Borging van de kwaliteit van digitale toepassingen: uitdagingen voor de IT-auditor

Prof. dr. Rob Fijneman
RE RA is partner bij
KPMG AG Zwitserland.

Sinds de start van het gebruik van digitale oplossingen speelt de vraag of het allemaal betrouwbaar en veilig is. Meer en meer vragen zowel individuen als bedrijven om zekerheid. Er is behoefte aan standaarden om over de kwaliteit van het gebruik van digitale oplossingen te rapporteren. Deze verantwoordelijkheid ligt eerst en vooral bij het management van een organisatie, maar het inschakelen van een onafhankelijke IT-auditor kan meerwaarde geven.

IT-governance vergt dat het management zijn verantwoordelijkheid neemt voor kwaliteit

INLEIDING

Digitale ontwikkelingen gaan razendsnel. We zijn ons allemaal bewust van de vele digitale toepassingen en mogelijkheden in zowel ons zakelijke leven als ons privéleven. Vaak kennen en gebruiken we overigens maar 10 tot 20 procent van de toepassingsmogelijkheden van de huidige oplossingen, en toch zoeken we steeds weer naar iets nieuws. Of overkomt ons dat allemaal vanuit een zich steeds versnellende 'technologiepush'? De covidpandemie – startend in 2020 – heeft ons nog eens extra laten zien dat digitale hulpmiddelen onmisbaar zijn. Dankzij digitale hulpmiddelen konden we contact houden met elkaar en blijven functioneren en communiceren.

Hoe weten we of de digitale toepassingen en oplossingen voldoende veilig zijn? Zijn de antwoorden die bijvoorbeeld algoritmes genereren wel integer en eerlijk? Zijn we voldoende weerbaar tegen cyberaanvallen en geven we ons geld wel uit aan de juiste digitale oplossingen? Deze vragen zijn uiterst relevant voor bestuurders en toezichthouders van organisaties, aangezien zij zich moeten kunnen verantwoorden voor hun keuzes. Het bestuursverslag vormt extern de basis voor verantwoording over het beleid. Het is vooral terugkijkend van aard en kent een jaarcyclus. In het bestuursverslag zou expliciet over de digitale agenda kunnen worden gesproken. De beroepsorganisatie van IT-auditors (NOREA) onderzoekt of er ook een (externe) IT-audit-'verklaring' ([NORE21]) aan kan worden toegevoegd (zie ook dit artikel over de nieuwe IT-auditverklaring). De verantwoording over de kwaliteit van de digitale toepassingen en of alles veilig, integer en effectief verloopt, krijgt nieuwe dimensies nu de ontwikkelingen razendsnel gaan en iedereen met iedereen is gekoppeld. Zowel bestuurders, toezichthouders alsook eindgebruikers en/of consumenten zoeken zekerheid dat de digitale toepassingen en de daaruit voortkomende data kloppen. Een bevestiging daarvan in de vorm van assurance door een IT-auditor is hierbij een goed instrument. Een bevestiging van de kwaliteit op de digitale snelweg moet en kan worden gevonden.

Niet alleen binnen organisaties, maar ook in de bredere samenleving spelen deze vraagstukken. Het beschermen van de privacy staat stevig onder druk, de talrijke digitale oplossingen bouwen een continu persoonlijk profiel op. Tevens zijn er pijnlijke voorbeelden van het gebruik van algoritmes in het publieke domein ([AR21]) die een aantal burgers ernstig heeft geschaad. Een verantwoorde ontwikkeling naar complexere geautomatiseerde toepassingen vereist beter overzicht en betere kwaliteitscontrole, aldus de Algemene Rekenkamer in haar rapportage over algoritmes in 2021 ([AR21]). Vraagstukken van digitale integriteit, eerlijkheid, redelijkheid en veiligheid hebben een maatschappelijke betekenis gekregen.

