Wat zijn de beste praktijken voor een bedrijfsrevisor bij het gebruik van AI?

Waarschuwing

De aanbevelingen in deze brochure bevatten aandachtspunten en goede praktijken met als oogmerk kantoren te ondersteunen bij hun reflectie over het gebruik van artificiële intelligentie. Zij zijn niet exhaustief en bestrijken niet alle situaties die zich in de praktijk kunnen voordoen. Elk kantoor blijft verantwoordelijk om de risico's te identificeren en te beoordelen die voortvloeien uit zijn eigen context, opdrachten, organisatie en gebruikte tools, en dienvolgens zijn beleid, procedures en interne beheersingsmaatregelen aan te passen aan deze omstandigheden.

1. Algemeen

1.1. Het kernprincipe: AI ondersteunt, maar vervangt het oordeel niet

De bedrijfsrevisor behoudt de volledige verantwoordelijkheid voor zijn opdracht en zijn oordeel. AI is een hulpmiddel, nooit een vervanging voor een professioneel oordeel of een kritische ingesteldheid. Dit is het principe van de '*human in the loop*': in elke fase moet een betekenisvolle menselijke betrokkenheid behouden blijven. Bedrijfsrevisoren moeten hun professionele oordeelsvormingen kritische ingesteldheid blijven toepassen wanneer zij de resultaten van AI-tools interpreteren. Concreet moet de bedrijfsrevisor steeds voor elke output van een generatieve tool oordelen of die output dient te worden gecontroleerd en getoetst aan andere bronnen. De bedrijfsrevisor zal de bronnen die de AI tool heeft gebruikt voor zijn output opvragen, nagaan op correcte verwijzing en beoordelen op betrouwbaarheid. Modellen kunnen immers plausibele maar foutieve resultaten produceren ('hallucinaties'), en de gegenereerde output vormt op zich geen voldoende en geschikte controle-informatie in de zin van de ISA-normen.

Er dient een onderscheid te worden gemaakt tussen generatieve AI-tools, die inhoud creëren of aanpassen (bijvoorbeeld, een document samenvatten of gegevens analyseren), en automatiseringstools die bedoeld zijn om administratieve of repetitieve taken te vergemakkelijken (zoals agendabeheer, documentclassificatie of het verzenden van meldingen). Bijzondere voorzichtigheid is geboden wanneer een tool wordt ingezet voor de productie van inhoud of voor werkzaamheden die het professioneel advies of oordeel kunnen beïnvloeden. In dergelijke gevallen moeten de verantwoordelijke bedrijfsrevisor de gegenereerde resultaten kritisch beoordelen en op passende wijze valideren.

1.2. Het beroepsgeheim en de vertrouwelijkheid

Dit is waarschijnlijk het meest gevoelige punt voor een Belgische bedrijfsrevisor, die gebonden is aan het beroepsgeheim. Vertrouwelijke of identificeerbare cliëntgegevens mogen niet worden ingevoerd in 'publieke' AI-tools die deze gegevens zouden kunnen hergebruiken voor de training van modellen of op enige andere manier zouden kunnen blootstellen. In de praktijk mogen voor de verwerking van cliëntgegevens uitsluitend professionele oplossingen worden gebruikt die contractuele waarborgen bieden (niet-hergebruik van gegevens, hosting, beveiliging), of gesloten omgevingen. Bovendien moet worden nagegaan waar en hoe deze gegevens worden verwerkt en opgeslagen.

1.3. Naleving van de AVG en de AI Act

De Algemene Verordening Gegevensbescherming (AVG – Verordening (EU) 2016/679) is van toepassing zodra persoonsgegevens worden verwerkt. Daarnaast is de Europese verordening inzake

artificiële intelligentie (AI Act – Verordening (EU) 2024/1689) sinds 2 augustus 2026 volledig van toepassing. De meeste tools die in audit worden gebruikt, vallen onder beperkt of minimaal risico, maar er bestaan transparantieverplichtingen en het gebruik moet in kaart worden gebracht om na te gaan of geen enkel gebruik in een strengere categorie valt.

