de kennis over de impact van audit-tools op uitgevoerde wettelijke controles. We zien dat samenwerking binnen (een netwerk van) accountantsorganisaties kennisdeling kan bevorderen. Bijvoorbeeld het organisatiebreed delen van innovatieve toepassingen die van toegevoegde waarde zijn geweest bij controles in bepaalde klantsegmenten. Of het delen van specifieke ervaringen over de bijdrage van audit-tools bij het behalen van controledoelstellingen en de risico's die in dit proces zijn opgemerkt of opgelost. Ook zien we goede voorbeelden van het delen van de interpretatie en afwerking van resultaten uit audit-tools.

41 AFM - Sector in Beeld 2025 p. 13-14 (gepubliceerd in november 2025)

Good practice
Wij hebben gezien dat verschillende accountantsorganisaties netwerken opzetten van tool-specialisten: de meer ervaren gebruikers van audit-tools. Binnen deze netwerken wisselen de specialisten kennis uit en delen zij goede én minder goede ervaringen van audit-toolgebruik. Door deze uitwisseling kunnen zij praktische richtlijnen opstellen. Deze worden binnen de accountantsorganisatie met alle toolgebruikers gedeeld. De richtlijnen bieden een basis waarmee accountants audit-tools efficiënt en beheerst kunnen inzetten om de gewenste resultaten te behalen.

Toelichting
Een netwerk van ervaren toolgebruikers kan effectief zijn om kennis te delen over het gebruik van tools. Wanneer deze gebruikers werkzaam zijn op verschillende locaties of in diverse klantsegmenten, kan het specialistennetwerk kennisoverdracht in de gehele accountantsorganisatie stimuleren. Hierdoor beschikken medewerkers sneller over voldoende kennis om audit-tools effectief in te zetten.

3.2 Bouwsteen 8: integreer de toepassing van de audit-tooling in de controlestrategie en het controleplan

De wettelijke controle kent verschillende fases. Tijdens de planningsfase en de risico-inschattingsfase is het van belang om te bepalen hoe audit-tooling wordt ingezet. Op basis van de inherente en interne-controlerisico's bij de controlecliënt bepaalt de externe accountant welke controledoelstellingen relevant zijn. Vervolgens kiest de accountant een tool waarmee deze doelstellingen gerealiseerd kunnen worden. De geïdentificeerde risico's en de daarop aansluitende controledoelstellingen zijn leidend; audit-tooling is slechts een middel om deze doelstellingen te behalen. De voorwaarden voor het gebruik van audit-tooling bij risico-inschatting, kunnen verschillen van de voorwaarden voor het gebruik van audit-tooling bij het verkrijgen van controlebewijs. Wij zien al goede voorbeelden van accountantsorganisaties die in het controleplan opnemen welke tools worden gebruikt, voor welke procedures en in welke mate controlebewijs uit de tool wordt verkregen. Wanneer beleid voorschrijft welke voorwaarden de accountant moet beoordelen bij het gebruik van audit-tools, kan de accountant deze werkzaamheden al in de planningsfase meenemen. Dit voorkomt ad-hoc beslissingen tijdens de uitvoeringsfase van de controle, en draagt bij aan een efficiënte en beheerste toepassing van de audit-tool.

Good practice
Bij verschillende accountantsorganisaties hebben we gezien dat de externe accountant in het controleplan duidelijk vastlegt wat de relevantie is van audit-tools als deze worden ingezet voor de controle van materiële jaarrekeningposten. Het plan beschrijft welke invloed de (mogelijke) uitkomsten uit de audit-tool hebben ten opzichte van alle overige werkzaamheden die toezien op dezelfde controledoelstellingen. Voor uitzonderingen en afwijkingen verwijst de accountant naar het controleplan om de vooraf bepaalde invloed op overige controlewerkzaamheden te raadplegen, waarna de risico-inschatting voor deze werkzaamheden wordt aangepast.

Toelichting
Door in het controleplan vast te leggen wat de relevantie en invloed van audit-tools is bij de controle van materiële posten, kan de externe accountant deze informatie gebruiken om werkzaamheden goed op elkaar af te stemmen. Dit bevordert een consistente toepassing van audit-tools en maakt het mogelijk om bij uitzonderingen en afwijkingen snel en onderbouwd te bepalen welke aanvullende controlewerkzaamheden nodig zijn.

