

juli 2026

InAudit Magazine



4

Interview
Elles van Dijkman en
Laurien Jonkman
Centramed

10

Artikel
De nieuwe regels voor
loontransparantie

16

Interview
Danny Francken
IIA

24

De wereld van ...
Floris Stokkers

Overzicht over een dynamische wereld

Zoals altijd willen we in ons InAudit Magazine graag met u delen wat ons zoal bezig houdt, buiten onze reguliere werkzaamheden om. Dit eerste half jaar ging dat vaak om het bijhouden van het hoge tempo waarin technologie onze wereld binnenkomt. Enkele jaren nadat we ons verbaasden over wat ChatGPT allemaal kon, lijkt de wereld nu in paniek over wat Mythos allemaal kan: blijkbaar probleemloos de zwakheden van bestaande software blootleggen. In deze dynamische wereld willen we graag met u delen waarin wij investeren.

CISO-functies

In een wereld waarin het tempo van de spraakmakende datalekken steeds hoger wordt, wordt de inrichting van de security-functie (CISO) steeds relevanter. Maar voor kleine organisaties is daar vaak geen fulltime budget voor. Vandaar dat steeds meer organisaties de CISO-functie parttime aan ons uitbesteden. Inmiddels hebben al diverse collega's daarvoor relevante certificaten gehaald of zijn daartoe onderweg.

Capture the Flag ('CTF')

Eens in de zoveel jaren nodigen we beveiligings-expert Henk van Ee uit om ons uit te dagen om te leren denken als een hacker. In verschillende teams gingen we onderling aan de slag met uitdagende opdrachten om door te hacken 'geheime' informatie te achterhalen. Toch verrassend hoe creatief je kunt worden als je wordt uitgedaagd om buiten de normale kaders te gaan denken.

Advanced in AI auditor ('AAIA')

Information auditors met een CISA-titel kunnen sinds dit voorjaar hun titel uitbreiden met de AAIA-titel. Gezien alle ontwikkelingen is het verkrijgen van skills op het gebied van AI-auditing ook voor onze organisatie relevant. Vandaar dat we deze titel nu ook in huis hebben en kritisch naar uw AI-governance of AI-operaties kunnen kijken. Uiteraard blijft de essentie vooral kritisch nadenken. Maar AI brengt wel nieuwe risico's en nieuwe inzichten over beheersing met zich mee.

Cyber Ellende PubQuiz (CEPQ 2026)

Ook deze zomer gaan we weer het land in met de inmiddels beroemde cyberellende pubquiz. Want het is belangrijk dat we ondanks alle zorgen rondom de beheersing van technologische risico's ook vrolijk en optimistisch kunnen blijven.

Tot slot

Als we dan ook nog even aan DORA refereren, dan maken we de lettersoep compleet: AAIA, CTF, CEPQ, BCP, DORA, Cbw, NIS2 en zo kunnen we doorgaan. U kunt er in elk geval op vertrouwen dat wij voor u het overzicht zullen blijven behouden. Wij zijn gecommitteerd om hierin te blijven investeren en we doen ons best!

Verder hebben we in deze editie ook nog wel ander leuk nieuws en graag wil ik ook Centramed bedanken voor hun bijdrage aan ons magazine. Ik hoop dat u er met net zo veel plezier in leest als wij!

Ronald van de Langenberg

Algemeen directeur



Inhoud

4

Interview

Elles van Dijkman en
Laurien Jonkman
Centramed

8

Artikel

ISAE 3402

10

Artikel

De nieuwe regels voor
loontransparantie:
is uw beloningsbeleid uitlegbaar?

13

Klantevaluatie 2025

14

InAudit in beeld

16

Interview

Danny Francken
Instituut van Internal Auditors

20

Artikel

De overheid kan iets leren
van de aanpak van risico's
in het bedrijfsleven

22

Artikel

Nieuwe fase in de strijd
tegen witwassen

24

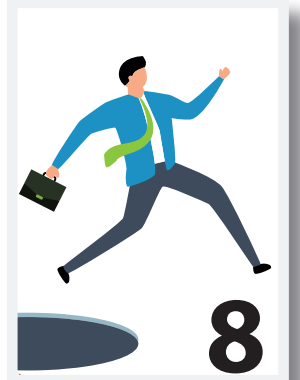
De wereld van ...

Floris Stokkers

27

Artikel

Afstudeerstage:
Integrale Veiligheidskunde



Ketenkracht in de zorg

Hoe Centramed preventie, schadebehandeling en kennis verbindt.

Medische aansprakelijkheid gaat altijd over mensen. Over vertrouwen, zorgvuldigheid en eerlijke oplossingen. Centramed is de verzekeraar die dat principe in de praktijk brengt. Samen met twee mensen uit het hart van de organisatie, Elles van Dijkman en Laurien Jonkman, ga ik in gesprek over drie pijlers: preventie, schadebehandeling en de rol als kenniscentrum.

Wie is Centramed en wat maakt jullie bijzonder als verzekeraar?

Centramed is een onderlinge waarborgmaatschappij. Dat betekent: Centramed is er "van, voor en door haar leden". Onze leden zijn grote zorginstellingen. Ziekenhuizen, ggz-instellingen en andere zorgaanbieders. Wij verzekeren medische aansprakelijkheidsrisico's voor onze leden. Als er een claim bij ons binnenkomt, onderzoeken we of een zorgverlener aansprakelijk is. Kernvraag hierbij is of het fout is gegaan of dat het fout is gedaan. Als er foutief is gehandeld, kijken we vervolgens naar de causaliteit, dus wat is de relatie tussen de gemaakte fouten en de gevolgen? Dat maakt ons zeer gespecialiseerd. We hebben geen winstoogmerk. Alles wat we doen, doen we voor de leden en daarmee voor hun patiënten en/of cliënten.

We behandelen claims zorgvuldig en proberen tegelijk de doorlooptijd te verkorten. Dat klinkt

vanzelfsprekend, maar het is in de praktijk een uitdaging. Een medische aansprakelijkheidsclaim duurt nu eenmaal langer, dan een gewone aansprakelijkheidsclaim. We streven ernaar aan alle betrokkenen zo snel mogelijk duidelijkheid te geven.

Preventie

Welke rol speelt preventie binnen jullie werk?

Preventie begint bij inzicht, voor ons en onze leden. We kunnen veel informatie afleiden uit de claims die binnenkomen. Via dashboards geven we leden inzicht in claimpatronen. Welke afdeling? Welke expertise? Welke trend? Dat helpt leden om hun eigen processen te verbeteren.

Leden kunnen bij ons ook een Quick Scan aanvragen. Tijdens de Quick Scan kijken onze

Naam: Laurien Jonkman
Functie: Bestuurssecretaris / Compliance Officer
Bedrijf: Centramed

mr. L.S. (Laurien) Jonkman is bestuurssecretaris en compliance officer bij Centramed. Ze houdt zich bezig met juridische en governance-vraagstukken maar niet met claimbehandeling. Denk aan de inrichting van de tweede en derde lijn en compliance-gerelateerde dossiers. Als lid van het managementteam is ze betrokken bij de strategische koers van Centramed.



preventiespecialisten samen met het lid naar het totale klacht-claimproces: van eerste signaal tot afhandeling. We bieden daarmee overzicht en advies over het huidige proces en het lid krijgt direct toepasbare verbeterpunten. Dit levert een kwaliteitsvergroting van de processen op en uiteindelijk ook een kostenbesparing. Minder claims, lagere schadelast.

Wat levert preventie de leden concreet op?

Uiteraard leidt preventie tot lagere kosten. Daarnaast is een patiënt die een klacht heeft, vaak nog steeds verbonden aan diezelfde zorginstelling. Die moet er soms nog terugkomen voor verdere behandeling. Als kan worden voorkomen dat de vertrouwensband wordt geschaad, helpt dat in de verdere behandeling. Preventie beschermt dus niet alleen de financiën van de zorginstelling, het ondersteunt ook in het behoud van de relatie met de patiënt.

Preventie bij Centramed

- Dashboards geven leden inzicht in claimpatronen per afdeling of expertise.
- Quick scans helpen bij het omzetten van klachten naar preventieve maatregelen.
- Doel: minder claims, lagere kosten en behoud van de vertrouwensband met patiënten.

Schadebehandeling

Hoe ziet een claimbehandeling er bij Centramed uit?

We zijn bij de behandeling van een claim, als verzekeraar, de spin in het web. Onze leden hebben hoge eigen risico's en daardoor trekken we echt samen met hen op. We nemen hen mee

in het proces en in het oordeel, de medische kennis van de leden is essentieel. Daarnaast schakelen we gespecialiseerde medisch adviseurs in. Dat zijn vakgenoten. Bij een claim op gynaecologie vragen we een gynaecoloog als medisch adviseur. Geen generalist. Onze juristen doen vervolgens de juridische beoordeling van de ingediende claim. Zo kom je tot een zorgvuldig en goed oordeel.

Hoe zorgen jullie ervoor dat de keten goed op elkaar aansluit?

Elk lid heeft een vaste schadecontactpersoon bij Centramed. Eén aanspreekpunt, altijd. In ons schadehandboek staat vastgelegd wanneer we een lid informeren. Denk aan een reservewijziging, of het voornemen om aansprakelijkheid te erkennen. Dan nemen we altijd eerst contact op met het lid. De zorgverlener moet op de hoogte zijn voordat het standpunt aan de belanghebbende wordt gecommuniceerd.

We hebben ook contactpersonen bij de grote rechtsbijstandsverzekeraars, zoals DAS en ARAG. Dat houdt de lijnen kort. Zaken worden laagdrempeliger besproken waardoor eventuele escalatie wordt voorkomen.

Waarom bieden jullie een huisbezoek aan elke claimant?

Medische aansprakelijkheid is een complex, juridisch proces. Iemand gaat bijvoorbeeld naar het ziekenhuis met een aandoening en komt er soms slechter uit. De beoordeling is dan ingewikkeld: welke schade is toe te wijzen aan het handelen van de zorginstelling? Minstens zo belangrijk is: iemand heeft iets naars meegemaakt. Dat laat sporen achter. Vertrouwen in de zorg kan beschadigd zijn. Dat vraagt aandacht en ruimte voor emotie.