1.4. Integratie in het kwaliteitsmanagementsysteem (ISQM 1)

De invoering van een AI-tool moet worden ingebed in het kwaliteitsmanagementsysteem van het kantoor: evaluatie en validatie van de tool vóór de uitrol, risicoanalyse, betrouwbaarheidstesten, afbakening van het passende toepassingsgebied, monitoring in de tijd, en beheer van technologische middelen en competenties. De bedrijfsrevisor moet de werking, de beperkingen en de mate van betrouwbaarheid van de tool voldoende begrijpen om er op een beredeneerde manier op te kunnen steunen. Tevens zal hij moeten voorzien in adequate maatregelen ter bescherming van de bedrijfsgegevens.

De evaluatie van de tool moet ook betrekking hebben op de afhankelijkheid van het kantoor ten aanzien van zijn leverancier. In het huidige geopolitieke landschap kan een technologie onbeschikbaar worden of tijdens een opdracht worden uitgeschakeld (exportbeperkingen, sancties, stopzetting of wijziging van de dienst, hosting van gegevens buiten de Europese Unie). Het kantoor moet daarom de continuïteit en de locatie van de dienst beoordelen en een terugvalplan voorzien waarmee de opdracht zonder de tool kan worden voortgezet en afgerond. Werkzaamheden die essentieel zijn voor de oordeelsvorming mogen niet uitsluitend van de tool afhangen.

1.5. Documentatie

Ieder gebruik van AI in de auditwerkzaamheden moet in het dossier worden gedocumenteerd: welke tool werd gebruikt, voor welke procedure, en hoe de bedrijfsrevisor de resultaten heeft beoordeeld en bevestigd. De documentatie moet een derde in staat stellen de uitgevoerde werkzaamheden te begrijpen, met inbegrip van het menselijke controlegedeelte.

1.6. Onafhankelijkheid, objectiviteit en deskundigheid

De tool mag de onafhankelijkheid noch de objectiviteit in het gedrang brengen, en de bedrijfsrevisor moet zijn deskundigheid op peil houden: permanente vorming over deze technologieën, inzicht in mogelijke '*biases*' en waakzaamheid voor het risico van overmatig vertrouwen ('*automation bias*').

1.7. Een intern beleid op kantoorniveau

Het wordt sterk aanbevolen om een intern charter of beleid voor het gebruik van AI te formaliseren: toegelaten en verboden tools, toelaatbare soorten gegevens, verificatieregels, verantwoordelijkheden, voor welke doelstellingen/toepassingen het gebruik wordt toegelaten, en opleiding van medewerkers. Zo worden principes omgezet in operationele en controleerbare regels. Dit draagt bovendien bij tot de sensibilisering en de responsabilisering van medewerkers bij het gebruik van AI-tools, zowel om het gebruik van niet-goedgekeurde of niet-gecontroleerde oplossingen ('*shadow AI*')[1] te voorkomen als om het gebruik van de door het kantoor geselecteerde tools te omkaderen en te optimaliseren.

Voor gezaghebbende en actuele bronnen wordt verwezen naar het IBR en het ICCI (het informatiecentrum van het beroep), evenals naar de publicaties van de IAASB en de IFAC, die actief werken rond de impact van AI op auditmethodologieën.

[1] *Shadow AI*: het niet-officiële of ongecontroleerde gebruik van tools en toepassingen van artificiële intelligentie door medewerkers binnen een organisatie.

