

Vijftig jaar IT-audit in de accountants- controle

Een reis door
verleden, heden
en toekomst



Zo'n vijftig jaar geleden deed de IT-audit zijn intrede in de accountantscontrole, wat ook de aanleiding was om vaktechnische ontwikkelingen uit te wisselen via een nieuw vakblad: *Compact*. Natuurlijk is er sindsdien heel veel veranderd, maar bepaalde activiteiten zijn – weliswaar in een nieuw jasje – toch nog niet zo veranderd. Maar zoals in die vijftig jaar zo vaak gezegd is, gaat er natuurlijk wel behoorlijk veel veranderen, niet alleen omdat de aanpak van de accountantscontrole zelf voortdurend verandert, maar ook omdat IT en audittechnieken zich voortdurend ontwikkelen. Nu zien we weer de trend van AI opkomen. Wat gaat dat voor het vakgebied betekenen? Genoeg reden om u mee te nemen in een reis van vijftig jaar terug en twintig jaar vooruit in de ontwikkeling van de IT-audit in de accountantscontrole.



Drs. Peter van Toledo RE
is directeur KPMG IT Assurance
& Advisory.



Drs. Herman van Gils RE
is veertig jaar werkzaam
geweest bij KPMG.

HET BEGON MET DE GEGEVENSGERICHTE CONTROLE

Het verleden van de IT-audit (toen nog EDP-audit geheten [EDP: Electronic Data Processing]) begint zo'n vijftig jaar geleden, vandaar ook het vijftigjarige bestaan van *Compact*. En natuurlijk staat de IT-audit direct al geheel in het teken van de accountantscontrole, omdat de IT-audit wordt ontwikkeld door de grote accountantskantoren. In die tijd staat de aanpak van de accountantscontrole nog nagenoeg geheel in het teken van gegevensgerichte¹ controle.

De kwaliteit van de IT van de gecontroleerde organisatie is eigenlijk helemaal niet relevant, want de accountant neemt omvangrijke steekproeven en voert veel gedetailleerd check- en vinkwerk uit. Van systeemgerichte controle is dan nog geen sprake. Natuurlijk moeten de steekproeven wel wiskundig verantwoord zijn en blijkt het bepalen van de steekproef en de te trekken posten best nog wel lastig in verband met de verschillende soorten steekproefroutines en keuzes zoals stratificeren, wel of geen negatieve posten, perioden, sorteringen en natuurlijk het aselechte karakter, et cetera. Ha, hier verschijnt de IT-auditor dan voor het eerst op het toneel. De IT-auditor is dan eigenlijk primair programmeur, want met wat theoretische steekproefkennis en kennis van de bestanden van de auditee kan de IT-auditor prima ondersteuning verlenen. Nu kan de IT-auditor vooraf inzicht bieden in de posten in het bestand, waardoor de selectie door de accountant effectiever en efficiënter kan plaatsvinden. Overigens is goede kennis van en ook ervaring met programmeren wel van belang, want standaardauditsoftware bestaat nog niet. Veelal gaat het programmeren nog in talen als COBOL (Common Business Oriented Language, een taal die conceptueel bijna niet te vergelijken is met de hedendaagse programmeertalen), in die tijd 'de' standaardprogrammatuur voor administratieve toepassingen. Daarnaast moet je goed kunnen (over)typen, want iedere programmaregel moet afzonderlijk in een ponskaart komen. De accountant/IT-auditor heeft zelf nog geen computer, dus moet de verwerking plaatsvinden op de computer van de klant of in uitzonderingsgevallen op de computer van een bevriende relatie, bijvoorbeeld een verzekeringsbedrijf, want servicebureaus zijn er ook nog nauwelijks. Alles is mainframegericht! Maar daar leert de IT-auditor al wat nieuws, namelijk de rol van besturings-