Naam: Elles van Dijkman
Functie: Manager Schade
Bedrijf: Centramed

Mr P.A.J.M. (Elles) van Dijkman is één van de twee managers Schade bij Centramed. Zij is verantwoordelijk voor de operationele uitvoering van de claimafhandeling. Ze stuurt het team van schadebehandelaars aan en bewaakt de kwaliteit van het claimproces. Ze is betrokken bij de onboarding van nieuwe leden en de samenwerking met externe partijen. Als lid van het managementteam is zij betrokken bij de strategische koers van Centramed.





Kantoor
Centramed
Zoetermeer

Conform de GOMA bieden we bij elke claimant een huisbezoek aan. De GOMA staat voor Gedragscode Openheid Medische Incidenten: Betere Afwikkeling Medische Aansprakelijkheid. Het is de gedragscode voor verzekeraars en zorginstellingen bij medische aansprakelijkheid. Een expert Personenschade komt bij de patiënt thuis om in alle rust het persoonlijke verhaal te horen. Niet alleen om het proces toe te lichten. Juist ook om de mens te horen. We zijn dan het visitekaartje van de instelling waar het incident plaatsvond.

Dit past ook bij ons als organisatie. Mensgericht handelen is een kernwaarde. Het staat in de GOMA, maar het past ook bij hoe wij een claim willen behandelen.

Claimbehandeling bij de zelfregelende ziekenhuizen

Een aantal grote ziekenhuizen heeft een zelfregelende bevoegdheid. Dat betekent dat ze onder supervisie van Centramed zelfstandig claims mogen afhandelen. De gedachte is simpel: hoe dichterbij je bij de patiënt staat, hoe beter het is. Die ziekenhuizen hebben eigen gespecialiseerde juristen. Ze handelen een claim af conform onze voorwaarden. Ook zij werken volgens de GOMA. Het borgen van de kwaliteit van claimbehandeling is een harde eis.

Om de kwaliteit te bewaken doen we eens in de drie jaar een externe audit. We lichten dossiers door en toetsen het proces. Hoe is het proces georganiseerd? Zijn de afspraken nageleefd? Daarnaast doet elk zelfregelend ziekenhuis jaarlijks een self-assessment op eigen dossiers.

Zelfregelende ziekenhuizen

- Grote ziekenhuizen behandelen claims zelfstandig, onder supervisie van Centramed.
- Behandeling conform afgesproken voorwaarden én de GOMA-gedragscode.
- Externe audit eens per drie jaar op kwaliteit van de claimafhandeling.
- Jaarlijks self-assessment door het ziekenhuis zelf.
- Voordeel: de instelling staat dichterbij de patiënt en kan sneller en persoonlijker handelen.

Kenniscentrum

Hoe ziet Centramed zichzelf als kenniscentrum voor de leden?

Wij stimuleren onze overige leden die geen zelfregelende bevoegdheid hebben, om kleine claims laagdrempelig zelf op te lossen. Als je in het ziekenhuis het gesprek met de patiënt aangaat, sta je dichterbij de mens. Zodra een claim bij een verzekeraar belandt, juridiseert het snel. Wij helpen leden daarin door onze kennis te delen. We organiseren ook regelmatig diverse webinars en masterclasses voor onze leden. Daarnaast kunnen zij altijd met ons sparren over aansprakelijkheid.

Hoe houden jullie de kennis op peil?

We hebben vakgroepen binnen Centramed. Zo is er een vakgroep 'Grote claims'. Daarin bespreken we grote letselschadedossiers en delen we expertise en inzichten met elkaar. Neem bijvoor-

Over Centramed

Centramed is een onderlinge waarborgmaatschappij zonder winstoogmerk, gevestigd in Zoetermeer. De organisatie verzekert ruim 80 grote ziekenhuizen, ggz-instellingen en andere zorgaanbieders, tegen het risico van medische aansprakelijkheid. Centramed telt ruim 70 medewerkers en opereert vanuit vier kernwaarden: mensgericht, actief, zorgvuldig en van, voor en door leden. Meer informatie:

www.centramed.nl

beeld geboorteschade, permanent letsel bij een pasgeborene. Dat komt gelukkig weinig voor, maar als het speelt, is de impact groot. Wij zien dit soort claims van diverse instellingen, terwijl een ziekenhuis deze misschien eens in de vier of vijf jaar treft. Dan is het verschil in kennis en ervaring aanzienlijk. Wij hebben die expertise in huis en zetten deze in voor onze leden. Verder hebben we een eigen opleider voor nieuwe medewerkers. Die begeleidt de onboarding inhoudelijk. Er zijn dossieroverleggen, kennismiddagen en een maandelijks overleg geleid door de kennismanager. Onze advocaten houden jurisprudentie bij en delen dat actief met collega's en leden.

Welke actuele thema's zien jullie terugkomen?

Actueel is de Rotterdamse Schaal. Dat is de nieuwe richtlijn voor smartengeld waardoor de eerder gebruikte ANWB Smartengeldgids nu achterhaald is. Belangenbehartigers halen in actuele claims de Rotterdamse Schaal veel aan. We bereiden leden hierop voor.

Kennisactiviteiten voor leden

- Masterclasses: o.a. Rotterdamse Schaal, AI in de zorg, werkgeversaansprakelijkheid.
- Webinars over actuele thema's zoals agressie in de zorg.
- Jurisprudentieoverleg: advocaten delen actualiteiten met medewerkers en leden.
- Kennismiddagen en dossieroverleggen voor kennisdeling binnen Centramed.
- Interne vakgroepen per thema, zoals 'grote claims', werkgeversaansprakelijkheid en zelfstandigen-/overlijdensschades.

Als we kijken naar het klacht-claimproces zien we dat zorginstellingen bijvoorbeeld steeds meer te maken krijgen met AI-gegenereerde correspondentie. Klachtfunctionarissen zien dat daardoor dossiers uitgebreider worden en soms lastiger te behandelen. Fraude (via AI) zien we nauwelijks in de ingediende claims. Dat heeft te maken met de aard van medische aansprakelijkheid waarvan de oorsprong altijd ligt in een medische behandeling door de zorginstelling.

Agressie in de zorg baart ons zorgen. Bij ziekenhuizen én ggz-instellingen neemt de agressie tegen zorgpersoneel toe. Dat zien we terug in claims op het gebied van werkgeversaansprakelijkheid. Wij brengen leden met elkaar in contact, organiseren webinars en geven dit signaal door. De oplossing hebben wij helaas niet. Aan de hand van onze claims maken we zichtbaar dat dit een groeiend maatschappelijk probleem is.

Centramed staat, als onderlinge verzekeraar, naast hun leden om medische aansprakelijkheid claims zorgvuldig te behandelen en streeft naar een voor alle partijen eerlijke oplossing.



ISAE 3402

Wat moet je er mee?

Een assurance-rapport is geen vinkje. Het is een instrument, maar alleen als je weet hoe je het moet lezen. Veel financiële instellingen hebben het afgelopen jaar flink geïnvesteerd in DORA-implementatie. Beleid staat op papier, leveranciers zijn geregistreerd en we kijken naar hun IT-security door middel van het ISAE 3402-rapport.

Maar wat staat er eigenlijk in zo'n rapport? En wat zegt het en wat zegt het níet?

Die vragen zijn urgenter dan ze klinken. Want de NBA, NOREA en IIA Nederland waarschuwen in hun gezamenlijke publicatie Vertrouwen in de kwetsbare keten (2026) voor een hardnekkig misverstand: bestuurders verwachten soms méér zekerheid van assurance-rapporten dan die rapporten kunnen bieden.

“ Assurance geeft slechts zekerheid over een afgebakend deel van de werkelijkheid en over een specifieke periode. Niet over de keten als geheel.

NBA, NOREA & IIA Nederland,
Vertrouwen in de kwetsbare keten, 2026

”

bestaan én werken. Het rapport is bedoeld voor klanten van die leverancier zodat zij kunnen steunen op de bevindingen.

Er zijn twee varianten. Een type I geeft een oordeel over de opzet op één moment. Een type II gaat verder: die beoordeelt ook de werking over een periode van minimaal zes maanden. Voor grip op uitbestede risico's is een type II dus aanzienlijk waardevoller.

Wat een ISAE 3402-rapport je vertelt

Een ISAE 3402-rapport geeft inzicht in hoe een leverancier kritieke processen beheerst die de financiële verantwoording raken. Denk aan toegangsbeheer, wijzigingsbeheer, back-up en herstel, incidentopvolging en functiescheiding. Processen die verband houden met de financiële verantwoordingen.

Wat is een ISAE 3402-rapport?

ISAE 3402 is een internationale standaard voor assurance bij uitbestede diensten. Een externe accountant of IT-auditor onderzoekt of de beheersmaatregelen bij een serviceleverancier

De waarde zit in drie dingen: het geeft een grondslag voor je leveranciersbeoordeling, het biedt aanvullende zekerheid over specifieke onderdelen, en het levert gespreksstof op met de leverancier, met interne audit en met het bestuur.

ISAE 3402 in de PDCA-cyclus

Plan

- Stel eisen aan assurance per kritieke leverancier
- Leg scope-eisen vast in leveranciersbeleid
- Betrek interne audit vooraf bij de risicoanalyse

Internal audit: adviseert over scope en criteria

DO

- Bevorder het opstellen van ISAE 3402 rapportages door kritieke leveranciers
- Registreer ontvangen security rapportages in het informatieregister
- Controleer of het rapport type II is en actueel
- Sla het rapport op, klaar voor inhoudelijke review

Internal audit: toetst of proces wordt gevolgd

Act

- Ga in gesprek over mogelijke verbeteringen
- Beslis: aanvullende assurance of contract-aanpassing
- Rapporteer restrisico's aan bestuur en compliance
- Gebruik leerpunten voor volgende Plan-fase

Internal audit: bewaakt opvolging van bevindingen

Check

- Beoordeel scope: wat valt er buiten?
- Analyseer bevindingen en uitzonderingen
- Toets of gebruikerscontroles intern zijn belegd
- Koppel conclusies aan eigen risicoanalyse

Internal audit: onafhankelijke toets op de review

De vier valkuilen bij assurance-rapporten

1 Scope: wat valt er buiten?

Welke diensten, systemen, locaties en onderaannemers zijn expliciet uitgesloten? Als iets niet is onderzocht, heb je geen zekerheid. En in hoeverre is het relevant voor het product of dienst dat je afneemt?