In de jaren tachtig van de vorige eeuw ontstond gekoppeld aan de introductie van de Wet computercriminaliteit (WCC I) voor het eerst een expliciete koppeling met het afleggen van verantwoording over de geautomatiseerde gegevensverwerking. Inmiddels is sinds 2019 de Wet computercriminaliteit III (WCC III) ([Rijk19]) van kracht, die rekening houdt met vele ontwikkelingen op het gebied van internet en privacy. De controlerend accountant moet zich als sluitstuk in de keten van controle en verantwoording vanaf de WCC I volgens Burgerlijk Wetboek 2, artikel 393 lid 4, expliciet uitspreken over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking voor zover relevant voor de financiële verslaglegging. Inmiddels zijn we ruim veertig jaar verder en hebben we te maken met veel meer wetgeving op het gebied van de beheersing van digitale oplossingen, hebben we digitale oplossingen die niet alleen de administratieve processen raken maar alle primaire bedrijfsfuncties, en zijn de risico's ook in een ander perspectief terechtgekomen.

Kortom, tijd om eens na te gaan hoe kwaliteit op de digitale snelweg (zoals veiligheid, integriteit, eerlijkheid, efficiëntie, effectiviteit) kan worden geborgd. Op welke wijze kunnen verantwoordingen worden gevormd, welke rol spelen bestuurders en toezichthouders daar zelf in en hoe kan IT-auditing van toegevoegde waarde zijn? Zoals aangegeven spelen deze vraagstellingen niet alleen op individueel organisatieniveau een rol, maar juist ook op maatschappelijk niveau. Hoe kan bijvoorbeeld de overheid het vertrouwen van burgers herstellen of terugwinnen door zich expliciet te verantwoorden over de inzet van haar digitale oplossingen?

IT-auditing betreft het onafhankelijk beoordelen van de kwaliteit van informatietechnologie (processen, governance, infrastructuur). Kwaliteit kent daarbij vele deelaspecten. Niet alleen gaat het om integriteit, beschikbaarheid en beveiliging, maar ook om redelijkheid en eerlijkheid. Daarnaast is de mate van effectiviteit en efficiëntie

ook te beoordelen. Tot op heden is de invulling van IT-auditing nog veelal gericht op individuele digitale toepassingen en nog te beperkt als het gaat om de gehele samenhang van digitale toepassingen passend binnen de IT-governance van een organisatie. IT-auditing kan bij een integralere inzet een belangrijk instrument zijn in het bevestigen van de kwaliteit of het signaleren van risico's bij het ontwikkelen en toepassen van digitale oplossingen. Er ontstaat dan een mooi samenspel tussen de verantwoording door de organisatie over haar IT-governance en de bevestiging van de kwaliteit hiervan door een IT-auditor.

TECHNOLOGIEONTWIKKELINGEN

De coronacrisis heeft het thuiswerken definitief op de kaart gezet en heeft nog meer nadruk gelegd op het belang van flexibele IT. Er zijn een paar trends te noemen die een beeld geven van de digitale oplossingen en ontwikkelingen.

Interessant daarbij is dat relatief veel organisaties een complexe mix van technologieoplossingen kennen, van deels oudere (legacy)systemen en deels nieuwe online (frontoffice)oplossingen. Het is zeker geen sinecure om te zorgen voor integere data, alle oplossingen in continuïteit te laten functioneren, de juiste investeringen te kunnen doen en de kosten te kunnen betalen voor onderhoud van oudere oplossingen en dat alles planmatig te laten verlopen.

Laten we kort een paar trends belichten die veel worden genoemd door meerdere auteurs ([KPMG20]; [Wilr20]):

