TIAS

SCHOOL FOR
BUSINESS AND SOCIETY

Veertig jaar aan het digitale front

Van mainframes tot kunstmatige intelligentie: terugblik op een loopbaan in IT-auditing

Professor Rob Fijneman

Toen ik halverwege de jaren tachtig begon in het vak, konden maar weinig mensen voorzien dat informatietechnologie zou uitgroeien tot het zenuwstelsel van vrijwel iedere organisatie. Wat begon als een specialistisch vakgebied ter ondersteuning van de financiële controle, draait inmiddels om onderwerpen als digitaal vertrouwen, weerbaarheid, cybersecurity, governance en steeds vaker kunstmatige intelligentie.

Als ik terugkijk op de afgelopen veertig jaar, zie ik vijf grote veranderingen die ook mijn loopbaan hebben bepaald:

- van mainframes naar netwerken;
- van beheersmaatregelen naar governance;
- van financiële assurance naar digitaal vertrouwen;
- van periodieke audits naar continue assurance;
- van traditionele informatiesystemen naar kunstmatige intelligentie.

Kenmerkend voor informatietechnologie is dat oud en nieuw meestal naast elkaar blijven bestaan. Organisaties werken vaak met een combinatie van oplossingen uit verschillende generaties. Ik wil hier dan ook geen volledige geschiedenis van IT-auditing schrijven. Het is mijn persoonlijke terugblik, gevormd door veertig jaar werk voor klanten, professionele praktijk en academische betrokkenheid.

Mijn loopbaan is bovendien nog niet voorbij. Ik blijf actief binnen IT- en digital auditing, zowel in het bedrijfsleven als in de academische wereld. Maar na vier decennia is dit wel een goed moment om terug te kijken: hoe heeft het vak zich ontwikkeld, wat is hetzelfde gebleven en wat staat ons nog te wachten?

Auditen in de computerruimte

In de jaren tachtig richtte IT-auditing zich vooral op grote, centraal beheerde omgevingen. We controleerden fysieke toegangsbeveiliging, batchverwerkingen, systeemwijzigingen en herstelprocedures. Bewijs verzamelden we handmatig, vaak aan de hand van papieren rapportages en omvangrijke documentatie.

De vragen waren relatief overzichtelijk:

- Kan het management vertrouwen op de geautomatiseerde verwerking?
- Werken de beheersmaatregelen zoals bedoeld?
- Zijn de financiële gegevens betrouwbaar?

Voor die tijd was dit sterk technisch werk. Tegelijkertijd vormde het de basis voor een ontwikkeling die het vak ingrijpend zou veranderen.

"Bij de introductie van mainframes werd al duidelijk hoe belangrijk het is om de betrouwbaarheid en beveiliging van gegevens en de verwerking daarvan te kunnen toetsen."

De fundamenten van het huidige vak werden toen al gelegd.

Naarmate computers niet langer op zichzelf stonden maar steeds meer met elkaar verbonden raakten, namen zowel de mogelijkheden als de complexiteit toe. Daardoor ontstond behoefte aan specialisten die niet alleen konden beoordelen of financiële gegevens correct werden verwerkt, maar ook of de bredere digitale omgeving beheersbaar en betrouwbaar bleef. In die periode kreeg ook het onderscheid tussen algemene IT-beheersmaatregelen en applicatiecontroles een vaste plek binnen het vak.

De eerste wetgeving rond computercriminaliteit in de jaren tachtig liet zien dat het besef breder werd: organisaties moesten verantwoording kunnen afleggen over de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking. In de decennia daarna nam de regelgeving rond cyberrisico's, privacy en weerbaarheid sterk toe, naarmate organisaties en de samenleving afhankelijker werden van digitale technologie.

IT-auditing wordt een zelfstandig vakgebied

Toen technologie zich door de hele organisatie begon te verspreiden, werd duidelijk dat financiële en operationele audits alleen niet meer voldoende waren.

Nederland liep voorop bij de ontwikkeling van specifieke opleidingen en professionele standaarden voor IT-auditing.

"De eerste IT-audits vonden plaats in de grote mainframeomgevingen van internationale ondernemingen. Daaruit ontstond behoefte aan een eigen, gespecialiseerd IT-auditvak."