3 Carve-outs: wat is weggelaten?

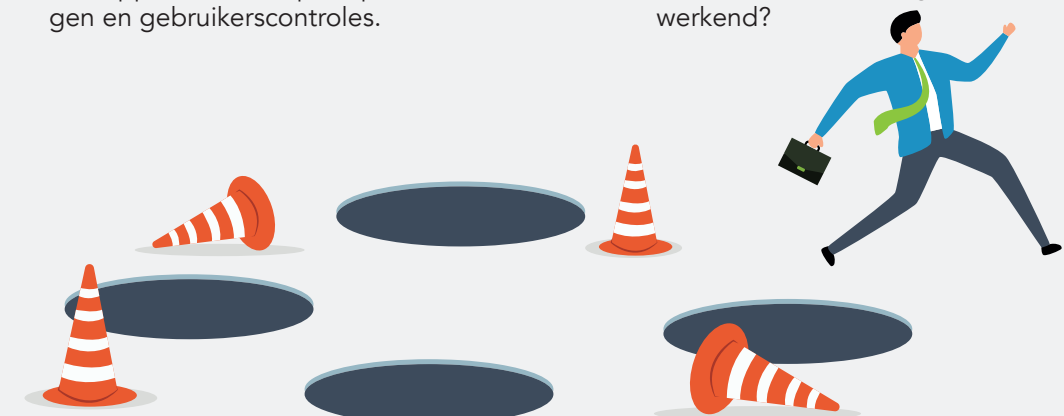
Delen van de dienstverlening kunnen buiten het onderzoek zijn gebleven. Lees het rapport kritisch op scope, uitsluitingen en gebruikerscontroles.

2 Periode: hoe oud is de informatie?

De rapportages kijken terug, maar hoe is het nu? Tussen het einde van de onderzochte periode en het moment van publicatie kunnen nieuwe risico's zijn ontstaan.

4 Gebruikerscontroles: uw eigen verantwoordelijkheid

Veel rapporten benoemen maatregelen die u zelf moet uitvoeren. Zijn deze inderdaad intern belegd en aantoonbaar werkend?



Wat een ISAE 3402-rapport je níet vertelt

Hier gaat het in de praktijk vaak mis. Een ISAE 3402-rapport dekt altijd een afgebakende scope en periode. Wat buiten die scope valt, is niet beoordeeld en dat kan veel zijn. Onderaannemers van de leverancier vallen er vaak buiten. Crisismanagement, exitplannen en cyberveerkracht ook. Het rapport gaat over de afgelopen periode, maar de wereld is dynamisch.

Geen DORA-vinkje

De belangrijkste valkuil is dat een ISAE 3402-rapport wordt gezien als bewijs dat de leverancier "DORA-compliant" is. Dat is het niet. ISAE 3402 is geen DORA-certificaat. Het is ook geen algemene verklaring dat een leverancier volledig in control is. De bruikbaarheid hangt volledig af van de scope, de periode, de onderzochte beheersdoelstellingen, de uitkomsten van de testwerkzaamheden en de relevantie voor uw eigen risicoanalyse.

Een assurancerapport is geen eindpunt

Een rapport ontvangen is niet hetzelfde als grip hebben. De NBA, NOREA en IIA zijn hier helder over: assurance is een hulpmiddel, geen garantie. Het vergroot vertrouwen waar dat kan maar het neemt onzekerheid niet weg en vervangt het eigen oordeel nooit.

De betere vraag is dus niet: "Hebben wij een ISAE 3402-rapport ontvangen?", maar: "Wat leert dit rapport ons over de werking van onze ketenbeheersing, en wat verbeteren we in de volgende cyclus?"

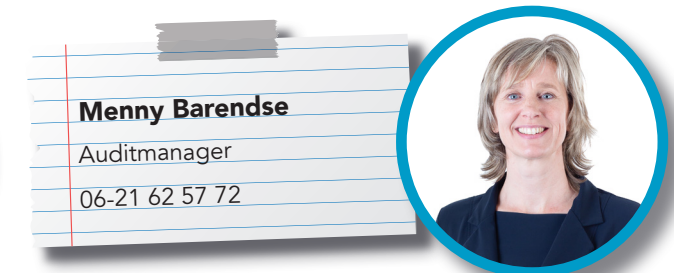
Juist daar ligt de meerwaarde van een goede interne auditfunctie: onafhankelijk toetsen, scherp doorvragen en helpen voorkomen dat aanvullende zekerheid wordt verward met volledige zekerheid.



Yorick Harmsen

Senior auditor

06-29 43 44 00



Menny Barendse

Auditmanager

06-21 62 57 72

De nieuwe regels voor loontransparantie: is uw beloningsbeleid uitlegbaar?

Wat de nieuwe regels betekenen voor werknemers, werkgevers en de inrichting van beloningsbeleid. De Europese Richtlijn loontransparantie is op 7 juni 2023 in werking getreden. Deze richtlijn heeft als doel om het recht van werknemers op gelijke beloning van mannen en vrouwen voor gelijk of gelijkwaardig werk beter zichtbaar en eenvoudiger afdwingbaar te maken. In Nederland wordt deze richtlijn geïmplementeerd via de Wet implementatie Richtlijn loontransparantie mannen en vrouwen. Het wetsvoorstel bevindt zich in de nationale implementatiefase, maar de richting is duidelijk: werknemers krijgen meer inzicht in beloning en werkgevers moeten beter kunnen uitleggen hoe beloning tot stand komt. Volgens de Rijksoverheid treedt het wetsvoorstel naar verwachting op 1 januari 2027 in werking.

Loontransparantie raakt daarmee aan een onderwerp dat in iedere organisatie speelt: hoe wordt bepaald wat iemand verdient? In veel organisaties is daar beleid voor. Er zijn functieprofielen, salarisschalen, cao-afspraken of interne richtlijnen. Toch is de praktijk vaak minder eenduidig dan het beleid op papier. Een medewerker kan in de loop der jaren anders zijn ingeschaald dan een collega. Een markttoeslag kan ooit terecht zijn toegekend, maar daarna nooit opnieuw beoordeeld. Of functies met vergelijkbare werkzaamheden kunnen in verschillende onderdelen van de organisatie anders zijn beschreven.

Voor werkgevers betekent dit dat loontransparantie niet alleen vraagt om kennis van nieuwe wetgeving, maar ook om inzicht in de werking van het eigen beloningsproces. Dat is relevant voor HR, maar ook voor het bestuur, finance, compliance, risk, privacy én interne audit. De vraag is immers niet alleen of beleid bestaat, maar ook of de organisatie kan aantonen dat dit beleid zorgvuldig, objectief en consistent wordt toegepast.

Doel en belangrijkste verplichtingen

De Richtlijn loontransparantie moet ongelijke beloning zichtbaar en bespreekbaar maken. Werknemers krijgen daarom meer recht op informatie over hun eigen loon en over gemiddelde beloningsniveaus van collega's die hetzelfde, of gelijkwaardig werk doen. Dat betekent niet dat individuele salarissen openbaar worden, maar wel dat organisaties moeten kunnen uitleggen hoe beloning tot stand komt en waardoor verschillen worden veroorzaakt.

Ook voor sollicitanten verandert de informatiepositie. Werkgevers moeten transparanter worden over de beloning of beloningsband-

breedte van een functie. Daarnaast wordt het verboden om sollicitanten te vragen naar hun salarisgeschiedenis, zodat mogelijke eerdere loonverschillen niet worden meegenomen naar een nieuwe werkgever.

Voor werkgevers betekent dit dat beloningsbeleid minder impliciet kan blijven. Zij moeten beschikken over loonstructuren met objectieve, genderneutrale criteria. Denk aan criteria zoals relevante ervaring, opleidingsniveau, functie-zwaarte, verantwoordelijkheden, prestaties of arbeidsomvang, mits deze criteria vooraf duidelijk zijn, consequent worden toegepast en niet direct of indirect tot onderscheid naar geslacht leiden. Volgens de Rijksoverheid wordt een systeem van functiewaardering en -indeling verplicht voor alle werkgevers na implementatie van de Europese richtlijn. Werkgevers met 100 werknemers of meer krijgen daarnaast een rapportageplicht over loonverschillen binnen de organisatie. Voor werkgevers met 100 tot en met 249 werknemers geldt deze verplichting eens per drie jaar. Werkgevers met 250 of meer werknemers moeten jaarlijks rapporteren. Als uit een rapportage blijkt dat beloningsverschillen niet goed te verklaren zijn, kan dit leiden tot aanvullende analyse en verbetermaatregelen, zoals een gezamenlijke loonbeoordeling.

Een eenvoudig voorbeeld maakt dit concreet. Als een werknemer vraagt waarom een collega in een vergelijkbare functie een hoger salaris ontvangt, zal een algemene verwijzing naar "historie" of "individuele afspraken" in veel gevallen onvoldoende zijn. De organisatie moet kunnen terugvallen op een heldere functie-indeling, objectieve beloningscriteria en betrouwbare gegevens. Is het verschil niet objectief en genderneutraal te verklaren, dan ontstaat een verbeterpunt.

De organisatie moet dan kunnen vastleggen en, waar nodig, onderbouwen hoe dit is beoordeeld en opgevolgd richting de daarvoor aangewezen partijen, zoals de betrokken werknemer, de ondernemingsraad of een bevoegde instantie.

Handreiking Loonstructuren

Om werkgevers te helpen deze verplichtingen praktisch te vertalen naar hun eigen organisatie heeft de Rijksoverheid op 15 april 2026 de handreiking "Systeem van functiewaardering en -indeling (loonstructuur)" gepubliceerd, met een checklist voor werkgevers. De handreiking en checklist zijn in opdracht van het ministerie van Sociale Zaken en Werkgelegenheid ontwikkeld en helpen werkgevers bij het inrichten of beoordelen van een systeem voor functiewaardering en -indeling.