- Flexibel werken wordt de norm. Afgelopen jaar is de cloudwerkplek – meer dan voorspeld – in populariteit toegenomen. Medewerkers moesten vanuit huis gaan werken en dat vraagt om een flexibele en veilige IT-werkplek.
- *Distributed cloud* biedt nieuwe kansen voor automatisering. Ook de cloud zal zich blijven ontwikkelen, waardoor continu nieuwe mogelijkheden ontstaan die zakelijke groei ondersteunen. Een daarvan, volgens de analisten van Gartner ([Gart20]), is de distributed cloud. Het kan de dataoverdracht versnellen en kosten daarvan verminderen. Ook is het opslaan van data binnen specifieke geografische grenzen (vaak bij wet of vanwege compliance verplicht) een belangrijke reden om te kiezen voor de distributed cloud. De provider van de clouddiensten blijft verantwoordelijk voor het toezicht en het beheer ervan.
- De zakelijke inzet van artificial intelligence (AI) neemt toe. Denk bijvoorbeeld aan het gebruik van chatbots en navigatie-apps. Deze technologie is in de nabije toekomst echter ook zakelijk steeds prominenter aanwezig. De reden? Computerkracht en software worden steeds goedkoper en breder beschikbaar. Zo zal AI steeds vaker worden ingezet voor het analyseren van patronen uit allerlei soorten data.
- *Internet of Behaviours*. Data vormen tegenwoordig de spil in een groot deel van de bedrijfsprocessen. Data bieden inzicht en spelen daardoor een steeds grotere rol bij het nemen van strategische beslissingen. Deze datagedreven werkwijze wordt ook toegepast voor het veranderen van menselijk gedrag. Dit noemen we ook wel het Internet of Behaviours. Op basis van die analyses kunnen suggesties of autonome handelingen worden ontwikkeld die bijdragen aan zaken als menselijke veiligheid en gezondheid. Een voorbeeld is de smartwatch die de bloeddruk en het zuurstofgehalte bijhoudt en op basis daarvan gezondheidstips geeft.
- Volwassenheid van 5G in de praktijk. 2020 was het jaar waarin de providers in Nederland hun eerste 5G-netwerken uitrolden. Met 5G is er geen afhankelijkheid van wifi onderweg of op locatie. Behalve dat de upload- en downloadsnelheid van data hoger is, zitten de grote veranderingen vooral in nieuwe toepassingen, en dan met name op het gebied van het Internet of Things. Voorbeelden zijn zelfrijdende auto's en een chirurg die via een operatierobot op duizend kilometer afstand zijn patiënt opereert. Zulke toepassingen zijn veelbelovend.

MANAGEMENTVERANTWOORDELIJKHED

Het aansturen van en toezicht houden op digitale oplossingen is geen vanzelfsprekendheid. 'Onbekend maakt onbemind' speelt hier nog menig bestuurder parten. De complexiteit van technologie schrikt af, de mengeling van legacysystemen en nieuwe digitale oplossingen maakt het niet erg inzichtelijk, vele partijen beheren een deel van de technologieketen en de kwaliteitseisen zijn niet altijd expliciet.

Toch is een vorm van 'good governance' nodig. Collega-professor Steven de Haes ([DeHa20]) heeft in Antwerpen vele inzichten opgedaan in zijn studies over IT-governance. In zijn ogen moet het bestuur twee zaken regelen rondom digitale oplossingen. De eerste vraag is of de digitale risico's worden beheerd. Dat vergt een standaard om aan te toetsen. In lijn met het bij governancevraagstukken veelal gebruikte COSO-framework (COSO: Committee of Sponsoring Organizations), kan daarbij worden gekozen voor (delen uit) het internationale CoBiT-framework (CoBiT: Control Objectives for Information Technology) ([ISAC19]). Het management maakt daarbij expliciet welke beheerstandaarden in en rondom de digitale oplossingen van toepassing zijn en kan zowel de opzet alsook de operationele werking daarvan (laten) vaststellen.

De tweede vraag is strategisch van aard: kloppen de digitale ontwikkelingen? Is de strategie rondom de inzet van digitale oplossingen correct en kloppen de benodigde

investeringen? Dit te beantwoorden vergt een goede analyse van de organisatiedoelstellingen en de daarbij benodigde digitale oplossingen. Zoals eerder aangeduid, gaat het hier dan vooral om de effectiviteit en efficiëntie.

Het geheel inregelen in een organisatie start met een goede organisatorische opzet. Veelal wordt daarbij gebruikgemaakt van een 'lagenmodel' om de diverse verantwoordelijkheden in te regelen. Duidelijk is dat de primaire verantwoordelijkheid voor het juiste gebruik van de digitale oplossingen ligt bij het eerstelijnsmanagement. Dat kan zich laten bijstaan door een 'risk & control'-functie die als 'tweede lijn' mee kan helpen bij het inrichten van de juiste controles en bij het uitvoeren van risicobeoordelingen. Ook kan de tweede lijn vormen van monitoring op de juiste uitvoering en het juiste gebruik van de digitale oplossingen inrichten. Vervolgens kan een interne auditfunctie als derde lijn beoordelen of de controles in en rondom de digitale oplossingen goed zijn opgezet en werken; indien gewenst, kan de externe auditfunctie dit ook bevestigen. Kortom, er ontstaat een gelaagd model dat gezamenlijk de kwaliteit van de digitale oplossingen moet waarborgen.