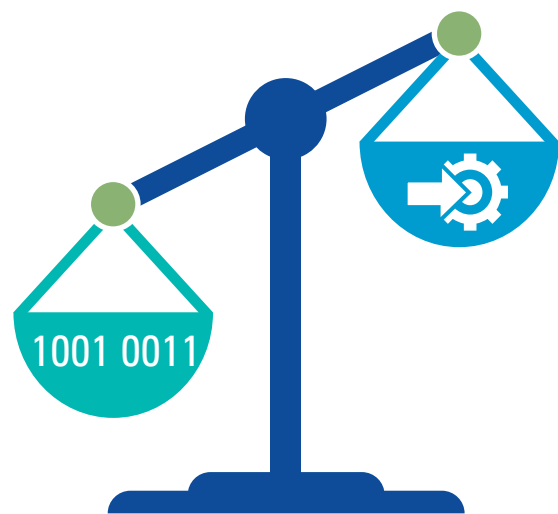
¹ Gegevensgericht versus systeemgericht: bij een gegevensgerichte controleaanpak verkrijgt de auditor zo veel mogelijk controlebewijs door gegevens te selecteren en deze te vergelijken met externe bronnen of door ze te vergelijken met andere reeds gecontroleerde gegevens. Veelal gaat dat steekproefsgewijs. Bij een systeemgerichte controleaanpak verkrijgt de auditor controlebewijs door de toereikendheid van het stelsel van interne controle in de processen en systemen te beoordelen (opzet) en de werking van de interne controles te toetsen.

software en ook de risico's als die besturingssoftware, bijvoorbeeld toegangsbeveiliging en logging, niet goed is ingericht. Ten slotte moet de IT-auditor zich er natuurlijk wel van vergewissen dat er met zijn programma's en data niet is geknoeid. De eerste generatie IT-auditors was relatief technisch onderlegd.

Gelukkig begint de IT-markt ook de accountant (IT-auditor) als doelgroep te zien en komen voorzichtig de eerste standaardauditsoftwarepakketten op de markt. Het bekendst uit die tijd is CARS, een groot COBOL-programma met steekproefroutines en tellingen waarin de IT-auditor zelf COBOL-regels kan toevoegen om het organisatiespecifiek te maken. Omdat de laptop nog niet is uitgevonden, loopt de gemiddelde IT-auditor met flinke koffers rond om al die ponskaarten mee te zeulen (en oh wee als ze door elkaar raakten ...). Maar het is nog relatief eenvoudig, want de bestandsstructuur is nog sequentieel.

Introductie van de database

Kort daarna doet het fenomeen database zijn intrede. COBOL is daar niet zo geschikt voor en de databases krijgen eigen ondersteunende programmatuur. En de IT-auditor leert al snel dat het gebruiken van die databaseware makkelijker is dan CARS, al is in het begin die databaseware geen auditsoftware, maar vooral querysoftware. Natuurlijk laat een integratie niet lang op zich wachten en is er echt sprake van auditsoftware voor verscheidene databasetechnologieën, zoals het onafhankelijke pakket Culprit voor onder andere IBM-mainframes. De problemen in die tijd zijn vooral het benaderen van de bestandsdragers (meestal grote tapes of heel gevoelige schijven), die nog eens heel specifiek voor een bepaald type machine gelden. Kortom, alleen toe te passen op grote bekende computersystemen en dus



Figuur 1. Gegevensgerichte controle voert de boventoon.

alleen voor grote klanten. Dus toch behoorlijk specialistisch. In de jaren zestig en zeventig heeft een groot accountantskantoor zoals (nu) KPMG wel dertig programmeurs die alleen programmeren in het kader van de jaarrekeningcontrole.

De pc komt breed beschikbaar

De grote doorbraak komt begin jaren tachtig. Dan doet de pc zijn intrede en ook de floppy drive (nog wel van 8 inch formaat). Daardoor komen ook middelgrote organisaties in beeld voor ondersteuning van de dienstdoende accountant. Maar weer loopt de auditsoftware op de feiten achter: de (bestaande) mainframepakketten draaien niet op die pc's en de floppy's willen niet in een mainframe. KPMG maakt zelfs een eigen softwarepakket, natuurlijk weer gericht op het bepalen en trekken van steekproeven, en op het maken van allerlei tellingen om aan te sluiten bij de financiële administratie van de klant. Er komt zelfs een aanvullende module waarmee meerdere bestanden met elkaar vergeleken kunnen worden, een hoogstandje in die begintijd van de pc. Wanneer de geautomatiseerde financiële administratie gemeengoed wordt, komen ook de standaardpakketten breed beschikbaar. ACL en iets later IDEA zijn enkele voorbeelden.