De handreiking vormt daarmee een praktisch vertrekpunt voor organisaties die hun loonstructuur willen ontwerpen, beoordelen of aanscherpen. Een loonstructuur gaat over de manier waarop wordt bepaald wat een functie waard is en welke beloning daarbij hoort. Denk aan functi omschrijvingen, functiewaardering, functie-indeling, salarisschalen of salarisbandbreedtes en de criteria die worden gebruikt voor inschaling en salarisontwikkeling.

De handreiking helpt bij het ontwerpen of beoordelen van zo'n structuur. De echte toets ligt vervolgens in de toepassing. Want een loonstructuur heeft pas waarde als deze actueel is, consequent wordt gebruikt en goed is ingebed in de organisatie. Dat betekent bijvoorbeeld dat duidelijk moet zijn wie functieprofielen beheert, wie uitzonderingen mag goedkeuren, hoe markttoeslagen worden vastgelegd en wanneer beloningsafspraken opnieuw worden beoordeeld.

Van regels naar beheersing in de praktijk

De handreiking helpt vooral bij de vraag hoe een loonstructuur eruit kan zien; de implementatie vraagt vervolgens om governance, datakwaliteit, besluitvorming en periodieke monitoring. De impact van loontransparantie wordt daarom vooral zichtbaar in de dagelijkse uitvoering. Veel organisaties hebben een salarishuis, maar dat salarishuis sluit niet altijd volledig aan op de praktijk. Functietitels kunnen per afdeling verschillen. Rollen groeien door de tijd heen, zonder dat het functieprofiel wordt aangepast. Nieuwe medewerkers worden soms anders ingeschaald dan bestaande medewerkers, bijvoorbeeld door arbeidsmarktdruk. Ook kunnen uitzonderingen ontstaan die op zichzelf verklaarbaar zijn, maar later moeilijk zijn terug te vinden of te onderbouwen.

Loontransparantie in 6 stappen

Van regelgeving naar aantoonbaar uitlegbaar beloningsbeleid



Daarmee wordt loontransparantie ook een vraagstuk van interne beheersing. Het gaat niet alleen om de aanwezigheid van beleid, maar om de inrichting van processen, data, verantwoordelijkheden en monitoring. Wie is eigenaar van de loonstructuur? Hoe worden functies gewaardeerd? Wie beoordeelt uitzonderingen? Hoe wordt gecontroleerd of beloningscriteria consequent worden toegepast? En hoe wordt omgegaan met signalen dat verschillen mogelijk niet goed verklaarbaar zijn?

Naast beleid, processen en data speelt ook gedrag een belangrijke rol. Loontransparantie vraagt om een organisatie waarin beloningskeuzes zorgvuldig worden gemaakt en uitgelegd. Leidinggevendenden moeten weten welke criteria zij moeten toepassen, welke ruimte zij hebben voor maatwerk en hoe zij vragen van medewerkers op een consistente manier beantwoorden. Als afspraken verschillend worden toegepast, kan er alsnog verschil ontstaan tussen het beleid op papier en de praktijk.

Deze vraagstukken maken het onderwerp relevant voor interne audit. Interne audit bepaalt het beloningsbeleid niet, maar kan wel toetsen of het proces erachter goed is ingericht. Voor bestuur, directie en audit committee is het belangrijk om te weten of de organisatie in staat is om beloningsvragen zorgvuldig te beantwoorden. Zijn de gegevens betrouwbaar? Worden criteria consequent toegepast? Zijn uitzonderingen goed vastgelegd? En is privacy voldoende geborgd?

Betrouwbare gegevens en privacy

Goede datakwaliteit is daarbij essentieel om beloningsverschillen betrouwbaar te kunnen analyseren en uitleggen. Beloningsinformatie staat vaak verspreid over HR-, payroll- en finance-systemen. Denk aan functiegegevens, arbeidsduur, toeslagen, variabele beloning en historische afspraken. Als deze gegevens niet volledig of niet op dezelfde manier zijn vastgelegd, worden analyses en rapportages minder betrouwbaar.

Ook privacy vraagt om duidelijke afspraken. Meer transparantie betekent niet dat salarisinformatie zomaar gedeeld kan worden. De Raad van State wijst op het belang van waarborgen om te voorkomen dat informatie direct of indirect herleidbaar is tot een individuele werknemer. Organisaties moeten daarom vooraf bepalen hoe zij omgaan met informatieverzoeken, welke gegevens gedeeld mogen worden en wie daarbij betrokken is. Denk aan afspraken over minimale groepsomvang, aggregatie van gegevens, autorisaties, logging, bewaartermijnen en een

vast procedure voor informatieverzoeken. Daarmee raakt loontransparantie niet alleen aan HR, maar ook aan interne beheersing en toezicht. De vraag is of een organisatie voldoende grip heeft op het proces achter beloning en dit ook kan aantonen. Dit vormt de brug naar de rol die interne audit hierbij kan spelen.

Wat kan InAudit betekenen?

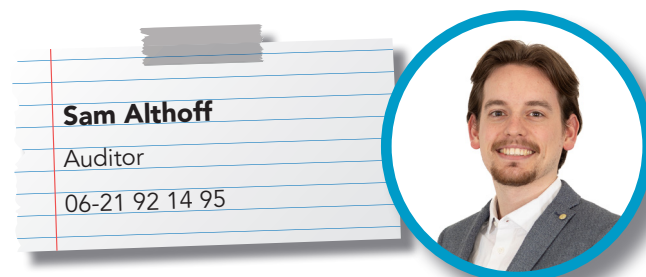
InAudit kan organisaties ondersteunen bij de voorbereiding op de nieuwe regels rond loontransparantie. Dat kan met een onafhankelijke readiness scan of met een thema-audit gericht op beloningsbeleid, functiewaardering, datakwaliteit, governance, privacy en interne beheersing. Daarbij kijken we niet alleen naar de aanwezigheid van beleid, maar vooral naar de inrichting en (beoogde) werking hiervan in de praktijk en stellen we vragen als:

- Is er een actueel en vastgesteld systeem voor functiewaardering en functie-indeling?
- Zijn beloningscriteria objectief, genderneutraal en aantoonbaar toegepast?
- Zijn uitzonderingen, toeslagen en afwijken-de inschalingen goedgekeurd en periodiek herbeoordeeld?
- Is de HR- en payrolldata volledig, juist en herleidbaar tot betrouwbare rapportages?
- Zijn privacywaarborgen ingericht bij informatieverzoeken van werknemers?

Afhankelijk van de organisatie kan de nadruk verschillen. Bij sommige organisaties ligt de focus op de inrichting en toepassing van de loonstructuur. Bij andere organisaties speelt vooral de betrouwbaarheid van HR- en payrollgegevens, de voorbereiding op informatieverzoeken of de rapportageplicht.

In alle gevallen staat dezelfde vraag centraal: kunt u uitleggen hoe beloning tot stand komt en aantonen dat dit proces zorgvuldig is ingericht?

Wij denken graag met u mee.



Klantevaluatie 2025

Hoe ervaren onze klanten de interne auditdienstverlening van InAudit Audit Services? Om dat te meten, vragen wij onze klanten jaarlijks een evaluatieformulier in te vullen. Daarin beoordelen zij niet alleen de inhoudelijke kwaliteit van onze dienstverlening, maar ook het samenwerkingsproces.

Deze inzichten helpen InAudit om zich continu te blijven ontwikkelen en onze werkwijze verder af te stemmen op de wensen van onze klanten.

Een gemiddelde waardering van 9,2

Vorig jaar waren we al zeer tevreden met een gemiddelde waardering van 9,1. De klantevaluatie van 2025 laat een nóg iets hogere score zien: gemiddeld een 9,2 over alle zes beoordelingscategorieën. De hoogste scores zijn toegekend aan het auditjaarplan (9,5) en de professionals van InAudit (9,4).

Klanten waarderen InAudit als een professionele, flexibele en persoonlijke partner met korte lijnen, vakinhoudelijke diepgang en bruikbare rapportages. Opvallend in 2025 is de nadruk op de menselijke kant van de samenwerking: wederzijds vertrouwen en de warme persoonlijke relatie worden dit jaar nadrukkelijker benoemd dan voorheen.

Ruimte om verder te groeien

Verbeterpunten richten zich vooral op verdere optimalisatie, zoals scherpere doorlooptijden, meer maatwerk en een proactievare adviserende rol. Tegelijkertijd zien klanten kansen in bredere kennisdeling, bijvoorbeeld via seminars en sectorinzichten.

En verder...

In 2025 is Thomas Pater gestart als junior auditor. Sam Althoff en Ruben Kamstra zijn doorgeschoold naar auditor. Yorick Harmsen is doorgeschoold naar senior auditor en Wessel Westerveld vervult bij een aantal klanten inmiddels de rol van auditmanager.

Namens het hele Team InAudit Audit Services: hartelijk dank voor uw betrokkenheid, waardering, feedback en blijvende samenwerking.



Klantevaluatie Interne Audit 2025

Zo beoordelen onze klanten de interne audit service van InAudit



Relatie met het Management

De auditmanager is een volwaardig gesprekspartner voor bestuursleden, de voorzitter van de auditcommissie en de sleutelfunctiehouders.

9,1

9,4

Professionals InAudit

De auditprofessionals zijn objectief en de samenwerking verloopt prettig en professioneel.



Het Audit jaarplan

Het audit jaarplan is duidelijk en biedt voldoende ruimte voor speciale verzoeken.

9,5

9,0

Het Audit proces

De scope van de audit is duidelijk afgestemd. De pragmatische en proportionale aanpak wordt gewaardeerd.



Het Audit rapport

Het auditrapport is helder en begrijpelijk. Aanbevelingen zijn bruikbaar voor de organisatie en kunnen concreet worden doorvertaald naar het bedrijfsproces.