Gelet op de enorme snelheid van de digitale veranderingen is continu nieuwe kennis nodig van de technologie. Dat te organiseren in samenhang met oog voor de kwaliteit van de oplossingen en soms ook de inherente beperkingen, is wat maakt of de governance goed werkt. Het is geen statisch geheel, continu zullen veranderingen in de keten moeten worden geëvalueerd en indien nodig bijgesteld. Denkbaar is dat de IT-functie (de CIO of de IT-directie) een structurele technologiedialoog organiseert die begint met kennissessies en vandaaruit ook de kwaliteit van de digitale toepassingen aan de orde stelt. De eindgebruikers en het management moeten hun verantwoordelijkheid nemen om de kwaliteitseisen expliciet te maken, tijdens verandertrajecten ook daarop te sturen en te (laten) bewaken dat de kwaliteit van de digitale toepassingen en de data ook is geborgd.

De leveranciers van de digitale oplossingen vervullen ook een belangrijke rol. Zij moeten goed huisvaderschap betrachten en zorgen voor steeds betere en veiligere oplossingen. Dat gaat niet vanzelf, zo blijkt regelmatig, de focus ligt toch meer bij de functionele vernieuwing dan bij goed beheer en veiligheid. De afnemers van de oplossingen bevragen de aanbieders ook nog te weinig op een 'secure by design'-aanbod. Tijdens het ontwerpen van de oplossing kunnen, en eigenlijk moeten, al de juiste controles worden ingebouwd.

Keert de wal het schip? Met andere woorden, worden de nieuwe digitale oplossingen zo complex dat niemand meer de inhoudelijke juistheid kan vaststellen? Vanuit de managementverantwoordelijkheid kan niet worden gekozen voor een dergelijke 'black box'-benadering. We kunnen niet accepteren dat we bijvoorbeeld een digitale toepassing inzetten zonder te weten of die veilig werkt. Het management zou dan pas op de plaats moeten maken en de kennis eerst moeten organiseren dan wel zich moeten laten informeren over de kwaliteit, voordat de verdere inzet verantwoord is.

UITDAGINGEN VOOR DE IT-AUDITOR

Deze kwaliteitsvraagstukken kunnen worden beantwoord door inzet van IT-auditors. In Nederland is dit vakgebied al ruim dertig jaar georganiseerd, mede via de beroepsorganisatie NOREA (Nederlandse Orde van EDP Auditors)[1] en de universitaire IT-auditopleidingen.

De IT-auditor beschikt over een instrumentarium om de digitale oplossingen op diverse kwaliteitsaspecten te beoordelen. Meer en meer zijn auditing- en rapportagestandaarden ontwikkeld om opdrachtgevers te voorzien van zekerheden of een juist risicobeeld.

Positief is dat de huidige IT-auditstandaarden veel vragen van opdrachtgevers over digitale oplossingen al kunnen beantwoorden. Zaak is vooral dat IT-auditors voldoende kenbaar maken wat ze kunnen en dat wordt samengewerkt met toezichthouders om het instrumentarium te verrijken. De IT-auditor zal eenvoudiger taal moeten gebruiken om duidelijk te maken wat er nu echt aan de hand is. Opdrachtgevers kunnen en moeten hun vraagstelling aanscherpen en zelf ook hun verantwoordelijkheid nemen, zoals het inrichten van het juiste niveau van beheersing.

IT-auditors zoeken het nu vooral nog in vaktechnisch juiste antwoorden en methodologieën, terwijl een dialoog nodig is over de relevante managementvragen rondom IT-governance. Welke dilemma's ervaren bestuurders en toezichthouders bij het vaststellen van het kwaliteitsniveau van digitale toepassingen en welke onzekerheden bestaan er? Daarop zou de IT-auditor zich moeten richten. Vanuit een heldere managementvraag kan het onderstaande, al beschikbare instrumentarium van de IT-auditor veel gerichter worden ingezet.