Het vak professionaliseerde snel. Halverwege de jaren tachtig ontwikkelden verschillende Nederlandse universiteiten gespecialiseerde opleidingen voor IT-auditors. Rond 1988 gingen deze opleidingen van start, in dezelfde periode waarin NOREA werd opgericht. Zo ontstond een professionele route waarin academische opleiding, praktijkervaring, registratie, standaarden en methodologie samenkwamen. IT-auditing groeide uit tot een erkend vakgebied op het snijvlak van technologie, auditing en governance.

In die jaren raakte ik ervan overtuigd dat opleiding een van de belangrijkste pijlers onder het vak zou worden. Met de ontwikkeling van technologie werden ook de curricula steeds breder en gingen ze de volledige levenscyclus van technologie omvatten. De noodzaak om voortdurend te blijven leren is een belangrijke reden waarom ik mij gedurende mijn hele loopbaan intensief met academische programma's ben blijven bezighouden.

TIAS

Van beheersmaatregelen naar governance

In de jaren negentig en het begin van deze eeuw deden enterprise-systemen, wereldwijde netwerken en internetgedreven bedrijfsmodellen hun intrede. Technologie was niet langer alleen een verantwoordelijkheid van de IT-afdeling. Besturen werden er voor het functioneren en presteren van hun organisatie steeds afhankelijker van.

Daarmee drong een belangrijk inzicht door: **"Technologie werd steeds meer onderdeel van de business zelf."**

Ook de audit veranderde. De aandacht verschoof van beheersmaatregelen rond afzonderlijke systemen naar governance over complete technologielandschappen. Tegelijkertijd werden de verschillende verantwoordelijkheden binnen organisaties duidelijker. Het management was verantwoordelijk voor de kwaliteit van processen en digitale oplossingen, risk- en compliancefuncties hielpen bij het inrichten en bewaken van de beheersing, en interne en externe auditors beoordeelden die beheersing en verschaften assurance. Later schreef ik daarover:

"Het is tijd dat bestuurders en managers op de digitale snelweg op zoek gaan naar zekerheid."

Governance van technologie werd een verantwoordelijkheid van het bestuur. De IT-auditor kreeg daarbij steeds meer de rol van verbindende schakel tussen technologie, risico's en bedrijfsstrategie.

In de praktijk kent goede governance altijd twee kanten. Aan de ene kant gaat het om beheersing: zijn digitale risico's voldoende in beeld en worden ze volgens duidelijke normen beheerst? Aan de andere kant is er de strategische vraag: sluiten de technologische keuzes, investeringen en capaciteiten van de organisatie aan bij haar doelstellingen? IT-auditing voegt de meeste waarde toe wanneer beide vragen aan bod komen, en het vak zich niet beperkt tot technische compliance.

De opkomst van digitaal vertrouwen

Met de komst van internet veranderde ook het karakter van IT-auditing. Cybersecurity werd een belangrijk thema. Privacy kreeg veel meer gewicht. Uitbestedingsketens werden complexer en algoritmen gingen steeds vaker beslissingen beïnvloeden.

Daarmee werden ook de vragen breder en maatschappelijk relevanter.

"Digitale integriteit, eerlijkheid, rechtvaardigheid en veiligheid hebben een maatschappelijke betekenis gekregen."

Voor het eerst ging IT-auditing niet meer alleen over de risico's van een individuele organisatie. Het ging steeds vaker om het vertrouwen van de samenleving, omdat digitale oplossingen invloed kregen op de privacy, kansen en behandeling van burgers, en niet alleen op de interne efficiëntie van organisaties. Die ontwikkeling heeft veel van mijn latere werk bepaald.

"IT-auditing gaat over het onafhankelijk beoordelen van de kwaliteit van informatietechnologie, waaronder infrastructuur, applicaties, processen, data en governance."

Het werkterrein was aanzienlijk breder geworden. We beoordeelden niet langer alleen systemen. We droegen eraan bij dat mensen en organisaties op digitale systemen kunnen vertrouwen.

Ook het begrip kwaliteit kreeg daardoor een bredere betekenis. Betrouwbaarheid, beschikbaarheid en beveiliging bleven essentieel, maar daarnaast kwamen privacy, rechtvaardigheid, eerlijkheid, effectiviteit, efficiëntie en weerbaarheid te staan. Alleen vaststellen dat technologie werkt zoals ontworpen, is niet langer voldoende. Ook de vraag of dat ontwerp verantwoord, proportioneel en vertrouwenwekkend is, hoort bij het vak.