Het is verstandig om de juiste beheersmaatregelen te treffen wanneer de tools voor het eerst worden geïmplementeerd. Bij innovatieve tools is het vooraf niet altijd duidelijk of de inzet ervan zal leiden tot uitkomsten die voldoende en geschikte controle-informatie opleveren, zeker als de accountantsorganisatie de technieken nog niet eerder heeft toegepast voor bepaalde controlewerkzaamheden. We zien al goede voorbeelden van accountantsorganisaties die nieuwe tooling eerst uitproberen in een testomgeving, en hiervoor fictieve (maar representatieve) data gebruiken om een reële verwachting te verkrijgen over de potentie van de audit-tool voor bepaalde controlewerkzaamheden. Ook zien we voorbeelden van accountantsorganisaties die de inzet van audit-tooling synchroon laten lopen met de traditionele controlewerkzaamheden. Vervolgens wordt vergeleken welke invloed de audit-tool heeft op de efficiëntie en controlekwaliteit, voordat de tool breed wordt geïmplementeerd. Door éérst vast te stellen welke invloed audit-tools hebben op de kwaliteit van controlewerkzaamheden voordat ze breed binnen de organisatie worden uitgerold, kan de accountantsorganisatie kwalitatieve en beheerste inzet bij wettelijke controles bevorderen.

3.3 Bouwsteen 9: volg de uitkomsten van audit-tooling op de juiste manier op

Wanneer audit-tooling als uitkomsten risico-indicatoren, uitzonderingen en afwijkingen van de vooraf gestelde norm genereren, zal de externe accountant hieraan opvolging moeten geven. Duidelijke richtlijnen en voorbeelden vanuit beleid helpen tool-gebruikers om de juiste afwegingen te maken bij tooluitkomsten. Zo wordt geborgd dat signalen uit audit-tools niet alleen worden herkend, maar ook op een consistente en onderbouwde wijze leiden tot passende vervolgacties binnen de wettelijke controle. Vanuit ons onderzoek is ons beeld dat er ruimte voor verbetering is op dit onderwerp.

Bad practice

Bij meerdere accountantsorganisaties hebben we gezien dat de externe accountant een audit-tool gebruikt voor de rondrekening van de geld-goederenbeweging. De accountant heeft - voorafgaand aan de analyse - een controledoelstelling bepaald op het vaststellen van bestaan en afgrenzing van de omzet. Uit de analyse kwamen uitzonderingen en afwijkingen naar voren die, op basis van de vooraf opgestelde norm, verder onderzocht hadden moeten worden. De externe accountant heeft niet alle uitzonderingen en afwijkingen opgevolgd met verdere werkzaamheden en hierop niet zijn risico-inschatting opnieuw beoordeeld. Daarnaast heeft de externe accountant voor uitzonderingen en afwijkingen die wél opgevolgd zijn, geen feitelijke levering vastgesteld met externe brondocumenten (leveringsbewijzen).

Good practice

Een accountantsorganisatie heeft bij de wettelijke controle een audit-tool toegepast voor een gegevensgerichte cijferanalyse van kosten. Uit deze analyse kwamen uitzonderingen en afwijkingen naar voren. Het opdrachtteam heeft de relevante data-elementen aangesloten op externe bronnen ter onderbouwing en vervolgens geëvalueerd dat de vooraf gestelde verwachting voldoende nauwkeurig was om voldoende en geschikte controle-informatie te verkrijgen. De evaluatie is duidelijk in het controledossier opgenomen.

Toelichting

De accountant heeft een verwachting opgesteld en toetst de uitkomsten uit de tool aan deze vooraf gestelde normen. Bij afwijkingen van de vooraf gestelde verwachting of norm is het van belang dat de externe accountant relevante afwijkingen opvolgt door inzicht te verkrijgen in de aard en de omvang van deze afwijkingen, voordat de tool-uitkomsten worden meegewogen in de conclusie over risico's of worden gebruikt als onderdeel van het controlebewijs. De accountant kan zijn professionele oordeelsvorming gebruiken om te bepalen welk bewijs de beste basis biedt voor deze beoordeling. Wij hebben goede voorbeelden gezien van accountants die onafhankelijke (externe) informatiebronnen gebruikten wanneer deze beschikbaar waren. Ook zagen wij voorbeelden van accountants die hun risico-inschatting opnieuw uitvoeren op basis van de tool-uitkomsten, en hierop het controleplan hebben aangepast. Dit borgt dat de werkzaamheden, waarvoor de audit-tools zijn ingezet, leiden tot voldoende en geschikte controle-informatie ter onderbouwing van het oordeel van de externe accountant.

Bij het gebruik van audit-tools kunnen uitkomsten leiden tot bevindingen; deze bevindingen kunnen, in het geval ze niet triviaal zijn, moeten worden opgenomen in communicatie met de met governance belaste personen in lijn met NV COS 450.[42] Wanneer audit-tools worden ingezet voor het testen van interne beheersmaatregelen, kunnen bepaalde tools – door de wijze waarop zij de uitkomsten van procedures presenteren – scherp inzicht bieden in geconstateerde tekortkomingen bij de controlecliënt. Bijvoorbeeld via een dashboard waarop alle resultaten worden weergegeven, waardoor de accountant visueel kan beoordelen welke beheersmaatregelen op welk moment zijn toegepast en of dit aansluit bij het beleid van de organisatie. Bij gegevensgerichte werkzaamheden bieden sommige tools duidelijke visualisaties van analyse-uitkomsten, gekoppeld aan de materialiteit of de vooraf bepaalde norm voor de beoordeling van deze resultaten. Dit ondersteunt de externe accountant bij het evalueren van afwijkingen en het bepalen of deze tot bevindingen leiden die gecommuniceerd moeten worden aan het management of de met governance belaste personen bij de controlecliënt.