Vanuit de accountantscontrole is bij outsourcing de standaard ISAE 3402 (ISAE: International Standards on Assurance Engagements)[2] ontwikkeld om zowel de accountant als de klantorganisatie geïnformeerd te houden over de kwaliteit van de controles uitgevoerd door de serviceorganisatie. De focus ligt hierbij op de betrouwbaarheid en continuïteit van de financiële gegevensverwerking. Het

1 Zie www.norea.nl.

2 Zie www.iaasb.org, 'Standards and resources'.

resulterende rapport wordt ook wel een SOC 1-rapport (SOC: Service Organization Control) genoemd.

Bij een ISAE 3402-audit is een goede afstemming nodig over de scope van de werkzaamheden en daarmee de te testen controls (zowel in opzet als in operationele werking). De uitvoerende IT-auditor heeft overleg met zowel de serviceorganisatie als de ontvangende klantorganisatie om alles goed in te regelen. Dit betreft ook specifieke aandacht voor zowel de 'Complementary User Entity Controls' (CUEC's), de aanvullende interne beheersingsmaatregelen die de klantorganisatie moet treffen, als de 'Complementary Subservice Organization Controls' (CSOC's), de beheersingsmaatregelen die hun eventueel ingezette IT-serviceproviders moeten treffen. Veelal vindt ook overleg plaats met de accountant van de klantorganisatie, die het ISAE 3402-rapport gaat gebruiken als onderdeel van zijn accountantscontrole.

De omvang van een ISAE 3402-audit kan aanzienlijk zijn en daarmee al een stevige basis bieden voor de kwaliteitsverantwoording van de digitale toepassingen. Een voorbeeld uit de IT-auditpraktijk betreft een verkochte divisie van een onderneming die nu deel uitmaakt van een andere internationale groep. De verkochte divisie heeft fabrieken in ruim dertig landen die allemaal nog gebruikmaken van de IT-services van de oorspronkelijke groep. Er is een testplan opgezet om de relevante algemene computercontroles te testen (zoals logische toegangsbeveiliging, wijzigingenbeheer en operationeel beheer, ook wel 'general IT controls' genoemd), en alle relevante geprogrammeerde financiële controles in de geselecteerde financiële systemen. In dit voorbeeld levert dit een toetsing op van ruim tachtig algemene computercontroles en ruim tweehonderd geprogrammeerde controles door een centraal groepsauditteam en auditteams in de diverse landen.

Een ander assurancerapport is een ISAE 3000-rapport, dat wordt opgesteld om aan te tonen dat de interne beheerprocessen die een organisatie heeft ingericht, ook daadwerkelijk worden uitgevoerd zoals beschreven. In principe is deze standaard ontwikkeld voor zekerheden over niet-financiële informatie. Dit kan in de vorm van een ISAE 3000-attestatie (3000A), waarbij de organisatie zelf de normen en controles heeft gedefinieerd en intern reviewt en de IT-auditor bevestigt of dit allemaal functioneert, of in de vorm van een 3000D ('direct reporting'), waarbij de IT-auditor de toetsingsnormen en controls mede definieert.
Het ISAE 3000-rapport (ook wel aangeduid als SOC 2[3]) kan zich richten op vele vraagstukken en kent ook meerdere kwaliteitsaspecten als invalshoek, bijvoorbeeld ook vertrouwelijkheid en privacy. Er zijn intussen standaardnormenkaders opgesteld voor het uitvoeren van bijvoorbeeld privacy-audits ([NORE23])[4] op basis van ISAE 3000. Vanuit de Noord-Amerikaanse accountantsorganisaties AICPA, CPA Canada en CIMA[5] zijn er generieke standaardkaders ontwikkeld in de vorm van SOC 2-modules inzake onder andere Security, Availability, Processing Integrity en Confidentiality.[6] Deze zijn goed toepasbaar op IT- en SaaS-diensten en worden in toenemende mate door IT-serviceproviders in Europa omarmd. Voor specifieke IT-auditobjecten, zoals de concreet geleverde online diensten/functionaliteiten, zijn deze nader toe te spitsen of uit te breiden met de – voor de klantorganisatie relevante – IT-(applicatie)controls.