Gedurende mijn loopbaan ben ik IT-auditing dan ook steeds meer gaan zien als een manier om organisaties én de samenleving houvast te bieden op de digitale snelweg. Naarmate digitale systemen sterker met elkaar verbonden raakten en meer invloed kregen, wilden stakeholders niet alleen zekerheid over betrouwbaarheid en beveiliging, maar ook over integriteit, rechtvaardigheid, weerbaarheid en verantwoordelijkheid.

Verschillende vormen van assurance

In de loop der jaren heeft het vak steeds meer instrumenten ontwikkeld om verschillende soorten vragen te beantwoorden. Assurance over serviceorganisaties geeft bijvoorbeeld vertrouwen in uitbestede processen. Bredere niet-financiële assurance kan betrekking hebben op beveiliging, privacy, vertrouwelijkheid en andere kwaliteitsaspecten. Bij overeengekomen specifieke werkzaamheden worden feitelijke bevindingen gerapporteerd, waarna gebruikers daar zelf conclusies aan kunnen verbinden.

Deze rapportagevormen liggen op een continuüm. De beste keuze is niet automatisch de rapportage die de meeste zekerheid biedt. Het gaat om de vorm die het beste past bij de vraag van het management, de gehanteerde criteria, de beoogde gebruikers en de volwassenheid van de beheersmaatregelen. Een heldere scope en formulering zijn cruciaal. Assurance heeft alleen waarde als stakeholders begrijpen wat wel en niet is onderzocht.

Kwaliteit van digitale toepassingen vanaf het begin borgen

Eén vraag keert in mijn publicaties en klantwerk steeds terug: hoe kunnen organisaties aantonen dat hun digitale oplossingen betrouwbaar zijn? Juist in een tijd waarin veranderingen elkaar steeds sneller opvolgen, is governance onmisbaar.

Een uitspraak vat die uitdaging goed samen:
"De verantwoordelijkheid voor de kwaliteit van digitale oplossingen krijgt een nieuwe dimensie nu ontwikkelingen elkaar razendsnel opvolgen en iedereen met iedereen verbonden is."

Gaandeweg ben ik er steeds sterker van overtuigd geraakt dat kwaliteit niet achteraf in een systeem kan worden gecontroleerd. Ze moet vanaf het begin in het ontwerp worden meegenomen.

"Het is effectiever en efficiënter om de beheersing al tijdens de implementatie van digitale oplossingen goed in te richten dan achteraf reparaties uit te voeren."

Dit uitgangspunt wordt tegenwoordig vaak aangeduid als **Secure by Design**. Het geldt evenzeer voor cybersecurity en privacy als voor kunstmatige intelligentie.

Secure by Design maakt ook duidelijk waar in de technologieketen de verantwoordelijkheden liggen. Leveranciers moeten veilige oplossingen en transparante beheersmaatregelen in hun producten opnemen. Afnemers moeten vooraf duidelijke kwaliteitseisen stellen en leveranciers kritisch bevragen. Dat de technologie complex is, ontslaat het management niet van zijn verantwoordelijkheid. Een organisatie kan een black box niet zonder meer accepteren. De verantwoordelijkheid voor de inzet van technologie blijft bij de organisatie zelf.

Van jaarlijkse audits naar continue assurance

Cloudcomputing, DevSecOps en digitale platforms brachten een nieuw probleem met zich mee. Een jaarlijkse auditcyclus sluit steeds minder goed aan op systemen die dagelijks veranderen.

De stap naar continue assurance ligt daarom voor de hand. Enkele jaren geleden schreef ik:

"Naarmate steeds meer continue monitoring plaatsvindt, kan ook de IT-auditor zich ontwikkelen richting continuous auditing en op ieder gewenst moment assurance bieden."

Ik zie dit nog altijd als een van de belangrijkste ontwikkelingen binnen ons vak. De toekomst vraagt niet om minder assurance, maar om assurance die sneller beschikbaar is.

Continue monitoring vormt daarvoor de basis. Wanneer beheersmaatregelen doorlopend worden gevolgd en afwijkingen betrouwbaar worden vastgelegd, kan de auditor met actueler

bewijsmateriaal werken en de aandacht richten op veranderingen, afwijkingen en nieuwe risico's. Dat maakt periodiek professioneel oordeel niet overbodig. Het zorgt er juist voor dat assurance beter aansluit bij het tempo waarin digitale omgevingen veranderen.

Jaren geleden stelde ik al dat continue monitoring uiteindelijk een vorm van auditing mogelijk zou kunnen maken die altijd en overal beschikbaar is. Zover zijn we nog niet helemaal, maar de richting is duidelijk: assurance moet actueler, meer geïntegreerd en beter afgestemd op verandering worden.