De wijze waarop audit-tools uitkomsten presenteren, kan bovendien waarde toevoegen aan de natuurlijke adviesfunctie van de externe accountant. Wij hebben voorbeelden gezien van presentatietechnieken waar de informatie duidelijker wordt weergegeven dan wanneer traditionele technieken waren gebruikt. Bijvoorbeeld omdat het dashboard een 'drill-down' optie heeft, waarmee vanuit hoofdbevindingen doorgeklikt kan worden naar bepaalde relevante details om het verhaal van de accountant te ondersteunen. Het is daarom raadzaam dat accountantsorganisaties beoordelen hoe audit-tools externe accountants kunnen faciliteren bij het vervullen van de verantwoordelijkheden uit NV COS 450.

NV COS 230[43] **en NV COS 500 vereisen dat de externe accountant controledocumentatie opstelt die voldoende en geschikt is om de controleverklaring te onderbouwen.** Afhankelijk van de gebruikte audit-tool en de controlewerkzaamheden waarvoor deze is ingezet moeten procedures, databronnen, verwerkingshandelingen, resultaten en conclusies adequaat worden vastgelegd. Wij zien goede voorbeelden waarin duidelijk is gedocumenteerd hoe analytische procedures zijn uitgevoerd, hoe brondata zijn gevalideerd en hoe tool-uitkomsten zijn gekoppeld aan auditconclusies. Ook zien wij voorbeelden waarbij reproduceerbaarheid van tool-uitkomsten is gewaarborgd door het vastleggen van parameters, aannames en de gebruikte toolconfiguratie (inclusief versienummering). Dit is in het bijzonder van belang wanneer audit-tools worden gebruikt voor het verkrijgen van controlebewijs over relevante beweringen of voor significante risico's. Door duidelijke documentatie en reproduceerbaarheid te waarborgen kan de accountant aantonen dat audit-tools op een consistente en beheerste wijze zijn toegepast.

42 NV COS 450 paragraaf 8
43 NV COS 230 paragraaf 5

Inzet en reikwijdte audit-tools – observaties uit het verkennend onderzoek

Observaties tool-inzet voor specifieke controlewerkzaamheden: Tijdens ons onderzoek hebben we het gebruik van audit-tools verkend binnen diverse controlewerkzaamheden[44]:

Data-analyse: De meeste tools ondersteunen data-analyse voor risicoanalyses en gegevensgerichte werkzaamheden (NV COS 315/330/520), waarbij meerdere databronnen efficiënt worden verwerkt.

Visualisatie: Accountantsorganisaties gebruiken dashboarding-tools om resultaten visueel te presenteren, ook richting het management of commissariaat van de controlecliënt (NV COS 260).

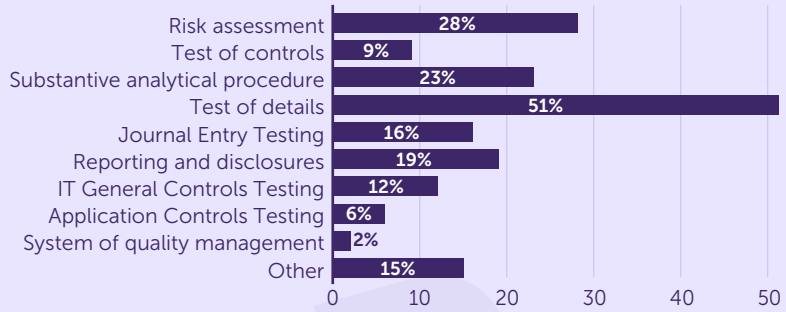
Cliëntacceptatie: Tools worden ingezet bij cliënt- en opdrachtacceptatie en- continuering, als basis voor de eerste analyse, voor verder onderzoek of bij vastlegging van de resultaten van werkzaamheden.

Gegevensgerichte controle: Tools ondersteunen werkzaamheden op het niveau van relevante beweringen of significante risico's, zoals:

- Detectie van ongebruikelijke transacties op basis van parameters.
- Testen van interne beheersingsmaatregelen (GITC's/Application Controls) over volledige populaties.
- Documentanalyse, waarbij data-elementen uit ongestructureerde bronnen (documenten, afbeeldingen, etc.) worden geëxtraheerd en gestructureerd gepresenteerd, inclusief de koppeling naar bronlocaties. Bijvoorbeeld door de geëxtraheerde informatie uit het PDF-bestand zichtbaar te maken bij selectie van het betreffende data-element in het werkprogramma.