Behoeftte aan meer inzicht in beveiliging

In de jaren tachtig en zeker ook de jaren daarna ontstaat het besef dat aan al die IT ook wel risico's kleven, eerst op het gebied van beveiliging en vervolgens op dat van de betrouwbaarheid. De cliënten van de accountant krijgen ook meer behoefte om hierin beter inzicht te hebben. Daardoor krijgen de IT-auditors meer en meer de rol als specialist die namens de accountant ook naar de klant gaat en niet alleen om gegevensbestanden op te halen, maar om de kwaliteit van de IT te beoordelen en daarover te adviseren. Eerst komt de fysieke beveiliging van de IT-omgeving in het onderzoek naar voren, later meer de logische beveiliging. Tooling is daar nog vrijwel niet voor op de markt beschikbaar, dus moet de IT-auditor veel specifieke besturingssystemen en databases onderzoeken en leren hoe de beveiliging georganiseerd is.

Hoewel door het pc-gebruik het aantal uit te voeren gegevensanalyses toeneemt, neemt het aantal programmeurs behoorlijk af, omdat het maken van de analyses veel minder tijd kost door de standaardtoepassingen en de relatief kleinschalige omgeving waarin de programmatuur kan functioneren.

Een einde aan de bestandsanalyse?

In de jaren negentig komt de systeemgerichte controle sterk opzetten en neemt het 'klassieke' gebruik van auditsoftware snel af. De eerder genoemde groep van wel

De eerste generatie IT-auditors was relatief technisch onderlegd

dertig programmeurs bij een groot accountantskantoor is geheel verdwenen, al kan een aantal van hen door groeien als 'reguliere IT-auditor'. Toch betekent het niet het einde van de bestandsanalyses. Er zijn behoorlijk wat 'standaardisatie'-pogingen, vooral rond het veelgebruikte SAP-pakket. Maar door de vele instellingsmogelijkheden blijkt SAP toch niet zo standaard als wellicht gedacht. Hier ontstaat het idee om voor de extractie van de data uit de SAP-databases een frontend-deel te maken dat vervolgens klantspecifiek c.q. generatie-/versiespecifiek gemaakt kan worden. De data komen dan in een 'metadatabase' van waaruit analyses kunnen worden gemaakt en rapportages kunnen worden geproduceerd die sterk aansluiten bij de behoefte van de accountant. Dit backend-deel zou dan sterk gestandaardiseerd moeten zijn. Natuurlijk is de praktijk weerbarstig doordat het frontend-deel steeds aanpassingen behoeft na nieuwe SAP-versies of -implementaties, maar ook de vraag van de accountant wisselt steeds naarmate meer informatie en uitzonderingen uit de data verkregen worden, die weer verklaard moeten worden. De accountant heeft daar zijn/haar handen vol aan. Steeds wordt het kostenbatenplaatje tegen het licht gehouden. De voordelen voor de inzichten en zekerheid van de controleaanpak van de accountant wegen niet altijd op tegen de benodigde inspanningen van steeds aan te passen SAP-analyses.

Toch is het zaadje geplant en worden in meer branches pogingen gedaan de data-analyse nieuw leven in te blazen, zoals in de financiële wereld, waar vooral zelfontwikkelde systemen bij de instellingen de boventoon voeren. Hier zal het frontend-deel (data-extractie) steeds wisselend zijn, maar het backend-deel (analyse en rapportage) kan dan goed aansluiten bij de auditaanpak van de accountant. In verband met de kosten voor ontwikkeling van dergelijke oplossingen is de aanpak vooral internationaal. Maar daarmee is het scala van financiële systemen bij auditees nog veel groter (frontend complicatie) en zijn de wensen van de accountants verscheidener (back-end

complicatie). Mede daarom zijn er helaas slechts enkele oplossingen ontwikkeld en zijn die ook geen lang leven beschoren.