2. Goede praktijken in elke fase van de controle of beoordelingsopdracht: planning, risico-identificatie, uitvoering en reporting

Hierna worden de goede praktijken fase per fase uiteengezet. Zij richten zich tot alle kantoren, ongeacht hun omvang, en moeten worden toegepast in verhouding tot de omvang en de complexiteit van het kantoor en van zijn opdrachten. Voor de meeste kantoren, en in het bijzonder voor kleine en middelgrote structuren, is de meest realistische hypothese dat AI vooral beschikbaar is via ingebouwde functionaliteiten in hun auditsoftware (platformen zoals Caseware, MindBridge, enz.) en eventueel via een omkaderde generatieve assistent, eerder dan via intern ontwikkelde modellen. Grotere kantoren die hun eigen tools ontwikkelen of configureren, moeten de validatie- en monitoringstappen dienovereenkomstig versterken. De rode draad blijft in elke fase dezelfde: AI bereidt voor en signaleert, de bedrijfsrevisor beoordeelt en besluit.

2.1. Planning

AI is nuttig om inzicht te verwerven in de entiteit en haar omgeving: synthese van sectorrapporten, voorafgaande cijferanalyse, snelle lezing van verslagen van het bestuursorgaan, belangrijke contracten of interne documentatie, ondersteuning bij de opstelling van de oriëntatienota en bij de berekening van de materialiteit.

Aandachtspunten: laat geen vertrouwelijke cliëntgegevens of kantoorgegevens via een publieke tool verlopen. Gebruik professionele oplossingen die waarborgen bieden inzake niet-hergebruik van gegevens. Elke externe informatie die door een generatief model wordt geproduceerd (sectorcijfers, regelgevende verwijzingen), moet worden getoetst aan een primaire bron, aangezien het risico op verzonnen informatie reëel is. De bepaling van de materialiteitsdrempel en de auditstrategie blijven beslissingen van de bedrijfsrevisor: AI kan de reflectie voeden, maar mag de beslissing niet nemen. Documenteer reeds in deze fase welke tools worden gebruikt en waarvoor.

2.2. Identificatie en inschatting van risico's (ISA 315)

Doel: bepalen waar een afwijking van materieel belang waarschijnlijk is en van welke aard zij is, om de audit te sturen en te dimensioneren. Er wordt nog niets geconcludeerd; AI brengt aandachtspunten naar voren.

Relevante toepassingen: voorafgaande cijferanalyse (ratio's en trends tegenover uw verwachtingen, om onverklaarde schommelingen op te sporen); detectie van frauderisicofactoren (ISA 240); ondersteuning bij de verwerving van inzicht in de entiteit en haar omgeving; ondersteuning van de brainstorming binnen het team over risico's, ter aanvulling van de vereiste bespreking, zonder deze te vervangen.

Aandachtspunten: in deze fase is elke anomalie die de tool meldt een signaal dat moet worden onderzocht, nooit een automatisch 'bevestigd' of 'uitgesloten' risico. De risico-inschatting en de link met de auditstrategie blijven de verantwoordelijkheid van het team. Wees alert op '*automation bias*': de schijnbare verfijning of vermeende objectiviteit van de resultaten die door een AI-tool worden gegenereerd, kan ertoe leiden dat er te veel vertrouwen aan wordt gehecht. Het ontbreken van een alarm is geen bewijs dat er geen risico bestaat, en de tool mag uw reikwijdte niet onterecht beperken. Stel u vragen bij mogelijke *biases* van het model en bij de volledigheid en integriteit van de gegevens waarmee het wordt gevoed. Een analyse op basis van onvolledige gegevens geeft een vals gevoel van zekerheid. Documenteer de redenering die van de signalen van de tool naar uw risicoconclusies leidt.

2.3. Uitvoering (reacties op de risico's — ISA 330, 500, 520, 240)

Doel: voldoende en geschikte controle-informatie verkrijgen om conclusies te kunnen trekken over bepaalde beweringen. De verwerkingen kunnen lijken op die van de vorige fase, maar dienen hier om een vaststelling te onderbouwen, niet om de werkzaamheden te oriënteren.