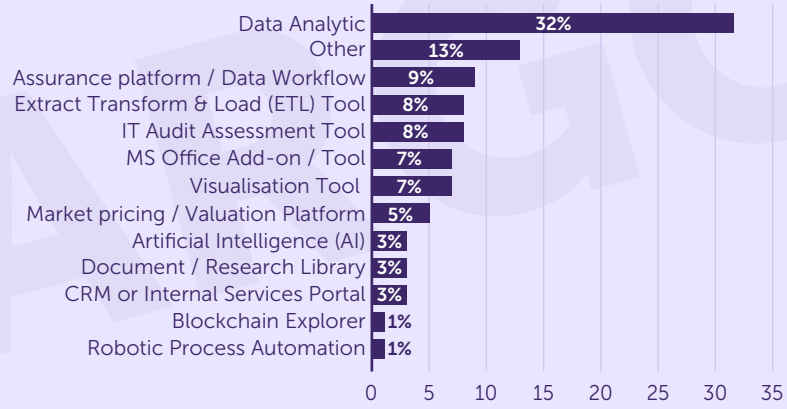
Resultaten data-uitvraag bij OOB-accountantsorganisaties: Uit onze data-uitvraag bij de zes OOB-accountantsorganisaties zien we dat audit-tools in iedere fase van de controle zijn ingezet. Dit ondersteunt het beeld vanuit de organisaties die tijdens het verkennend onderzoek zijn bezocht. De grafiek hiernaast laat zien wat de gemiddelde inzet van audit-tools bij OOB-accountantsorganisaties is voor verschillende categorieën controlewerkzaamheden. Een audit-tool kan in meerdere audit-gebieden ingezet worden, waardoor de som van alle percentages niet optelt tot 100%.

Inzet van audit-tooling per audit gebied (gemiddelde)



Met de data-uitvraag hebben wij inzicht verkregen in de typen audit-tools die voor de medewerkers beschikbaar zijn. Hieronder vallen tools die gebruikt worden voor controlewerkzaamheden (bijvoorbeeld: data-analysetools of visualisatietools), maar ook tools die de organisatie als geheel kunnen ondersteunen (bijvoorbeeld: CRM-systemen). Ook voor audit-tools die de hele accountantsorganisatie ondersteunen, kunnen de 12 bouwstenen uit dit rapport relevant zijn. Onderstaande grafiek geeft het gemiddelde percentage weer over de OOB-accountantsorganisaties.

Type audit-tooling beschikbaar voor personeel (gemiddelde)



44 Deze lijst is niet limitatief. Dit zijn de meest voorkomende toepassingen die wij tijdens het onderzoek hebben gezien.

4. Randvoorwaarde 4: de (Gen)AI-tool wordt beheerst toegepast

4.1 Bouwsteen 10: (Gen)AI-tools worden veilig en beheerst ingezet

De technologie die ten grondslag ligt aan (Gen)AI brengt nieuwe risico's met zich mee voor informatiebeveiliging. Waar traditionele tools werken met vaste functies en gecontroleerde algoritmes, is (Gen)AI-technologie dynamisch en minder transparant. Hierdoor is het lastiger te achterhalen wat er met ingevoerde data gebeuren, bijvoorbeeld of deze worden gebruikt als trainingsdata of worden verzonden naar externe systemen of derde partijen.[45] Het risico op datalekken bij gebruik van (Gen)AI-technologie is daardoor groter dan bij traditionele technologie. Een lek kan ertoe leiden dat vertrouwelijke informatie van de controlecliënt (bijvoorbeeld koersgevoelige informatie) ongewenst openbaar wordt of dat privacywetgeving[46] wordt geschonden doordat persoonsgegevens in trainingsdata van het (Gen)AI-model terechtkomen. In het ergste geval kan dit leiden tot schending van de geheimhoudingsplicht van accountants, bijvoorbeeld door non-compliance met de Wet toezicht accountantsorganisaties (Wta) en de Verordening gedrags- en beroepsregels accountants (VGBA). Informatiebeveiligingsrisico's zijn daarom bijzonder relevant bij de implementatie van (Gen)AI-tools in de sector. Het is essentieel dat de accountantsorganisatie duidelijke afspraken maakt over eigenaarschap en verwachte beveiligingsmaatregelen. Deze afspraken moeten worden gemaakt met zowel softwareleveranciers als controlecliënten, en eventuele derde partijen waarvoor data worden verwerkt, om risico's effectief te mitigeren.