Als laatste variant kan worden gekozen voor overeengekomen specifieke werkzaamheden, aangeduid als een ISAE 4400-rapport. Gebruikers van het rapport zullen zich dan zelf een oordeel moeten vormen over de werkzaamheden en (feitelijke) bevindingen die door de IT-auditor in het rapport zijn weergegeven.

In de afgelopen jaren wordt volop innovatie uitgevoerd binnen het werkveld van IT-auditing om bijvoorbeeld ook algoritmes te beoordelen en hierover een mededeling te doen. Denk aan het vraagstuk van eerlijkheid en non-biased zijn van de gegevens. Er ontstaat een samenspel tussen meerdere disciplines om het risicobeeld van complexe digitale oplossingen te doorgronden en zekerheden te verstrekken. IT-auditors werken samen met dataspecialisten en juristen rondom algoritme-assurance.

De laatste anderhalf jaar is ook een discussie gestart over een mogelijke IT-auditverklaring behorend bij of in aanvulling op het jaarverslag van een onderneming. Expliciet zou de onderneming zich dan moeten uitspreken over haar digitale oplossingen, het beheer daarvan en bijvoorbeeld de veranderagenda daaromtrent. Een IT-auditor zou dan een verklaring hierbij kunnen afgeven. De beroepsorganisatie van IT-auditors heeft een plan van aanpak ontwikkeld om in het komend jaar actief dit IT-verslag en de mededeling daarover verder uit te werken. Tevens wordt nagedacht over de mate van zekerheid die kan worden verstrekt via het oordeel; momenteel kennen we een redelijke en beperkte mate van zekerheid vanuit het verklaringenstelsel. Opdrachtgevers zoeken natuurlijk naar maximale of, wellicht beter, optimale zekerheid. Met andere woorden, de door hen gewenste zekerheid wordt niet altijd gevonden in een IT-auditmededeling. Nog mooier zou het zijn als de

3 SOC 2 gaat primair over beveiliging (verplicht), beschikbaarheid, integriteit, vertrouwelijkheid en/of privacy, zoals uiteengezet in de SOC 2-richtlijnen uitgegeven door het Assurance Services Executive Committee (ASEC) van de AICPA.

4 Er is overigens een Nederlandse en een Engelse versie van het Privacy Control Framework.

5 AICPA: American Institute of Chartered Professional Accountants; CIMA: Chartered Institute of Management Accountants.

6 Zie [Zwin21] voor een artikel over SOC 2 en [AICP23] voor de standaarden van AICPA en CIMA.

mededeling ook zekerheid geeft naar de toekomst, een door IT-auditors nog onbetreden terrein.

CONCLUSIE

Zoals eerder aangegeven, bestaat er al een instrumentarium voor de IT-auditor om de kwaliteit van digitale toepassingen te bevestigen. Opdrachtgevers moeten hun verantwoordelijkheid nemen om de digitale toepassingen beter te begrijpen en de daarbij behorende IT-governance in te richten. IT-auditors kunnen hun communicatie verbeteren, kunnen zich nog meer inleven in de vraagstelling van het management (hun opdrachtgevers) en kunnen ook zorgen voor begrijpelijke rapportages.

Relevante maatschappelijke vraagstukken rondom de inzet van digitale oplossingen kunnen worden beantwoord via een goede risico-inventarisatie en ook een beoordeling van de aanwezige controles. Naast de traditionele vraagstelling gericht op betrouwbaarheid en beveiliging komen vraagstukken van effectiviteit, efficiëntie, privacy en eerlijkheid aan de orde. Tevens is de weerbaarheid van de digitale oplossingen een urgent vraagstuk. In de EU zijn de Network and Information Security Directive (NIS2-richtlijn)[7] en de Digital Operations Resilience Act (DORA)[8] voor financiële instellingen opgesteld om de digitale weerbaarheid te versterken. De toezichthouder van beursgenoteerde bedrijven in de Verenigde Staten (SEC) heeft eveneens richtlijnen uitgevaardigd voor het jaarlijks rapporteren over cyber security (risicomanagement, governance) en het tussentijds melden van ernstige incidenten ([SEC23]).