Kunstmatige intelligentie: een nieuw hoofdstuk

Sinds 2023 domineert kunstmatige intelligentie veel gesprekken over technologie. De mogelijkheden zijn enorm, maar de risico's zijn dat ook. Ik heb er regelmatig op gewezen dat governance moeite heeft om het tempo van innovatie bij te houden.

"De governance rond AI houdt geen gelijke tred met de snelheid waarmee AI wordt ingevoerd."

Tegelijkertijd geldt:

"Het potentieel van AI is enorm, net als de risico's. Met gezonde bedrijfsmatige uitgangspunten en goede governance biedt AI echter ongekende mogelijkheden."

Daarmee heeft ons vak er een nieuwe verantwoordelijkheid bij gekregen: AI-assurance.

Organisaties willen kunnen vertrouwen op onder meer:

- uitlegbaarheid;
- duidelijke verantwoordelijkheden;
- datakwaliteit;
- verantwoord en ethisch gebruik;
- naleving van wet- en regelgeving.

Zoals ik onlangs schreef: **"AI-assurance ontwikkelt zich tot een belangrijke pijler onder verantwoorde inzet van AI."**

Maar de belangrijkste les uit veertig jaar blijft overeind:

"Technologie kan beslissingen op grote schaal mogelijk maken, maar de verantwoordelijkheid blijft bij mensen."

AI maakt multidisciplinaire assurance daarom alleen maar belangrijker. IT-auditors moeten samenwerken met dataspecialisten, juristen, ethici, cybersecurityprofessionals en verantwoordelijken vanuit de business om het systeem, de data, het beoogde gebruik en de impact goed te begrijpen. De auditor neemt de rol van deze disciplines niet over, maar brengt ze samen

vanuit een onafhankelijke, kritische blik, onderbouwd met bewijs en met helderheid over de verantwoordelijkheden.

De volgende stap: geïntegreerde IT-assurance

We staan naar mijn overtuiging aan het begin van een volgende belangrijke fase voor het vak: geïntegreerde assurance.

Niet langer afzonderlijke rapportages over cybersecurity, continuïteit, privacy of AI, maar één samenhangend beeld van digitaal vertrouwen. In mijn Outlook voor 2026 formuleerde ik het als volgt:

"De volgende stap is geïntegreerde assurance over de volledige technologielevenscyclus van een organisatie."

Daaronder vallen, zoals ook uitgewerkt in de door NOREA geïnitieerde Integrated Digital Reporting Standard:

- digitale innovatie;
- data en AI;
- cybersecurity;
- management van externe partijen;
- privacy;
- weerbaarheid.

Voor het vak liggen hier grote kansen. Verschillende stakeholders zoeken vanuit hun eigen perspectief naar zekerheid. Financial auditors willen kunnen vertrouwen op technologische beheersmaatregelen. Besturen zoeken inzicht in strategie en governance. CIO's willen assurance over projecten, cyberrisico's, privacy, AI en externe leveranciers. Toezichthouders verwachten aantoonbare naleving van wet- en regelgeving.

Geïntegreerde IT-assurance kan deze perspectieven met elkaar verbinden in plaats van ze als losse vraagstukken te behandelen.

"IT-assurance moet de lat hoger leggen en een centrale rol spelen voor stakeholders."

Een gedeelde kennisbasis

Dat ons vakgebied steeds breder wordt, vraagt om meer dan individuele technische expertise. IT-auditors hebben een gedeelde kennisbasis nodig waarin auditprincipes worden verbonden met technologie, bedrijfsprocessen, governance en nieuwe wet- en regelgeving.

Het Nederlandse model laat zien wat de combinatie van een gedegen postacademische opleiding, praktijkervaring en professionele registratie kan opleveren. Internationale certificeringen en

vakgemeenschappen voegen daar een breder perspectief aan toe. Deze benaderingen zouden niet met elkaar moeten concurreren, maar elkaar juist moeten versterken.

Geen enkele discipline kan het huidige digitale landschap nog alleen overzien. IT-auditors werken samen met financial auditors, cybersecurityspecialisten, data scientists, privacyprofessionals, engineers, juristen en ethici. Onze eigen toegevoegde waarde zit in het verbinden van al die expertise vanuit een onafhankelijk en op bewijs gebaseerd assuranceperspectief.