Bij het gebruik van (Gen)AI-tooling is het, net als bij andere audit-tools, van belang om beleid op te stellen over onder andere minimalisatie, anonimisering, pseudonimisering en de bewaartermijn van data – om zo de vertrouwelijkheid van (klant)data te waarborgen. Dit geldt zowel voor verwerking binnen de eigen omgeving als voor verwerking bij externe partijen. Daarnaast is het bij (Gen)AI-tooling cruciaal om duidelijke afspraken te maken met stakeholders over de verwerking van data die kunnen worden gebruikt om (Gen)AI-modellen te trainen. Hierbij is het verstandig om te beoordelen of wettelijke (of andere) bepalingen vereisen dat er afspraken met derde partijen of controlecliënten worden gemaakt. Voor (Gen)AI-tooling gelden dezelfde informatiebeveiligingsvereisten als voor traditionele audit-tools. Een passend raamwerk voor informatiebeveiliging, zoals besproken in Hoofdstuk 2.1, moet daarom ook (Gen)AI-toepassingen afdekken. Dit geldt ook voor zelfontwikkelde tools die gebruikmaken van (Gen)AI, zoals bijvoorbeeld een eigen Python-script dat een Large Language Model (LLM) aanroept.

45 Autoriteit Persoonsgegevens ("AP") - AP-visie op generatieve AI (gepubliceerd in mei 2025)

46 AP - Let op: gebruik AI-chatbot kan leiden tot datalekken (gepubliceerd in augustus 2024)

Good practice
Verschillende accountantsorganisaties gebruiken een (Gen)AI-tool die informatie kan ophalen uit interne systemen, waaronder documentatie en handleidingen van de accountantsorganisatie. De accountant kan met de (Gen)AI-tool bijvoorbeeld antwoorden krijgen over de aansluiting van het door het opdrachtteam opgezette controleplan met de standaarden binnen de accountantsorganisatie. De accountantsorganisatie heeft met toolconfiguratie beheersmaatregelen geïmplementeerd om te borgen dat de tool geen vertrouwelijke informatie kan raadplegen. Daarnaast is er beleid gedeeld met alle medewerkers van de organisatie, zodat zij begrijpen hoe zij moeten omgaan met vertrouwelijke informatie bij het gebruik van de (Gen)AI-tool.

Toelichting
Wij moedigen aan dat accountantsorganisaties de configuratie van (Gen)AI-tools op een zorgvuldige wijze inregelen om risico's te beheersen die met deze tools gepaard gaan. Daarnaast onderkennen wij het belang van beleid dat ingaat op de vertrouwelijkheid van data en informatiebeveiliging om bewustzijn te creëren bij medewerkers. Bij het gebruik van (Gen)AI-tooling is dit extra relevant omdat deze technologie output kan generen op basis van grote hoeveelheden beschikbare data. Daarnaast zijn nog niet alle risico's van deze nieuwe technologie bekend bij accountantsorganisaties. Bij onjuiste tool-configuratie kan dit leiden tot bijzonder vervelende situaties voor accountantsorganisaties. Daarom vragen wij om gepaste aandacht te geven aan de systeemconfiguratie van (Gen)AI-tools en waar nodig experts in te schakelen om risico's te mitigeren.

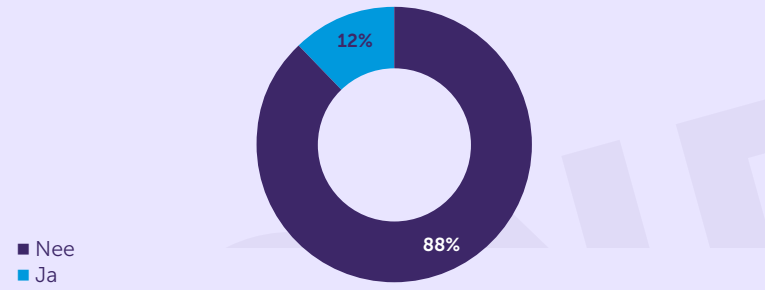
Accountantsorganisaties moeten begrijpen hoe accuraat de uitkomsten van (Gen)AI-tooling zijn als externe accountants deze uitkomsten gaan gebruiken als controlebewijs. Door de techniek achter (Gen)AI-tooling - die werkt op basis van waarschijnlijkheden in plaats van vaste regels - staat de accuraatheid van de uitkomsten niet altijd vast. Accountantsorganisaties hebben verschillende manieren om de accuraatheid van de (Gen)AI-tooling te meten. Bijvoorbeeld door een soll-positie voor de uitkomsten te bepalen en deze periodiek te toetsen voor specifieke werkzaamheden. Denk hierbij aan het reviewen van output bij goedgekeurde prompts uit een promptbibliotheek bij een update van het model. Zo kan worden gevalideerd dat de uitkomsten nog steeds in lijn zijn met de soll-positie. Een andere methode om de accuraatheid te meten is het monitoren van model-specifieke metrics en KPI's. Zo kan de kwaliteit van het model over tijd worden beoordeeld wanneer er veranderingen in de trainingsdata of de tool-configuratie zijn aangebracht (bijvoorbeeld door de F1-score / precision en recall te meten).[47]