Relevante toepassingen: gegevensgerichte controles op volledige populaties in plaats van op steekproeven; tests van journaalposten als reactie op het risico dat het management interne controles omzeilt (ISA 240); gegevensgerichte cijferanalyses (ISA 520); reconciliaties en '*three-way matching*'; extractie van gegevens uit facturen en contracten; corroboratie en beoordeling van eerder gesignaleerde anomalieën; ondersteuning bij steekproeftrekking; analyse van tests van interne beheersingsmaatregelen; voorontwerp van werkdocumenten.

Aandachtspunten: een AI-output vormt op zich geen voldoende en geschikte controle-informatie (ISA 500). U moet de betrouwbaarheid van de tool en van de brongegevens kunnen verantwoorden en de resultaten corroboreren. Dit veronderstelt dat de tool vooraf is gevalideerd binnen uw kwaliteitsmanagementsysteem (ISQM 1), en niet ad hoc per opdracht wordt beoordeeld. Let op de reproduceerbaarheid, controleer de volledigheid en integriteit van de ingevoerde datasets (een controle op zich) en documenteer nauwkeurig wat werd getest, hoe dit gebeurde en hoe de resultaten aan menselijke beoordeling werden onderworpen.

2.4. Reporting

AI kan helpen bij de opstelling van onderdelen van het verslag, de structurering van KAM's, de samenvatting van bevindingen, de voorbereiding van de management letter of de uitvoering van coherentiecontroles op het dossier.

Aandachtspunten: het oordeel en de conclusies worden nooit gedelegeerd. Zij moeten uw eigen oordeel weerspiegelen. Elke feitelijke bewering in een gegenereerde tekst moet worden gecontroleerd aan de hand van het dossier. Wees voorzichtig met generieke formuleringen die niet exact overeenstemmen met de concrete situatie. Het beroepsgeheim geldt ook in deze fase: wees waakzaam voor vertrouwelijke gegevens die in een schrijfassistent worden ingevoerd. Een menselijke controle en beoordeling van het verslag blijven onmisbaar.

Archivering: zorg er bij de definitieve samenstelling van het dossier (ISA 230) voor dat de elementen met betrekking tot het gebruik van AI zelfstandig in het dossier worden bewaard, zoals bijvoorbeeld relevante output, gebruikte prompts of parameters, de versie van de tool en sporen van de menselijke beoordeling. Het dossier moet gedurende de volledige wettelijke bewaartermijn volledig en begrijpelijk blijven, ook wanneer de tool niet langer beschikbaar is of werd gewijzigd. Het mag niet afhankelijk zijn van een extern platform om de uitgevoerde werkzaamheden te reconstrueren.

2.5. De transversale basis, eenmalig op te zetten

Ongeacht de omvang van het kantoor wordt aanbevolen om een kader te formaliseren in plaats van AI geval per geval te behandelen. Concreet gaat het om: een intern charter (toegelaten tools, toelaatbare soorten gegevens, verificatie- en documentatieregels, verantwoordelijkheden); integratie van de tools in uw ISQM 1-kwaliteitsmanagementsysteem (validatie vóór de uitrol, betrouwbaarheidstesten, monitoring in de tijd); het gebruik van oplossingen met contractuele vertrouwelijkheidswaarborgen in plaats van publieke tools; naleving van de AVG en de AI Act (volledig van toepassing sinds 2 augustus 2026, met de bijhorende transparantieverplichtingen); en permanente vorming van medewerkers, inclusief over de beperkingen en '*biases*' van modellen. Het principe '*human in the loop*' en de professionele scepsis zijn zonder uitzondering van toepassing op alle vier fasen.

Een nuttige methodologische aanbeveling, in het bijzonder voor kleine en middelgrote kantoren: voer AI niet in alle fasen tegelijk in. Een geleidelijke uitrol, vaak te beginnen met risico-identificatie en populatietests, waar de winst het duidelijkst en het best meetbaar is, maakt het mogelijk om de tools te valideren en de documentatie op punt te stellen voordat het gebruik wordt uitgebreid naar de andere fasen van de audit.