Die samenwerking moet verder gaan dan individuele kantoren, universiteiten of nationale beroepsorganisaties. Gezamenlijke leerdoelen, curricula die kunnen meebewegen met nieuwe ontwikkelingen en sterkere internationale samenwerking kunnen bijdragen aan zowel meer capaciteit als meer samenhang binnen het beroep. Een wereldwijd vraagstuk vraagt om een beroepsgroep die wereldwijd van elkaar leert en tegelijkertijd oog houdt voor de lokale context.

“Het vak is op zijn sterkst wanneer diepgaande expertise wordt gecombineerd met een gemeenschappelijke taal van vertrouwen.”

Die gemeenschappelijke taal moet ook begrijpelijk zijn voor bestuurders en managers. IT-auditors kunnen meer impact maken door niet te beginnen bij de techniek, maar bij de beslissing of onzekerheid die voor stakeholders relevant is. Van daaruit kunnen zij de juiste standaarden, methoden en bewijsmiddelen kiezen. Technisch correct zijn blijft noodzakelijk, maar is op zichzelf niet meer genoeg.

IT-auditors moeten daarom betere vertalers worden. Onze uitdaging is niet alleen technologie te begrijpen, maar ook de risico’s, kwaliteit en beperkingen ervan uit te leggen in taal die bestuurders, toezichthouders en burgers begrijpen.

Zes lessen na veertig jaar

Mensen vragen mij geregeld wat er in mijn loopbaan het meest is veranderd. Mijn antwoord verrast hen vaak.

De technologie is volledig veranderd. De principes niet.

Zes lessen zijn voor mij in al die jaren overeind gebleven:

- Technologie verandert sneller dan de principes die eraan ten grondslag liggen.
- Risico verdwijnt niet, maar verplaatst zich.
- Goede governance is belangrijker dan de technologie zelf.
- Vertrouwen blijft het uiteindelijke doel.
- Opleiding en ontwikkeling zijn essentieel.
- Menselijk oordeel is niet te vervangen.

Een belangrijke les voor mij is dat stakeholders zelden om technische perfectie vragen. Ze zoeken vooral duidelijkheid. Welke onzekerheid doet ertoe? En welke beslissing moet worden genomen? De toekomstige impact van IT-auditing hangt daarom niet alleen af van een goede methodologie, maar ook van ons vermogen assurance te koppelen aan de vragen die voor management en maatschappij daadwerkelijk relevant zijn.

De beste IT-auditors die ik in mijn loopbaan ben tegengekomen, onderscheidden zich nooit alleen door hun technische kennis. Ze combineerden expertise met nieuwsgierigheid, integriteit, onafhankelijkheid en moed.

Vooruitkijken

De komende jaren krijgen we te maken met autonome monitoring, AI-ondersteunde audits, quantumcomputing, nieuwe regelgeving en digitale ecosystemen die nog complexer worden. Deze ontwikkelingen zullen onze middelen veranderen en onze mogelijkheden vergroten. Maar de mens moet een wezenlijke rol blijven houden. Professioneel-kritisch denken, ethisch oordeel en verantwoordelijkheid kunnen niet aan een algoritme worden overgelaten.

Als beroepsgroep moeten we twee uitersten vermijden. We moeten niet iedere nieuwe technologie behandelen alsof alle assurancevraagstukken opnieuw moeten worden uitgevonden. Maar we moeten nieuwe risico's evenmin in oude checklists proberen te persen. Principes als onafhankelijkheid, bewijs, professionele scepsis en verantwoordelijkheid bieden continuïteit. Onze methoden, vaardigheden en manieren van rapporteren moeten zich tegelijkertijd blijven ontwikkelen.

De kern van ons werk verandert naar mijn overtuiging niet.

"De toekomst van IT-auditing wordt niet alleen door technologie bepaald. Doorslaggevend is of wij ervoor kunnen zorgen dat innovatie betrouwbaar, transparant en verantwoord blijft."

Na veertig jaar ben ik er nog altijd van overtuigd dat vertrouwen het waardevolste bezit op de digitale snelweg is.

Bronnen

Dit artikel bouwt voort op ideeën uit eerdere publicaties en presentaties van de auteur, waaronder IT auditing, a strong foundation for the future (2023), Securing the quality of digital applications: challenges for the IT auditor (2023), Exporting the Dutch IT auditing profession, the common body of knowledge approach (2024), The future of IT auditing (2024) en bijdragen aan Advanced Digital Auditing: Auditing Advanced Information Systems and Technologies in a Modern Digital World (2022).