Nieuwe vaardigheden en kennis zijn nodig voor een beheerste inzet van (Gen)AI-tooling – en in de toekomst mogelijk ook agentic-AI. (Gen)AI-tooling kan taken overnemen die voorheen door assistent-accountants werden uitgevoerd, waardoor de rol van de assistent-accountant verder verandert. Startende accountants zullen waarschijnlijk nog sneller complexere werkzaamheden oppakken. Dit vraagt om gerichte training en kennisontwikkeling. Een aandachtspunt is dat beperkte ervaring met eenvoudige controlewerkzaamheden kan leiden tot lacunes in kennis, wat weer een risico vormt voor de kwaliteit van het werk dat door (Gen)AI-tooling (of audit-tooling) wordt ondersteund. De ontwikkelingen op het gebied van (Gen)AI dragen bij aan het belang om training van beginnende accountants te blijven evalueren en herzien waar nodig.

47 E-book Advanced Digital Auditing p. 31-32 (gepubliceerd in oktober 2022)

Audit-tools die gebruik maken van (Gen)AI-technologie
OOB-accountantsorganisaties geven bij ons via een data-uitvraag aan dat 12% van de audit-tools die in 2025 beschikbaar zijn, gebruikmaken van AI of Generatieve AI. Deze tools kunnen in de basis uit AI bestaan of een AI-component bevatten. Vanuit ons onderzoek begrijpen wij dat de verwachting is dat (Gen)AI-tooling, de komende jaren steeds relevanter zal worden in de controle-praktijk. Dit vernemen wij bij zowel accountantsorganisaties met een OOB-vergunning als bij reguliere vergunninghouders.

AI in audit-tooling



Wat verwacht de AFM?
(Gen)AI vraagt om een nieuwe manier van werken van huidige en nieuwe medewerkers. De uitkomsten van (Gen)AI-tools moeten kritisch worden beoordeeld. Medewerkers moeten getraind worden in deze nieuwe manier van werken. Daarbij moeten zij de juiste kennis hebben voor de beheersing van de variabiliteit in uitkomsten en andere risico's die aan deze technologie verbonden zijn.

We verwachten dan ook dat accountantsorganisaties zich in elk geval de volgende vragen stellen: Welke werkzaamheden krijgen door (Gen)AI-tools minder menselijke aandacht? Hoe beïnvloeden deze veranderende werkzaamheden de vaardigheden van de accountant op de korte, middellange en lange termijn? Welke kennis en vaardigheden moet u uw medewerkers daarom bij-brengen om potentiële risico's te beheersen en de kwaliteit van de wettelijke controle te waarborgen?

4.2 Bouwsteen 11: de uitkomsten uit de (Gen)AI-tool zijn verifieerbaar of reproduceerbaar

De output van (Gen)AI-tooling kan niet altijd exact gereproduceerd worden, maar de uitkomsten moeten wel verifieerbaar of repro-duceerbaar zijn. (Gen)AI-tooling is stochastisch van aard waardoor output kan variëren. Daarnaast bestaat een neuraal netwerk van een LLM uit een zeer groot aantal parameters, waardoor niet transparant is hoe een uitkomst tot stand komt. Hierdoor fungeert (Gen)AI-tooling in sommige gevallen als een 'black box' bij accountantsorganisaties. Zeker wanneer de organisatie geen controle heeft over alle parameters die tot de output leiden.

Wanneer de externe accountant de output van (Gen)AI-tooling gebruikt als controlebewijs, is het van belang dat deze output wordt geverifieerd. Dit kan bijvoorbeeld door de tool-output aan te sluiten met externe bronnen of brondocumenten, zodat deze traceerbaar is. Als de output niet te verifiëren is, kan ervoor gekozen worden om de uitkomsten reproduceerbaar te maken. Bijvoorbeeld als een machine-learning model gebruikt wordt voor de herberekening van een schattingspost in de jaarrekening op basis van specifieke financiële elementen uit het grootbook en online-databronnen. Doordat het model een goed-geteste versie is, en de algehele betrouwbaarheid van de uitkomsten in het change-managementproces van de organisatie is gevalideerd, zijn de resultaten (binnen een acceptabel foutmarge) te reproduceren.