De overgang naar de systeemgerichte controle

De IT-auditor is in de jaren tachtig al betrokken bij het onderzoeken van processen en systemen. De IT-auditors van KPMG ontwikkelden dan de CASA-methode (Cursus Aanpak Systeem Audits), die door het NBA (dan nog NIVRA) wordt overgenomen in de publicatie FASA (Feitelijke Aanpak Systeem Audits; zie verder [Koed85] en [NIVR88]). De doelstelling is dan nog vooral 'understanding the business'. In de jaren negentig komt natuurlijk de systeemgerichte controle opzetten en is er meer behoefte aan heel concreet inzicht in de processen en de daarin opgenomen beheersingsmaatregelen. De IT-auditor past de FASA-methode aan en de Business Process Analysis (BPA) is geboren, waar nadrukkelijk de geautomatiseerde en de handmatige interne-controlemaatregelen afzonderlijk en per processtap/risico worden onderkend. Dat onderscheid is belangrijk omdat de controles natuurlijk anders zijn. Voor de IT-auditor betekent deze aanpak een serieus nieuw onderzoeksobject en het beoordelen van de geautomatiseerde controles aan de hand van de general IT-controls, en dan vooral het change- en testmanagement en de logische toegangsbeveiliging. Ook hier moet dus het bewijs van de goede werking van de geautomatiseerde (application) controls komen van een systeemgerichte controleaanpak, dus helemaal in lijn met de auditaanpak van de accountant.

Met de introductie van de Sarbanes Oxley (SOx) Act in 2002 komt er veel nadruk te liggen op de interne beheersing bij bedrijven. Onder druk van de toezichthouder PCAOB en de vereisten van SOx 404 ontwikkelt het vakgebied van de systeemgerichte controle zich razendsnel. De vraag van toezichthouders 'Hoe weet ik nu zeker dat niemand de betreffende data heeft kunnen manipuleren of application controls kan aanpassen?' heeft menig accountant bij PCAOB-inspecties en interne kwaliteitscontroles kopzorgen opgeleverd. In de afgelopen jaren zijn meer richtlijnen ontstaan over hoe om te gaan met IPE's (Information Provided by the Entity, oftewel: hoe stelt de accountant vast dat de informatie, zoals queries en rapportages, van de auditee betrouwbaar is?), de diverse lagen in de IT-omgevingen, interfaces, assurance-rapporten in de audit en cybersecurity. Wat heeft dit nu opgeleverd in de afgelopen jaren?

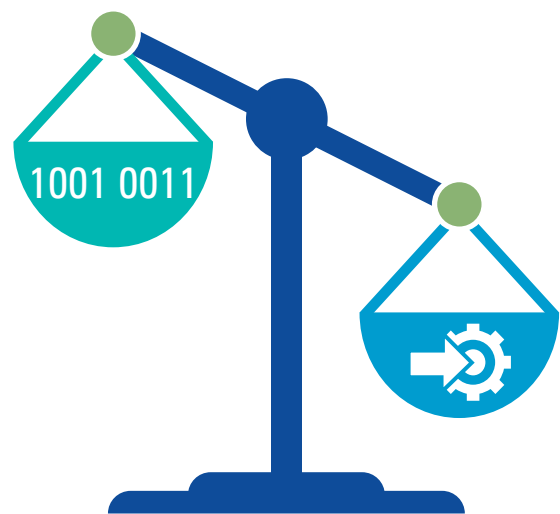
Accountants en IT-auditors werken beter samen en hebben meer begrip voor elkaars vakgebied. De auditmethodologieën van de diverse kantoren maken de rol van de IT-auditor steeds duidelijker. Ook de nieuwe ISA 315-standaard ('Risico's op een afwijking van materieel belang identificeren en inschatten') heeft daartoe bijge-