9,0

9,0

Effectiviteit v/d Interne Audit

De interne auditfunctie draagt bij aan effectieve interne controles.



www.inaudit.nl

InAudit in beeld



De Internal Auditor: De vuurtoren van de organisatie

We spreken Danny Francken, algemeen directeur van IIA Nederland, in het gloednieuwe onderkomen van de vereniging in Breukelen, een lichte, ruime plek aan de Corridor, naast het station en de A2. Meer dan 600 m² vergaderzalen, focusruimtes en ontmoetingshoeken, nadrukkelijk bedoeld als clubhuis voor iedereen in het vakgebied. Het is een bewuste keuze, legt Francken uit, om Internal Audit zichtbaar te maken. Precies dat thema, zichtbaarheid, bekendheid, en wat het vak eigenlijk inhoudt, loopt als een rode draad door ons gesprek. En natuurlijk de samenwerking tussen IIA Nederland en InAudit.

Wat is Internal Audit eigenlijk en wat is het niet?

De verwarring met accountancy ontstaat natuurlijk snel. En als je denkt dat interne audit hetzelfde is als accountancy, of alleen maar financial audit, dan zit je niet helemaal op het juiste spoor.

Het vak kenmerkt zich eigenlijk door drie grote gebieden. Het eerste is operational audit, waarbij je veel meer naar de processen kijkt en de beheersingsmaatregelen rondom die processen. Het tweede is IT-audit, alles wat met IT te maken heeft, infrastructuur, maar ook dreigingen. Denk aan externe invloeden waar je wellicht minder grip op hebt, maar ook invloeden van binnenuit. Als een medewerker zomaar AI gaat gebruiken zonder dat goed af te schermen, liggen al je gegevens op straat. Realiseert men zich dat wel? Dat stukje IT-audit zit dus gewoon in Internal Audit. En het laatste is financial audit, waarbij je anders dan een accountant naar financiële processen kijkt. Niet zozeer puur naar de cijfers,

maar naar hoe die cijfers tot stand komen. Welk proces ligt daar nou onder?

En dan is er eigenlijk geen enkel ander vakgebied dat zo breed kijkt en zo bijdraagt aan de doelstellingen van een organisatie als interne audit. Een externe accountant kijkt alleen of de cijfers die zijn aangeleverd kloppen. Je hebt een miljoen verlies gemaakt, maar perfect geadmistreerd, prima, dan is de jaarrekening in orde. Internal Audit zorgt er eigenlijk voor dat dat miljoen verlies überhaupt niet tot stand komt. Want zij zitten aan de vooravond van dat proces.

Als Internal Auditor ben je als onderdeel van het bedrijf ook medeverantwoordelijk voor de resultaten van het bedrijf. En dat is een vrij unieke positie. Je bent onafhankelijk, je rapporteert aan de baas van de baas, maar je zorgt er ook voor, niet als politieagent, maar als collega die helpt om processen te verbeteren zodat ze beter bijdragen aan het bedrijfsresultaat. Hoe mooi is dat?

Danny Francken in het nieuwe pand in Breukelen.



Je noemt het vakgebied ook wel de Vuurtoren van de organisatie. Wat bedoel je daarmee?

Kijk, je bent eigenlijk net als een vuurtoren. Je belicht de omgeving in 360 graden en je waarschuwt op voorhand voor mogelijke risico's. Je geeft richting aan, maar de stuurman is verantwoordelijk voor de verandering van richting. Je bent een onafhankelijk baken voor de organisatie, terwijl je mede verantwoordelijk bent voor de veilige thuiskomst (het bedrijfsresultaat).

Wat het vakgebied zo onwils krachtig maakt, is het totaaloverzicht. Iemand die op een afdeling werkt, weet precies hoe het op zijn afdeling werkt, maar snapt eigenlijk al niet zo goed hoe dat op de volgende afdeling gaat. Dan kom je al bij de manager terecht. Die denkt misschien: als ik iets verkoop, moet finance dat afhandelen en daar houdt het voor hem dan mee op. Maar dat is niet het enige. Er zit een hele productieafdeling achter, een magazijn, een logistiek apparaat, misschien legal. Dat besef is vaak heel beperkt.

Als Internal Auditor begrijp je het complete proces. Eigenlijk net zo goed als een algemeen directeur dat begrijpt. En dan moet je ook goed je mannetje kunnen staan. Niet alleen analytisch, maar ook goed kunnen verwoorden, en zorgen dat mensen jou de informatie geven die bijdraagt tot het behalen van die doelstellingen. Zonder dat je als politieagent wordt gezien, want dat is natuurlijk de valkuil.

Hoe scoort Nederland als je het vak vergelijkt met andere landen?

Wij zijn koploper. Het IIA zit momenteel in 122 landen en 50 staten, en we bestaan 80 jaar. We zijn één van de grootste wereldwijde beroepsverenigingen die ook internationaal standaarden uitgeeft, standaarden die in heel veel landen wettelijk verankerd zijn.

Binnen Europa zijn 35 landen verenigd in de ECIA, de Europese groep. En binnen die 35 landen is Nederland een top vijf land. Wereldwijd zitten we denk ik zelfs nog hoger.

Nederland is een ontzettend volwassen auditland. Wij doen dingen terwijl andere landen nog moeten beginnen met nadenken over wat wij hier al lang verankerd hebben. We hebben een stevig kwaliteitstoetsingsstelsel, elke auditfunctie moet elke vijf jaar worden getoetst op de standaarden. Maar in Nederland gaan we nog een stap verder: we hebben een toezichtsorgaan op de kwaliteitstoetsingen zelf. Wij toetsen de toetsers. Daarin zijn wij uniek, geen enkel ander land ter wereld doet dat.

In de Arabische wereld is er momenteel enorm veel focus op Internal Audit; het wordt daar in wet- en regelgeving verankerd. En ze huren Nederlanders in om die afdelingen vorm te geven, omdat Nederland bekendstaat als het meest vooruitstrevende toetsingsland ter wereld.

Naam: Danny Francken MA IAP CIA
Functie: Algemeen Directeur
Bedrijf: Instituut van Internal Auditors

Het Instituut van Internal Auditors Nederland (het IIA) is de grootste beroepsvereniging van Internal Auditors in Nederland. De vereniging telt zo'n 3000 leden. Het IIA is gelieerd aan de veel oudere, wereldwijde organisatie The Institute of Internal Auditors Inc. (IIA Inc.) die meer dan 270.000 leden telt in 122 landen. Het motto van IIA Inc. is 'Progress through Sharing'.



Waar liggen de blinde vlekken. In welke sectoren ontbreekt Internal Audit nog?

In de financiële sector is Internal Audit goed verankerd, mede door DNB. Maar er zijn heel veel sectoren die een bepaalde governance code naleven. In Nederland hebben we ook de corporate governance code, en daarin is Internal Audit redelijk verankerd maar niet iedereen volgt die code. In de zorg, bijvoorbeeld, hebben ze een eigen code. Als Internal Audit daar minder verankerd is, is dat geen blinde vlek maar een kans. De onbekendheid van de materie speelt daarin een grote rol.

Wat we nu gaan doen, is de Dag van de Waterschappen, een activiteit die ik samen met InAudit onderneem. We gaan met name laten zien wat de Internal Audit functie kan toevoegen aan de bedrijfsvoering van een waterschap. Vaak zijn dat partijen die te klein zijn voor een eigen interne afdeling. Voor hen is het heel waardevol om kennis te maken met een club die dat voor hen kan invullen.

Dat is ook precies waarom samenwerking zo goed werkt. InAudit brengt de specifieke branchekennis mee, hoe werkt Internal Audit in de praktijk? En wij vanuit het IIA geven vanuit ons normenkader en de wereldwijde standaarden aan wat er nodig is. We zijn onafhankelijk in dat verhaal.

Wat betekent het IIA-partnerschap concreet voor de klanten van InAudit?

Als je naar het drielinmodel kijkt, heb je de

tweede en de derde lijn. Bij het 3 lijnen model is Internal Audit de onafhankelijke 3e lijn. Eigenlijk zou elke organisatie een Internal Auditafdeling moeten hebben. Als ze daar te klein voor zijn dan komen partijen als InAudit deze rol invullen.

InAudit als partner is goed op de hoogte van alle standaarden, is bij het IIA aangesloten, weet hoe deze standaarden geïnterpreteerd moeten worden, weet wat guidance is en wat een topical requirement is. En zij kunnen dat voor organisaties perfect in balans brengen: wat heeft de organisatie nodig om goed Internal Audit te bedrijven, zonder de investering van een complete eigen afdeling die elke vijf jaar gecontroleerd moet worden?

Wat zo'n partnerschap ook meebrengt, is iets wat mensen onderschatten: je kunt best kennis nemen van standaarden, maar als je niet weet hoe je die moet integreren in je organisatie, ben je blij dat je een partner hebt die dat wél weet en die een directe ingang heeft tot het IIA als uitgifteorgaan van die standaarden. Dat is de combinatie die het doet.

Maar er is nog iets. Wij willen als IIA alleen partners hebben die daadwerkelijk iets toevoegen aan het vakgebied. Niet iedereen is partner van ons. Sommige grote organisaties vereenzelvigen zich schijnbaar niet met onze standaarden en willen ook niet op dat niveau getoetst worden. Die zijn dan ook geen partner.



Danny Francken samen met Ronald van de Langenberg bij het IIA Congres.

Hoe houdt InAudit als partner het vakgebied actief in stand?

Wat InAudit heel goed doet: als er vrijwilligers nodig zijn, staan jullie vooraan. Bij de nationale carrièrebeurs, bij de Dag van de Waterschappen: Ronald en Robert die met hun kennis en kunde meteen bijdragen en bij onze partner events altijd aanwezig. Yorick en Floris zitten bij onze Young Professionals; Floris ook nog eens bij het Ambition model.

Je kunt een partnerschap aan alle kanten invullen. En InAudit doet dat. Jullie maken gebruik van de mogelijkheden die in zo'n partnerschap zitten, en dat doet niet iedereen. Bij InAudit is de wederkerigheid zichtbaar. We doen het samen, en we worden er met zijn allen beter van. Niet alleen in geldelijke zin, maar ook gewoon door bij te dragen aan het vakgebied.

“

Weet je wat ik mooi vind? Samenwerking kan je altijd hebben. Maar bij jullie is het echt een SamenWerking.

”

Jullie hebben ook een nieuw pand. Wat moet dat uitstralen?

Het heeft best wat voeten in de aarde gehad om het bestuur te bewegen tot de keuze voor een nieuw pand. We zaten op 250 m² met één vergaderzaal waarin we 125 trainingen per jaar moesten proppen. De groei was al gestagneerd omdat we gewoon te klein zaten.