De documentatievereisten in het controledossier bij gebruik van (Gen)AI-tooling zijn gelijk aan die voor reguliere controlemiddelen. De documentatie moet voldoende gedetailleerd zijn, zodat een erva-ren accountant inzicht krijgt in de aard, timing, omvang, resultaten en conclusies van de uitgevoerde werkzaamheden. Dit betekent dat de resultaten van de tool verifieerbaar of reproduceerbaar moeten zijn en duidelijk moet blijken hoe de externe accountant voldoende en geschikte controle-informatie heeft verkregen.

Bij het gebruiken van alle (Gen)AI-tools is het van belang dat er inzicht is in de relevante keuzes die de (Gen)AI-tooling heeft gemaakt in het proces om tot de output te komen. Zo kan de externe accountant, maar ook een onafhankelijke derde, de relevante keuzes volgen en de uitkomsten controleren. Ook wordt daarmee de juiste informatie verkregen om de werkzaamheden opnieuw te kunnen uitvoeren. In feite is dit niet anders dan wanneer een medewerker of een deskundige in een voorbereidende rol de werkzaamheden vastlegt. Een 'reviewer' kan niet in het hoofd van de voorbereider kijken, maar kan de werkzaamheden van de voorbereider wel volgen als deze op de juiste manier zijn vastgelegd.

Bad practice
De (Gen)AI audit-tool is een 'black box'. Uitkomsten worden gegeven zonder dat er zichtbaar terug wordt gegaan naar specifieke brondocumentatie. Er is geen beleid vanuit de organisatie hoe uitkomsten moeten worden beoordeeld. Hierdoor ontstaat het risico dat de externe accountant de uitkomsten in het controledossier verwerkt, zonder deze eerst te verifiëren.

Toelichting
De uitkomsten zijn niet uitlegbaar, verifieerbaar of reproduceerbaar. Er is een kans op hallucinaties en biases. Doordat de externe accountant niet is uitgelegd hoe de uitkomsten geverifieerd moeten worden en de tool-configuratie complex is, ontstaan er risico's ten aanzien van onjuiste of niet-traceerbare conclusies.

Good practice
De (Gen)AI audit-tool biedt transparantie door bij elke uitkomst direct relevante fragmenten ('snips') uit brondocumentatie te tonen, bij de informatie waar de accountant naar op zoek is. Er is beleid dat voorschrijft hoe uitkomsten moeten worden beoordeeld en geverifieerd.

Toelichting
De resultaten zijn uitlegbaar, verifieerbaar en reproduceerbaar. De kans op hallucinaties en biases wordt beperkt, doordat de accountant inzicht heeft in de herkomst van informatie en weet wanneer aanvullende menselijke verificatie nodig is. Dit stelt de accountant in staat om de eindverantwoordelijkheid te nemen en zorgt voor een controleproces dat transparant en betrouwbaar is.

Een centrale promptbibliotheek voor (Gen)AI-tools is een effectieve manier om consistent gebruik binnen de organisatie te waarborgen. Door standaardprompts vast te leggen en te delen, wordt de kwaliteit van de input in (Gen)AI-tools beter beheerst en ontstaat uniformiteit in de toepassing bij wettelijke controles. Goedgekeurde prompts kunnen het risico op gevarieerde of ongewenste uitkomsten verminderen, zeker als deze voor specifieke doeleinden moeten worden ingezet. Daarnaast fungeert de bibliotheek als kennisplatform, waardoor 'best practices' eenvoudig beschikbaar gemaakt kunnen worden en de efficiëntie in het gebruik van (Gen)AI-tools kan toenemen. Accountantsorganisaties in ons onderzoek geven aan dat een promptbibliotheek kan bijdragen aan grip op kwaliteit, consistentie en kennisdeling binnen de organisatie.

4.3 Bouwsteen 12: de externe accountant is eindverantwoordelijk voor de uitkomsten uit de (Gen)AI-tool

(Gen)AI mag werk faciliteren, maar kan professionele oordeelsvorming nooit vervangen. De externe accountant is verantwoordelijk voor het beoordelen, wegen en valideren van (Gen)AI uitkomsten voordat die uitkomsten worden gebruikt. In onze verkenning hebben we gezien dat niet altijd duidelijk en zichtbaar is vastgelegd waar en hoe (Gen)AI in de controle wordt toegepast. Het is belangrijk dat de externe accountant weet waar (Gen)AI in de controle is toegepast, zodat in het 'reviewproces' hierbij gepaste verantwoordelijkheid genomen kan worden. Dit geldt in het bijzonder voor werkzaamheden waar professionele oordeelsvorming een belangrijke rol speelt.

Good practice
In ons onderzoek zagen wij dat externe accountants (Gen)AI-tools gebruiken als klankbord bij de (fraude)risico-inschatting voor een specifieke sector of bedrijfstypologie. Hierbij maakten zij eerst zelf de inschatting. Vervolgens gebruikten ze de (Gen)AI-tool om hun werk te klankborden en potentiële blinde vlekken weg te nemen.