dragen. In deze standaard zijn uitgebreide richtlijnen opgenomen voor het verwerven van inzicht in de verschillende lagen van informatietechnologie en general IT-controls. Er vindt beter overleg plaats over eventuele tekortkomingen in het stelsel van interne controle, over de risico-inschatting van die tekortkomingen en over eventuele compenserende controles. Maar wat ook blijkt is dat de werkzaamheden om zekerheid te krijgen over de effectieve werking van IT-controls toenemen. Dat is in onze optiek logisch omdat IT complexer wordt en omdat er in de IT-omgeving altijd wel iemand is die toch controles kan (of soms moet kunnen) omzeilen. Hoewel de kans van optreden laag is, kan de impact groot zijn. De uitdaging is om deze risico's te kunnen inschatten en de impact te bepalen. Er zijn niet veel organisaties die qua risicomanagement voldoende volwassen zijn om deze risico's toereikend te kunnen mitigeren en ook de investeringen daarvoor te kunnen of willen doen. Het blijft een select aantal organisaties waar de IT-auditor of accountant een uitsluitend systeemgerichte audit binnen het IT-domein kan uitvoeren. Dit besef leidt in een aantal gevallen weer tot gegevensgerichte detailcontroles van de IT-auditor of de accountant en zo is de cirkel tussen gegevensgerichte en systeemgerichte controles weer rond.

WAT KUNNEN WE IN DE (NABIJE) TOEKOMST VERWACHTEN?

Gegevensgericht

Op dit moment vindt weer meer data-analyse plaats. En met alle relatief steeds makkelijker te benaderen data, zal dit zich nog veel verder ontwikkelen. Denk maar



Figuur 2. De balans is omgeslagen naar systeemgericht.

eens aan de ontwikkelingen op het gebied van gecentraliseerde 'data lakes'. Die bevatten heel veel data van de organisatie (operationeel, financieel, et cetera) bij elkaar, waardoor analyses relatief eenvoudig kunnen plaatsvinden. Voor echt grote organisaties worden deze data lakes te omvangrijk en complex en is er een trend gaande naar 'data meshes', een vorm van gedecentraliseerde kleine(re) data lakes, waardoor de complexiteit (ook in het beheer en de verantwoordelijkheid) minder wordt. Natuurlijk zijn er dan weer tools die meerdere van deze data meshes kunnen koppelen en kunnen analyseren. Kortom, een geweldig terrein voor de data-analist (tegenwoordig veelal data scientist genoemd), zowel binnen een organisatie als bij de accountant. Een wens van de accountant om via data-analyse de geld-goederenstroom inzichtelijk te maken en (geautomatiseerd) analyses te krijgen van de bijzonderheden in deze geld-goederenstroom, zou dan toch eindelijk realiteit kunnen worden.

De vraag komt natuurlijk op of en wanneer de complexiteit zo groot wordt dat de accountant/IT-auditor andere tools gaat gebruiken om nog inzicht te krijgen in de grote hoeveelheid data die beschikbaar is, zowel binnen de te controleren organisatie als daarbuiten. Oftewel, hoelang duurt het nog voordat de accountant en IT-auditor samen zelf gebruik kunnen gaan maken van AI-toepassingen? Zeker bij de hiervoor genoemde analyses van afwijkingen in de geld-goederenstroom zou het toch ideaal zijn als AI-software de analyses kan uitvoeren. Wij verwachten dat met name voor een goed inzicht in de aard en oorzaak van afwijkingen en in de impact op de financiële stroom, AI-software een grote hulp kan zijn. Zeker in de huidige situatie dat data-analyse nogal eens een behoorlijke 'uitval' heeft en de accountant en/of IT-auditor nog veel kosten moet maken om de uitval te bestuderen en de impact te bepalen. Een actueel voorbeeld hiervan is MindBridge Ai Auditor, waarmee KPMG een alliantie heeft. MindBridge Ai Auditor ondersteunt door moderne technologieën data-analyses en stelt – met behulp van statistische analyse en machine learning op basis van een grote verscheidenheid aan datasets – de risico's per individuele grootboek- of verlies-en-winstrekening vast. Dit om mogelijke anomalieën en tekortkomingen in de financiële administratie te identificeren.