Na uitvoerig onderzoek is de keuze op Breukelen gevallen, op de Corridor. Naast het station, dus perfecte bereikbaarheid, en naast de A2 voor wie met de auto komt. We zitten nu ruim op 600 m², met vijf grote vergaderzalen en boardrooms, maar ook focusruimtes voor als je onderweg bent naar Amsterdam of Utrecht en je nog even wilt werken. Je kunt hier mensen ontvangen, het is een plek om te netwerken en van gedachten te wisselen. Ons pand is nadrukkelijk bedoeld als clubhuis voor onze leden.

Ik heb de ruimtes ook aangeboden aan andere brancheverenigingen zoals Norea, ISACA, de NBA, maar ook de VRC en de VCO, de compliance officers en de registercontrollers. En aan universiteiten en hogescholen: geef hier eens een keer je gastles, dan komen studenten in aanraking met dit vakgebied en zien ze wie wij zijn en wat we doen.

We zitten nu op een zichtlocatie waar we thuis horen. Dit is een vak en een vakgebied en een vereniging die trots op zichzelf kan zijn. En dat stralen we nu ook uit.

Wat houdt jou wakker als je kijkt naar de toekomst van het vak?

Wat mij bezighoudt, is hoe we zorgen dat onze perceptie in de markt de juiste is. De breedte van het vakgebied, en dat de juiste partijen Internal Audit op waarde weten te schatten.

Voorheen was Internal Audit echt intern gericht. Er werd alleen ledencommunicatie naar leden verstuurd, en de buitenwereld wist amper van het bestaan af. Dat vind ik een gemiste kans. Toen ik binnenkwam, is mijn focus juist extern geweest, zorgen dat dit vakgebied bekender wordt. Op het moment dat je meer draagkracht vanuit extern krijgt, wordt je functie serieuzer genomen en wordt het een aantrekkelijker vakgebied. Dan krijg je meer leden, en zo versterkt dat elkaar.

En dan is er het thema AI. Als je kijkt naar mens versus AI, wat is het grootste verschil?

Eén is creativiteit: de mens bepaalt hoe je AI inzet. En twee: hoe verkoop je een boodschap? Als jij als Internal Auditor bij de raad van bestuur moet zitten en een boodschap moet brengen, AI kan dat niet. AI kan alleen heel zakelijk, binair, zwart-wit een conclusie laten zien. Hij kan het niet verkopen. Hij kan niet inspelen op de sentimenten op dat moment. Dat is precies waar je als auditor straks het verschil mee maakt.

Ik denk dat de soft skills, communicatie, overtuigingskracht, je boodschap brengen aan mensen met een heel andere achtergrond, veel prominenter worden door de komst van AI. En dat is precies ons onderscheidend vermogen.

Ellen Koning

Communicatie

06-27 88 84 30



De overheid kan iets leren van de aanpak van risico's in het bedrijfsleven

“De overheid kan iets leren van de aanpak van risico's in het bedrijfsleven” was de krantenkop in het Financieel Dagblad deze ochtend (21 mei 2026). Een prikkelende stelling die ons als risicomangers meteen aansprak. In deze boodschap van Pieter Duisenberg zat bijna een moreel appèl om onze kennis te delen. Iets dat we als InAudit graag doen. Maar we beginnen eerst met goed luisteren.

Slagvaardigheid

De toespraak van de president van de Algemene Rekenkamer begint met een reflectie op het besluit uit 1864 om de Nieuwe Waterweg aan te leggen en daarmee de Rotterdamse haven beter te ontsluiten om vervolgens te constateren dat Nederland het afgelopen jaar stil is blijven staan. “We zien een opvallend gebrek aan vooruitgang”.

Hoewel de rechtmatigheid van de uitgaven boven de 99% ligt plaatst Algemene Rekenkamer een kanttekening bij de Rijksrekening: namelijk dat stilstand dreigt. De cijfers kloppen wel, maar er wordt geen vooruitgang gerealiseerd:

“Het is belangrijk dat we ons realiseren dat niets doen, dat kiezen voor stilstand, ons land miljarden kost. Dat is een keuze voor een onzekere toekomst met een onbekende rekening. Misschien niet meteen zichtbaar in de jaarverslagen van ministeries, maar wel voelbaar voor inwoners, voor bedrijven, voor toekomstige generaties. En dat kost niet alleen geld, maar ook vertrouwen. Het vertrouwen van burgers en bedrijven in de overheid. Het moet dus anders. Maar hoe?”

Is het bedrijfsleven wel het goede voorbeeld?

De krantenkop van het FD suggereert dat de strekking was dat de overheid iets kan leren van het bedrijfsleven, maar opvallend genoeg wordt de term “bedrijfsleven” helemaal niet gebruikt in de voordracht van de President van de Algemene Rekenkamer. In het interview van het FD wordt de connectie wel gelegd en wordt de balans geschetst tussen de onzekerheid die investeren oplevert versus de onzekerheid van wat er gebeurt als je niet investeert. Deze balans is min of meer vergelijkbaar met het dilemma van de overheid, met één groot verschil: niet investeren in de toekomst kan voor een onderneming het einde van het voortbestaan beteke-

nen. Maar voor de overheid niet, die zal altijd blijven bestaan. De suggestie daarmee is dat het ontbreken van existentiële angst de balans tussen direct risico en toekomstig risico negatief beïnvloedt. In andere woorden: je komt pas in actie, als je voortbestaan wordt bedreigd.

De lijst met 60 risico's

Behalve de voordracht over de staat van de rijksverantwoording heeft de Algemene Rekenkamer ook een lijst met 60 risico's opgesteld, de 'Hoogrisicolijst'. Deze is interessant en geeft op verschillende onderwerpen de afwegingen weer tussen het risico (bijvoorbeeld: “afzakken als concurrerende economie”), elementen van de bedragen die via het Rijk lopen (bijvoorbeeld: €23 miljard aan fiscale ondernemersregelingen) en de maatschappelijke impact (bijvoorbeeld beperkte economische groei). Hierbij valt direct op dat alleen wordt gesproken over risico's in termen van uitgaven en schade, maar niet in kansen of gemiste maatschappelijke opbrengsten.

Het waarden van 'missed opportunities'

Het denken over kansen en gemiste opbrengsten is niet alleen een thema voor de overheid, maar ook gewoon voor het bedrijfsleven. We nemen uitgaven of kosten mee in de winst- en verliesrekening en dat drukt de winst. Dat is een zekerheid. Deze kosten maken we echter met als doel om onze bedrijfsactiviteiten te kunnen uitvoeren en dat levert hopelijk winst op (maar dat is een onzekerheid).

Het feit dat we 'missed opportunities' niet waarderen als kostenpost zorgt niet alleen bij de overheid voor beïnvloeding van de besluitvorming. Het is eigenlijk gewoon een waarderingsvraagstuk. Want hoe zouden besluiten genomen worden wanneer je de 'missed opportunities' ook als kostenpost of verlies aan waarde in je jaarcijfers zou moeten verwerken?

In de Ster-campagne 'Tuincentra Tuinmart' wordt



de ondernemer verrast door het succes van zijn eigen campagne op de radio. Stel dat de kosten €50K van de campagne zijn en maar dat de toegenomen marge €500K bedraagt. Dan is de business case helder. Maar dat weet je pas achteraf. De kosten van de campagne zijn een zekerheid, de opbrengsten niet.

Maar wat als je dit omdraait en op het moment dat Mart niet zou besluiten om de campagne uit te voeren en dat hij daarom in plaats van €50K kosten, de schade van de 'missed opportunity' van €450K als verlies zou moeten nemen. Dit soort overwegingen zou besluitvorming, ook in het bedrijfsleven, flink beïnvloeden.

Vertaald naar de overheid: Als de overheid een miljardenverlies zou moeten verantwoorden vanwege het besluit om de Lelylijn niet aan te leggen, dan zouden de afwegingen ineens heel anders zijn.

Fundamentele verschillen tussen overheid en bedrijfsleven

Behalve het feit dat het bedrijfsleven wel een existentiële bedreiging kan ervaren en de overheid niet, zijn er ook andere fundamentele verschillen die besluitvorming door de overheid (veelal in negatieve zin) beïnvloeden. Het begrip rechtmatigheid is bijvoorbeeld voor het bedrijfsleven veelal een non-issue en ook morele afwegingen of de verantwoordelijkheid voor de maatschappij kunnen voor bedrijven heel anders worden ervaren. Wellicht een nog fundamenteeler probleem is de (in beginsel) vierjarige cyclus van verkiezingen en coalitievorming en de daarmee samenhangende behoefte om populair te zijn.

Deze cyclus maakt het aantrekkelijk om de focus ook op de korte termijn te houden en besluiten waarvan de toekomstige opbrengsten ver weg liggen (de Nieuwe Waterweg in Rotterdam) uit te stellen en de last daarvan door te schuiven naar de politieke opvolgers.

Kan de overheid iets leren van risicobeheer in het bedrijfsleven?

Binnen verschillende bedrijfstakken binnen het bedrijfsleven bestaat veel ervaring met risicobeheer. In sommige sectoren (zoals bijvoorbeeld transport en de (petro-)chemische industrie) is dat sterk verankerd in het veiligheidsdomein. Binnen andere sectoren, zoals de financiële sector, ligt veel focus op de toereikendheid van financiële buffers en weerstandsvermogen. Maar ook binnen de overheid is er veel risicobeheer. Denk daarbij aan de scenario's die de politie doorloopt bij grote evenementen, de oefeningen van de brandweer of de analyses die de toezichthoudende autoriteiten uitvoeren op de sector waarop ze toezicht houdt. Het belangrijkste verschil dat wij zien met het bedrijfsleven is dat binnen de overheid het risicomanagement over het algemeen meer versnipperd is. Omdat de integraliteit vaak ontbreekt kunnen we als auditors vaak ook minder goed samenwerken met of steunen op de 'tweede lijn' in vergelijking met het bedrijfsleven.

Welke kennis zouden we als InAudit willen delen?