Toelichting
We zien het belang van de professionele oordeelsvorming van de externe accountant en onderschrijven dat deze niet vervangen kan worden door (Gen)AI-tools. (Gen)AI-tooling kan wel een ondersteunende rol hebben bij de werkzaamheden van de externe accountant, maar mag de externe accountant en diens eindverantwoordelijkheid nooit vervangen.

Uitkomsten van (Gen)AI-tools kunnen overtuigend overkomen door de antropomorfische eigenschappen van sommige tools. Deze tools bootsen menselijke eigenschappen na, waardoor er een risico is dat de tool-gebruiker sneller vertrouwt op de uitkomsten en deze minder kritisch beoordeelt.[48] Dat de resultaten van GenAI-tooling overtuigend kunnen lijken door hun structuur en/of vorm, kan voor het 'halo-effect' zorgen. Wanneer (Gen)AI-tools op een zeer overtuigende manier uitkomsten presenteren, kan dit eraan bijdragen dat de externe accountant voorbijgaat aan mogelijke hallucinaties, biases en onjuistheden in antwoorden.[49] Dit vergroot het risico van 'overreliance' op (Gen)AI-tooling.

Er zijn beheersmaatregelen mogelijk om het risico van 'overreliance' op (Gen)AI-tooling te mitigeren. We zien goede voorbeelden bij de toepassing van (Gen)AI-tooling waarbij de externe accountant verplichte valideringsstappen met een vaste workflow afhandelt. In dit proces kan iedere werkstap pas worden afgerond nadat de externe accountant heeft bevestigd dat de uitkomst is beoordeeld en waar nodig onderbouwd is met onderliggend controlebewijs.

Tijdens ons onderzoek hebben we gezien dat vrijwel alle accountantsorganisaties (Gen)AI in meerdere of mindere mate gebruiken. Zij gebruiken bijvoorbeeld een 'chatbot' om notulen samen te vatten, als klankbord bij de risico-inschatting of voor het beantwoorden van eenvoudige vragen over methodologie. Accountantsorganisaties zijn ook aan het experimenteren met meer geavanceerde, audit-specifieke tools, zoals (Gen)AI-agents die zelfstandig controlewerkzaamheden kunnen voorbereiden en tot op zekere hoogte ook uitvoeren.

48 NBA - VGBA paragraaf 2.4.

49 DNB en AFM – De impact van AI op de financiële sector en het toezicht (Hoofdstuk 1.4) (gepubliceerd in april 2024) & AFM - Grip op modelrisico is cruciaal voor assetmanagers (gepubliceerd in december 2025)

Bad practice
De (Gen)AI-tooling presenteert een conclusie op zeer overtuigende wijze, waardoor de externe accountant de conclusie direct overneemt in het controledossier. De tool geeft geen duidelijkheid over de generatie van de output, welke data hierbij gebruikt zijn en hoe de betrouwbaarheid is gewaarborgd.

Toelichting
Doordat de tool uitkomsten op een zeer overtuigende wijze presenteert, kan het zijn dat de gebruiker de uitkomsten overneemt, zonder deze eerst kritisch te beoordelen. Het is belangrijk dat de gebruiker zich bewust is van het feit dat uitkomsten uit (Gen)AI-tooling stochastisch van aard zijn, en dat de externe accountant eindverantwoordelijk is voor het verkrijgen van voldoende en geschikte controle-informatie. Waaronder de traceerbaarheid en verifieerbaarheid van de gevormde conclusies.

Good practice
De (Gen)AI-tooling dwingt in de workflow af dat de uitkomsten door de externe accountant gevalideerd moeten worden, voordat doorgegaan kan worden naar de volgende werkstap in de tool. Daarbij staat er een betrouwbaarheidsscore van de uitkomsten en een alert in beeld die de gebruiker herinnert aan de risico's van (Gen)AI en aan de waarde die de gebruiker moet hechten aan de uitkomsten.

Toelichting
De tool dwingt af dat de gebruiker stilstaat bij het valideren van de tool-uitkomsten. De kans op 'overreliance' door de externe accountant wordt daarmee kleiner. Doordat de tool de gebruiker over risico's en de betrouwbaarheid informeert tijdens het gebruik van de tool, wordt de gebruiker gestimuleerd om de uitkomsten te verifiëren en conclusies traceerbaar vast te leggen.

Cultuur heeft een grote invloed binnen accountantsorganisaties op hoe medewerkers omgaan met (Gen)AI-tools. Het is van belang dat medewerkers zich bewust zijn van de risico's bij het gebruik van deze technologie. Tegelijkertijd kan psychologische veiligheid bijdragen aan het stimuleren van het gebruik van innovatieve audit-tools. Dit is een belangrijke balans voor duurzame innovatie.