Systeemgericht

Zoals hierboven is aangegeven zien wij voor de gegevensgerichte controle een goede toekomst. De vraag is of er dan nog behoefte is aan een beoordeling van het systeem van interne controle. Mogelijk gaat de balans tussen de gegevensgerichte controle met uitgebreide data-analyses enerzijds en de systeemgerichte controle met (beperkte) deelwaarnemingen anderzijds veranderen. Wij zijn van mening dat een zekere mate van systeemgerichte controle nog noodzakelijk zal blijven om vast te kun-

nen stellen dat de organisatie een zeker (minimum) niveau van beheersingsmaatregelen heeft genomen. Een controleaanpak van gegevensgerichte controle zonder dat de organisatie een bepaald minimumniveau van interne beheersing heeft, zal grotere onzekerheid geven over met name de kwaliteit (inclusief volledigheid) van de data. Dat kunnen gegevensgerichte controles niet of in beperkte mate vaststellen. Denk daarbij aan de vraag of alle gegevens daadwerkelijk in de administratie zijn opgenomen, oftewel het 'chiffre d'affaires', zoals accountants dat zo fraai noemen.

Daarnaast zullen de toezichthouders continu druk op organisaties en hun accountants willen blijven uitoefenen om zorg te dragen dat bij organisaties het stelsel van

Onze verwachting is dat de balans weer licht zal uitslaan naar data-analyse

interne controle toereikend is en blijft en dat daarmee de kans op discontinuïteit en fraude beperkt blijft. De SOX-wetgeving en de (verplichte) rol van de accountant daarbij is daarvan een goed voorbeeld en de verwachting is niet dat die snel zal verdwijnen. Voor de IT-auditor betekent dit dat er nog steeds systeemgerichte controles op het gebied van generieke IT-(beheer)processen en specifieke informatiesystemen zullen moeten plaatsvinden, in ieder geval bij een select aantal grote organisaties, al geldt dat op minder formele wijze ook voor minder grote organisaties.

In de praktijk zien we inmiddels organisaties AI-toepassingen gebruiken (bijvoorbeeld verzekeraars). Voor de interne beheersing van AI-applicaties zal de IT-auditor meer inzicht moeten hebben in de opzet en werking van dergelijke AI-applicaties. En dat het snel gaat, blijkt uit de diverse auditraamwerken die gepubliceerd zijn, onder andere door het Verbond van Verzekeraars, maar ook door NOREA (Beroepsorganisatie van IT-auditors in Nederland), IIA en diverse andere organisaties. De Kennisgroep Algorithm & Assurance van NOREA heeft al diverse publicaties laten zien.

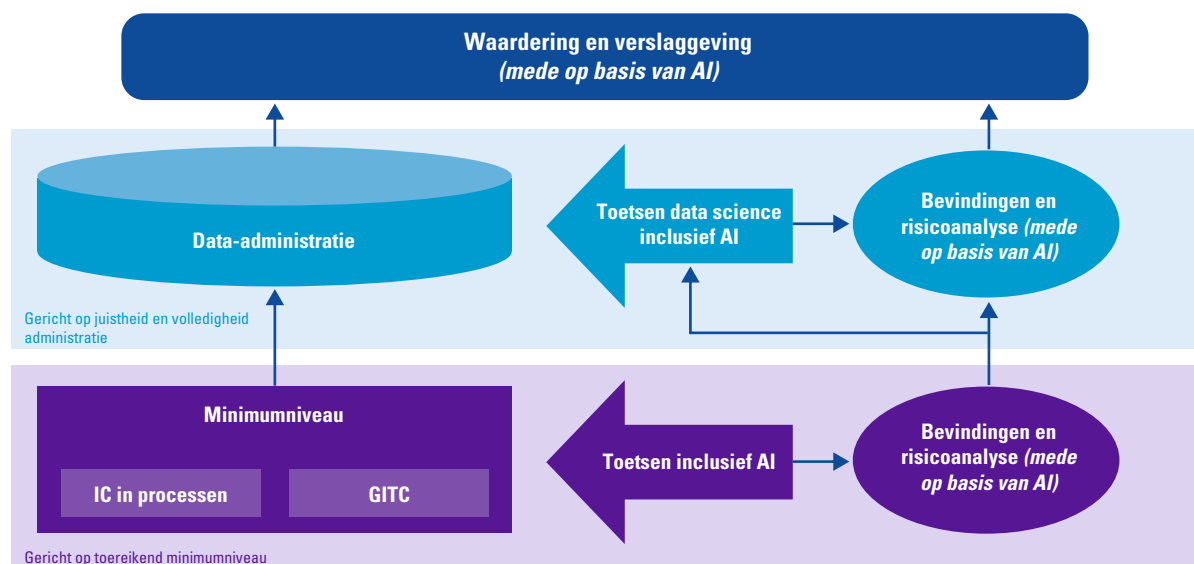
De aanpak van de jaarrekeningcontrole is in figuur 3 samengevat.