Secure by design zal naar verwachting meer de norm worden aangezien ook technologieleveranciers begrijpen dat bij de implementatie van een oplossing de juiste controls moeten worden geïmplementeerd. Sommige leveranciers voorzien ook in mechanismen om *continuous monitoring* in te richten, waarbij de ingerichte controls op continue juiste werking worden beoordeeld en uitzonderingen worden gerapporteerd. Hier speelt het management ook een belangrijke rol: omarm de principes zoals hiervoor beschreven. Bedenk dat het effectiever en efficiënter is om tijdens de verandering van digitale oplossingen de beheersing te ontwerpen dan naderhand te repareren.

Indien meer en meer wordt voorzien in continuous monitoring, kan de IT-auditor naar een vorm van *continuous auditing* toegaan, waarbij hij op ieder gewenst moment zekerheden over de inzet van de digitale oplossing kan verstrekken. Het 'anytime, anyplace, anywhere'-principe wordt dan in IT-auditing realiteit. Een mooi, ontspannend vooruitzicht binnen al de digitale snelheden.

7 Zie verder [NCSC23].

8 Zie [Alam22] voor een artikel over DORA.

Over de auteur

Prof. dr. Rob Fijneman RE RA is partner bij KPMG AG Zwitserland, professor in IT-auditing aan TIAS, Tilburg University, en gastdocent aan de St. Gallen Universität.

Literatuur

[AICP23] AICPA & CIMA (2023). SOC 2® – SOC for Service Organizations: Trust Services Criteria. Geraadpleegd op: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

[Alam22] Alam, A., Kroese, A., Fakirou, M., & Chandra, I. (2022). DORA: an impact assessment. Compact 2022/3. Geraadpleegd op: https://www.compact.nl/articles/dora-an-impact-assessment/

[AR21] Algemene Rekenkamer (2021, 26 januari). *Aandacht voor algoritmes*. Geraadpleegd op: https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes

[DeHa20] De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology* (3rd ed.). Springer.

[Gart20] Gartner (2020, 12 augustus). The CIO's Guide to Distributed Cloud. Geraadpleegd op: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-distributed-cloud

[ISAC19] ISACA (2019). COBIT 2019 or COBIT 5. Geraadpleegd op: www.isaca.org

[KPMG20] KPMG (2020). Harvey Nash / KPMG CIO Survey 2020: Everything changed. Or did it? Geraadpleeg op: https://kpmg.com/dp/en/home/insights/2020/11/harvey-nash-kpmg-cio-survey-2020.html

[NCSC23] Nationaal Cyber Security Centrum (2023). Samenvatting van de NIS2-richtlijn. Geraadpleegd op: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-richtlijn

[NORE21] NOREA (2021). Nieuwe IT check: NOREA ontwikkelt IT-verslag en -verklaring als basis voor verantwoording. Geraadpleegd op: www.norea.nl

[NORE23] NOREA (2023). Kennisgroep Privacy. Geraadpleegd op: https://www.norea.nl/organisatie/kennis-en-werkgroepen/kennisgroep-privacy

[Rijk19] Rijksoverheid (2019, 28 februari). Nieuwe wet versterkt bestrijding computercriminaliteit. Geraadpleegd op: https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit

[SEC23] SEC (2023, 26 juli). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies [Persbericht]. Geraadpleegd op: https://www.sec.gov/news/press-release/2023-139

[Wilr20] WilroffReitsma (2020). ICT Trends 2021: dit zijn de 10 belangrijkste. https://wilroffreitsma.nl/nieuws/ict-trends-2021/

[Zwin21] Zwinkels, S. & Koorn, R. (2021). SOC 2 assurance becomes critical for cloud & IT service providers. *Compact* 2021/1. Geraadpleegd op: https://www.compact.nl/articles/soc-2-assurance-becomes-critical-for-cloud-it-service-providers/