Terugkomend op de vraag wat wij als InAudit zouden willen betekenen voor de overheid (of voor decentrale overheden)? De belangrijkste verschillen tussen overheid en bedrijfsleven kunnen we immers niet oplossen. Maar wel hebben we enkele punten waarover we ons verwonderen.

Op de eerste plaats zouden we de Algemene Rekenkamer willen complimenteren met hun analyse. Maar we zouden ze ook graag willen uitdagen om nog iets verder te gaan, bijvoorbeeld door sommige business cases eens nader door te rekenen en te gaan rapporteren in termen van 'missed opportunities'.

Een van die 'missed opportunities' is voor veel decentrale overheden het ontbreken van een centrale interne auditfunctie die periodiek en onafhankelijk rapporteert en waarmee een lange termijn relatie kan worden opgebouwd. Een gesprekspartner voor de gemeentesecretaris, B&W en de Rekenkamer. Veel decentrale overheden vinden zichzelf daarvoor te beperkt van omvang. Maar daarvoor hebben wij als InAudit een perfecte oplossing, namelijk uitbesteden! Wij kunnen zorgen voor een inrichting in lijn met beroeps-standaarden, we zorgen voor gekwalificeerde mensen, continuïteit en kwaliteitsbewaking. We kunnen dat ook doen voor de kosten van één FTE of zelfs minder, schaalbaar en flexibel. Oh ja ... en dan kijken we meteen naar de aanpak van uw risicomanagement!

Ronald van de Langenberg

Nieuwe fase in de strijd tegen witwassen

Volgend jaar, om precies te zijn op 10 juli 2027 wordt het langverwachte zesde anti-witwaspakket van kracht. Dit pakket bevat een aantal belangrijke pijlers, waar we in dit artikel meer over vertellen.

Onderdelen

Het pakket bestaat uit drie grote wetten:

- de AMLA-verordening (Regulation (EU) 2024/1620; AMLAR) tot oprichting van de Europese Anti-Money Laundering Authority (AMLA);
- de Antiwitwasverordening (Regulation (EU) 2024/1624; AMLR) die de verplichtingen van meldingsplichtige entiteiten (ME's) regelt;
- de Antiwitwasrichtlijn (Directive (EU) 2024/1640; AMLD6) die de governance op nationaalniveau betreft, zoals het UBO-register en het toezicht.

De Antiwitwasrichtlijn zal de huidige Wet ter voorkoming van witwassen en terrorismefinanciering (Wwft) voor een groot deel vervangen. Deze witwasregels zijn niet van toepassing op schadeverzekeraars, wel op levensverzekeraars, banken en betaalinstellingen.

AMLA

Een van de meest in het oog springende maatregelen is de oprichting van de Anti-Money

Laundering Authority (AMLA). Deze autoriteit is inmiddels in oprichting, en zal vanaf 2028 rechtstreeks toezicht gaan houden op een aantal instellingen. Dit zijn circa 40 geselecteerde, hoogrisicovolle financiële instellingen in de Europese Unie. Daarnaast zal de autoriteit in iedere lidstaat in elk geval op één financiële instelling direct toezicht uitoefenen.

De selectie van deze instellingen wordt in 2027 afgerond. Het directe toezicht richt zich op:

- Grensoverschrijdende actieve instellingen: Dit zijn voornamelijk grote, systemische banken en financiële dienstverleners die in veel verschillende lidstaten opereren.
- Het hoogste risico op witwassen en terrorismefinanciering: De instellingen worden geselecteerd op basis van een gezamenlijk risicomodel waarin hun kwetsbaarheid centraal staat.
- De niet-financiële sector: Hoewel de AMLA indirect toezicht houdt op de gehele sector, voert zij in de praktijk alleen direct toezicht uit op financiële instellingen.



Voor instellingen die niet onder rechtstreeks toezicht vallen zullen (in de Nederlandse context) DNB en AFM de aangewezen toezichthouders blijven.

AMLR: single rulebook

De Anti-Money Laundering Regulation (AMLR) is een verordening en heeft vanaf 10 juli 2027 rechtstreekse werking in alle lidstaten van de Europese Unie. Daarom wordt de AMLR ook wel aangeduid als 'single rulebook'. Deze wet bevat een aantal wijzigingen ten opzichte van het huidige stelsel. Zo wordt het aantal onder toezichtstaande instellingen uitgebreid met onder meer profvoetbalclubs, voetbalmakelaars en crowdfundingplatformen, wordt de cashlimiet Europees gesteld op €10.000, waar Nederland dit zelf heeft bijgesteld naar €3.000, en wordt de UBO-grens gesteld op '25% eigendom/feitelijk zeggenschap of meer'. Dit is een verandering ten opzichte van de huidige wetgeving, die uitgaat van 'meer dan 25% eigendom/feitelijk zeggenschap'. Vennootschappen met vier gelijkwaardige aandeelhouders gaan daarmee ook onder de reikwijdte vallen.

Van ongebruikelijk naar verdacht

Daarnaast verschuift onder de AMLR de focus van het melden van ongebruikelijke transacties naar het beoordelen en melden van verdachte transacties. In Nederland lag de nadruk traditioneel op objectieve indicatoren: vooraf vastgestelde criteria die bepalen wanneer een transactie ongebruikelijk is, zoals transacties boven een bepaald bedrag, een groot aantal transacties binnen korte tijd of transacties met hoogrisicolanden. Deze systematiek sloot aan bij het uitgangspunt dat alleen opsporingsinstanties en het Openbaar Ministerie kunnen vaststellen of daadwerkelijk sprake is van een concrete verdenking.

De AMLR legt echter meer nadruk op een risicogebaseerde beoordeling. Daardoor worden subjectieve indicatoren belangrijker. Hierbij kijkt een instelling niet alleen naar vaste drempels, maar ook naar gedrag, context en patronen. Denk bijvoorbeeld aan klanten die zonder duidelijke economische reden grote contante stortingen doen, of transacties verrichten die niet passen bij hun profiel of bedrijfsactiviteiten. Deze ontwikkeling kan leiden tot minder automatische meldingen, maar vraagt wel meer analyse, expertise en verantwoordelijkheid van financiële instellingen.

AMLD: update Wwft

Tot slot staan we stil bij de Anti-Money Laundering Directive. Deze verordening wordt op dit moment omgezet in de Nederlandse wetgeving en zal daarmee de huidige Wwft actualiseren. De belangrijkste wijzigingen betreffen het harmoniseren van de bevoegdheden van de Financial Intelligence Units (FIU's). Dit zijn de instellingen die de meldingen van verdachte transacties moeten beoordelen en opvolgen. Tevens wordt in deze wetgeving de toegang tot het UBO-register uitgebreid met onder meer journalisten en organisaties die zich bezighouden met het voorkomen of bestrijden van witwassen en terrorismefinanciering en bevoegde autoriteiten van derde landen.

Tot slot

Met deze wetgeving veranderen een aantal zaken in de uitvoering, en wordt vooral verder gewerkt aan harmonisatie van wetgeving in de Europese Unie. Tegelijkertijd verandert het doel van de wetgeving niet: het voorkomen en indammen van witwassen en terrorismefinanciering. Heeft u vragen over de toepassing van de wetten, of wat dit voor uw organisatie betekent, schroom dan niet om contact met ons op te nemen. We helpen u graag met inventariseren en implementeren van maatregelen!



**AMLR**
single rulebook

- Directe werking vanaf **10 juli 2027**
- Nieuwe melders: crowdfundingplatformen, voetbalclubs, etc.
- Meldplicht verschuift van OT naar VT: meld vermoedens van criminele activiteiten EU-cashlimiet: max. **€10.000**, NL hanteert €3.000
- UBO: **25%** of meer eigendom/zeggenschap

**AMLD6**
zesde anti-witwasrichtlijn

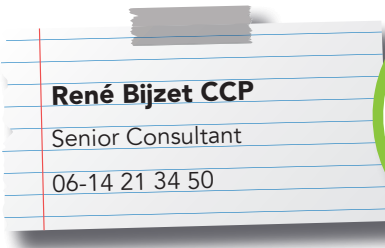
- Implementatie voor **10 juli 2027**
- Lastenluwe, risicogebaseerde implementatie via Implementatiewet ter voorkoming van witwassen en terrorismefinanciering
- UBO-registers: beperkte toegang, verplichte verificatie en melding bij FIU
- Bevoegdheden FIU's:
 - o spoedbevroezingsbevoegdheid;
 - o bron van melder afgeschermd;
 - o meer feedback aan poortwachters over verdachte transacties;
 - o grondrechtenfunctionaris;
 - o attendering.

**AMLAR**
Europese toezichthouder

- Oprichting van centraal toezichts orgaan **AMLA** (operationeel vanaf 1 juli 2025)
- Direct toezicht op een select aantal financiële instellingen met een hoog risico
- Indirect toezicht door coördinatie nationale toezichthouders
- Coördinatiemechanisme voor FIU's
- Sanctiebevoegdheid bij ernstige of herhaalde overtredingen

**Wessel Westerveld**
MSc CIA CISA
Auditmanager
06-21 62 77 50



**René Bijzet CCP**
Senior Consultant
06-14 21 34 50



Floris Stokkers over groeien in het auditvak:

‘Voor mij ligt de kracht in samenwerking’

Na zijn studie **Commerciële Economie** aan Hogeschool Leiden startte Floris Stokkers in 2020 bij InAudit als junior auditor. Inmiddels is hij senior auditor, behaalde hij zijn **Certified Internal Auditor (CIA)**- en **Certified Information Systems Auditor (CISA)**-certificeringen en is hij begonnen aan de **Executive Master of IT Auditing**. Daarnaast zet hij zich actief in voor het IIA. We spraken hem over zijn ontwikkeling, de combinatie van werk en studie en zijn blik op het auditvak.

Hoe kijk je terug op je begintijd bij InAudit?

Mijn start bij InAudit was allesbehalve standaard. Ik begon in 2020, midden in de coronaperiode, toen thuiswerken ineens de norm was. Voor iemand die net nieuw is in een organisatie, maakt dat het inwerken lastiger. Je spreekt collega's minder snel en loopt niet zomaar even ergens binnen.