Bredere rol van de IT-auditor

De laatste jaren laten zien dat van de accountant meer wordt verwacht dan een 'kale' jaarrekeningcontrole. Met name overige wet- en regelgeving, anders dan voor de jaarrekeningcontrole, dwingt een organisatie in het jaarverslag overige gegevens op te nemen, bijvoorbeeld over de inrichting en handhaving van privacy of informatiebeveiliging/cybersecurity. En natuurlijk zijn zij in

de nabije toekomst onderworpen aan de ESG-regelgeving (Environment [milieu], Social [mens en maatschappij] en Governance [behoorlijk bestuur]). Vanaf 2024 moeten alle beursgenoteerde bedrijven en grote ondernemingen verplicht verslag uitbrengen over duurzaamheidsbeleid en prestaties. Van de accountant wordt verwacht dat hij/zij daarover ook een oordeel heeft. Misschien niet met dezelfde mate van zekerheid als bij de financiële jaarrekening, maar zonder reviews en controles kan de accountant niet tot een oordeel komen.

Hoewel de Europese AI-wet nog niet is ingevoerd, is al wel duidelijk dat audits van producten en diensten uitgerust met AI in bestaande kwaliteitsmanagementsystemen van sectoren zoals logistiek en gezondheidszorg passen. Ook de Corporate Sustainability Reporting Directive (CSRD) zal de rol van de IT-auditor doen verbreden. Vanaf 2024 zullen de eerste organisaties aan deze vereisten moeten gaan voldoen. Vooralsnog is alleen 'limited assurance' (beperkte zekerheid) vereist, maar de verwachting is dat aan het eind van dit decennium ook 'reasonable assurance' (redelijke zekerheid) dient te worden verstrekt bij duurzaamheidscijfers. Organisaties investeren veel om deze cijfers ook te kunnen genereren. Betrouwbaarheidseisen spelen hier een rol. De uitdagingen zijn wellicht niet anders dan in normale financiële rapportageketens, maar er zijn specifieke aandachtsgebieden voor ESG, enerzijds door de bijzondere kennisgebieden, maar ook omdat de rapportageketens nog nieuw zijn en nooit eerder aan IT-audit/accountantscontrole onderhevig zijn geweest. Ook zijn de werknemers bij niet-financiële afdelingen binnen organisaties minder gewend aan strikte naleving van regelgeving om 'in control' te zijn, met als risico onvolledige informatie en controleerbaarheid.



Figuur 3. Aanpak van de jaarrekeningcontrole.

CONCLUSIE

De beroepsgroep van IT-auditors is groot geworden met het doen van bestandsonderzoeken en data-analyses, leidend voor de periode waarin accountants hoofdzakelijk de gegevensgerichte controlebenadering volgden. Wanneer in de jaren negentig de systeemgerichte controle komt opzetten, later versterkt door de SOx-regelgeving, wordt de focus van de IT-auditor minder gegevensgericht en wordt vooral de aandacht gelegd bij de beoordeling van geprogrammeerde controles in de financiële processen en de achterliggende generieke IT-beheerprocessen, zoals changemanagement en logische toegangsbeveiliging.

Hoewel de controlerichting nog steeds systeemgericht is, is er duidelijk sprake van een revival van de bestandsonderzoeken/data-analyses. De data zijn beter benaderbaar en de tools voor data-analyses zijn krachtiger. Systeemgericht wordt niet meer als de heilige graal gezien.

Onze verwachting is dat de balans weer licht zal uitslaan naar data-analyse, waarbij meer aandacht zal gaan naar enerzijds omspannende totaalcontroles (denk aan de geldgoederenstroom) en anderzijds vooral ook de (geautomatiseerde) analyse en risico-inschatting van de afwijkingen die worden geconstateerd. Aan de horizon gloort al een klein stipje van tools die door AI worden ondersteund.

De systeemgerichte controle zal niet verdwijnen, omdat die enerzijds een goed inzicht biedt in de organisatie en haar processen en anderzijds ook een kwaliteitsborging vormt voor de data die tijdens die processen worden vastgelegd. Waar kwaliteitsborging van IT-processen essentieel is voor de interne controles in financiële processen, zo is kwaliteitsborging in de processen essentieel voor de data-analyses. Het is dus niet of systeemgericht of gegevensgericht, maar het beste van beide werelden. En

die werelden worden groter nu steeds meer overige onderwerpen dan puur de jaarrekening in het jaarverslag en daarmee de scope van de accountant worden opgenomen. Het meest in het oog springend is de ESG-rapportering, waardoor nieuwe processen en data in scope komen.

In de jaren tachtig werd een presentatie van het Canadian Institute of Chartered Accountants (CICA, tegenwoordig CPA Canada) veelvuldig in Nederland getoond. De kern was dat accountant Kees in het magische jaar 2000 de jaarrekeningcontrole uitvoerde door zijn 'audit'-computer te koppelen met die van de auditee en het auditprogramma deed de rest. Juffrouw Janny bracht de koffie (dat ging nog zo in die tijd) en 's middags werden de resultaten besproken met de directeur van de gecontroleerde organisatie.

Kortom, in de toekomst van de IT-auditor in het kader van de 'jaarrekening'-controle is een stevige toolbox nog noodzakelijk, maar hopelijk niet zoals de ponskaartkasten en eerste sjouwbare desktopcomputers waarop de data-analyses plaatsvonden. In de onderste twee lagen van de eerder beschreven aanpak van de jaarrekeningcontrole lijkt een dubbelfunctie van accountantskennis en IT-kennis gewenst, wellicht in een geïntegreerd profiel van accountant en IT-auditor. Al zal dat, gegeven het voorbeeld van Kees hierboven, nog wel langer duren dan gewenst.

Literatuur

[**Koed85**] A.H.C. Koedijk (1985). Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: De CASA methode. *Compact*, 1985(4).

[**NIVR88**] NIVRA (1988). NIVRA-geschrift 44, Automatisering en Controle: Feitelijke Aanpak Systems Audit.

Over de auteurs

Drs. Peter van Toledo RE is director KPMG IT Assurance & Advisory. Hij is zijn carrière gestart bij KPMG Accountants en heeft eind jaren negentig de overstap gemaakt naar KPMG Advisory. Binnen KPMG heeft hij diverse opdrachten uitgevoerd, waaronder IT-auditing in het kader van de jaarrekeningcontrole, Assurance-opdrachten, due diligence-onderzoeken en Quality Assurance bij implementatietrajecten. Peter is verantwoordelijk voor IT-attestation-dienstverlening binnen KPMG EMEA.

Drs. Herman van Gils RE heeft veertig jaar bij KPMG gewerkt, eerst in de accountantscontrole en vervolgens in de IT-auditing. Bij zowel NOREA als NBA heeft hij in verschillende commissies geparticipeerd. Nu is hij gepensioneerd, maar hij is nog wel verbonden aan de Universiteit van Amsterdam.