Toch heb ik in die periode stap voor stap mijn plek gevonden. Ik ben gegroeid in mijn rol en voel me inmiddels echt thuis in het vak en binnen het team. Juist die beginperiode heeft mij laten zien hoe belangrijk samenwerking is. Als auditor werk je zelfstandig en heb je veel eigen verantwoordelijkheid, maar voor mij zit de kracht juist in het samen optrekken met collega's. Bij InAudit krijg ik veel vrijheid om mijn werk op mijn eigen manier vorm te geven, maar altijd met een team om op terug te vallen.

Wat spreekt je aan in die combinatie van vrijheid en samenwerking?

Dat is precies wat ik zo leuk vind aan mijn werk. Aan de ene kant krijg ik veel ruimte om mijn planning, aanpak en werkwijze zelf te bepalen.

Aan de andere kant sta ik er nooit alleen voor. We denken samen na, sparren met elkaar en reviewen elkaars werk. Dat teamgevoel maakt voor mij echt het verschil.

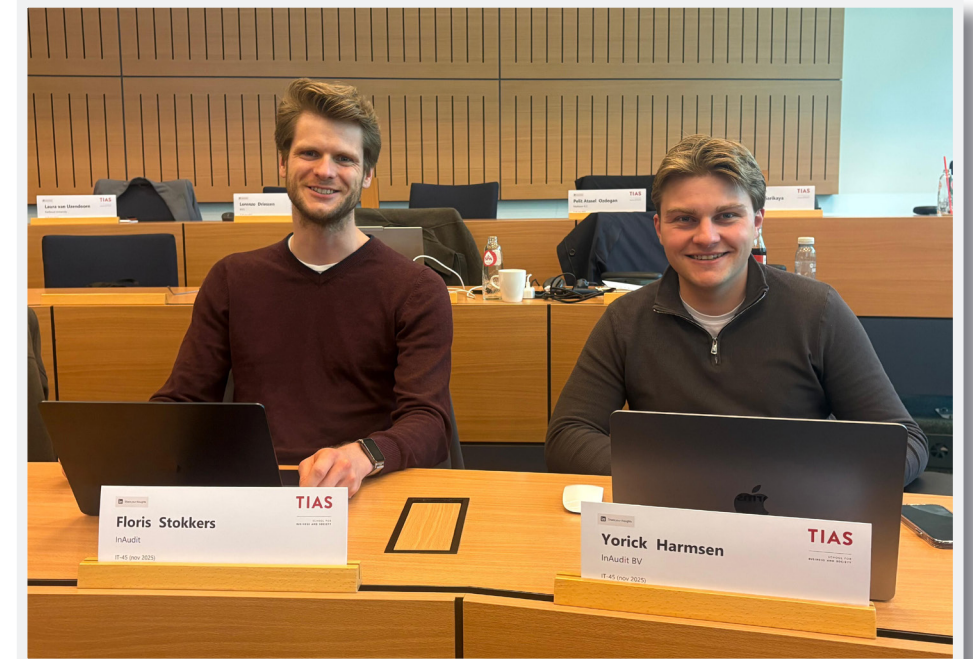
In een vak waarin je regelmatig met complexe vraagstukken te maken hebt, is het heel waardevol om op collega's te kunnen bouwen. Niet alleen om de kwaliteit te waarborgen, maar ook om van elkaar te leren. Voor mij zit daar een groot deel van het werkplezier: samen lastige vraagstukken oplossen en elkaar steeds beter maken in het vak.

Welke misverstanden kom je tegen over het auditvak?

Als ik op een verjaardag vertel wat ik doe, merk ik vaak hoeveel misverstanden er over audit bestaan. Mensen denken al snel aan accountancy, controles op cijfers of het afkeuren van wat niet goed gaat. Terwijl interne en IT-audit voor mij juist veel breder en vooral constructiever zijn.

Een audit draait niet om het aanwijzen van fouten zelf. Het gaat erom dat je onafhankelijk kijkt naar processen, risico's en beheersmaatregelen,

Floris Stokkers en
Yorick Harmsen
bij TIAS



zodat organisaties kunnen leren en verbeteren. Ik zie audits veel meer als een manier om problemen vroeg te signaleren en processen sterker te maken, voordat kleine tekortkomingen grote problemen worden.

Die misvatting leeft trouwens niet alleen buiten het vakgebied, maar soms ook bij klanten. Medewerkers die voor het eerst met auditors te maken krijgen, zijn regelmatig gespannen. Ze zijn bang om iets verkeerd te zeggen of denken dat bevindingen per definitie negatief zijn. Terwijl ik een bevinding juist zie als een kans om te leren. Wat mij betreft mag een audit veel vaker worden gezien als een gezamenlijk verbeterproces.

Je bent ook actief als vrijwilliger bij het IIA. Wat doe je daar precies?

Naast mijn werk bij InAudit ben ik actief bij het IIA, het Instituut van Internal Auditors. Ik zet me onder meer in voor de Young Professionals Commissie, de Ambition Model Commissie en de Professional Practices Network Group AI. Dat doe ik niet alleen omdat ik betrokken ben bij het vak, maar ook omdat ik het waardevol vind om samen met vakgenoten na te denken over de toekomst van interne audit.

Mijn betrokkenheid begon via een collega die al actief was binnen de Young Professionals. In eerste instantie dacht ik dat het misschien niet direct iets voor mij zou zijn, maar dat veranderde toen ik hoorde hoe leuk en waardevol het was om samen activiteiten te organiseren. Een bekend gezicht helpt om de drempel te verlagen, maar uiteindelijk waren het vooral de inhoud en de sfeer die mij overtuigden.

Wat maakt dat vrijwilligerswerk voor jou waardevol?

Binnen de Young Professionals Commissie houd ik me vooral bezig met het organiseren van evenementen, workshops en inhouse-dagen. Dat zijn momenten waarop jonge auditors en vakgenoten elkaar ontmoeten, kennis delen en nieuwe inzichten opdoen.

Wat ik daar vooral waardevol aan vind, is dat het verder gaat dan alleen inhoudelijke kennis. Ik leer ook hoe andere organisaties werken, welke uitdagingen daar spelen en hoe verschillend het vak in de praktijk kan worden ingevuld. Die uitwisseling van perspectieven helpt mij om ook in mijn eigen werk scherper te kijken en creatiever te denken.

Wat zijn inhouse-dagen precies?

Tijdens inhouse-dagen bezoeken we met een groep young professionals organisaties met een interessante auditpraktijk. De interne afdeling vertelt dan over de eigen aanpak, uitdagingen en innovaties. Zulke bezoeken leveren vaak veel inspiratie op, juist omdat je een kijkje krijgt in een heel andere context dan die van je eigen organisatie.

Een voorbeeld dat mij goed is bijgebleven, is het bezoek aan DELA. Misschien niet direct de meest voor de hand liggende organisatie, maar juist daardoor heel interessant. De combinatie van verzekeringsactiviteiten en uitvaartlocaties maakt het een veelzijdige organisatie met complexe processen en uiteenlopende risico's. Wat vooral indruk op mij maakte, was hun manier van werken met agile auditing.

Naam: Floris Stokkers BSc CIA CISA
Functie: Senior Auditor
Bedrijf: InAudit Audit Services
Vrijwilligerswerk: Young Professional bij het IIA
Huidige studie: De Executive Master of IT Auditing aan TIAS in Tilburg



Daarnaast ontwikkel ik in dat vrijwilligerswerk ook vaardigheden die je niet altijd automatisch in het dagelijkse auditwerk opdoet, zoals organiseren, afstemmen, contacten leggen, mensen enthousiasmeren en presenteren.

Ondertussen volg je ook nog een pittige opleiding. Hoe combineer je dat?

In november ben ik gestart met de Executive Master of IT Auditing aan TIAS in Tilburg. Die opleiding duurt twee jaar en is een belangrijke stap richting de RE-titel. Voor wie binnen het IT-auditvak verder wil groeien, is dat een logische en vaak noodzakelijke volgende stap.

De studie is intensief. Elke vrijdag staat in het teken van colleges en daarnaast gaat er wekelijks veel tijd zitten in opdrachten en voorbereiding. Dat betekent in de praktijk dat ook een deel van het weekend regelmatig opgaat aan de studie. De combinatie van werk, studie en andere verplichtingen vraagt dus om een strakke planning en veel discipline.

Tegelijk zie ik heel duidelijk de waarde ervan. De opleiding geeft mij niet alleen academische verdieping, maar ook direct toepasbare kennis. Onderwerpen als AO/IC, procesbeheersing, risicoanalyse en beroepsvereisten krijgen meer structuur en diepgang. Dat helpt mij om wat ik in de praktijk vaak al intuïtief aanvoel, beter te onderbouwen en scherper te verwoorden.

Merk je dat ook terug in je werk?

Zeker. Ik merk dat ik processen beter kan analyseren, risico's helderder kan formuleren en vraagstukken makkelijker in een breder kader kan plaatsen. De meerwaarde zit voor mij dan ook niet alleen in het diploma of de titel, maar juist in de directe toepasbaarheid in de praktijk.

Ook binnen InAudit heeft dat effect. Nieuwe inzichten uit de studie houd ik niet voor mezelf, maar deel ik met collega's. Daarmee draagt mijn eigen ontwikkeling ook direct bij aan de verdere ontwikkeling van het team en de dienstverlening. Dat past goed bij hoe ik naar groei kijk: niet als iets individueels, maar als iets dat je samen versterkt.

Alsof dat nog niet genoeg is, heb je ook nog een klushuis. Hoe houd je alles in balans?

Met werk, studie, IIA-activiteiten en daarnaast een recent gekocht klushuis is mijn leven op dit moment behoorlijk vol. Ik zie dat als verschillende dimensies: werk, studie, privé en alles wat daar nog bij komt. Zolang het er twee zijn, blijft het overzichtelijk, maar zodra er meer tegelijk naast elkaar lopen, wordt het ingewikkelder.

De uitdaging zit vaak niet in één groot probleem, maar juist in het samenkomen van allerlei deadlines, verplichtingen en verwachtingen. Werkdeadlines lopen door, studieopdrachten moeten af en privé vraagt ook aandacht. Dat maakt plannen soms best lastig.

Toch probeer ik daar realistisch in te blijven. Ik weet dat dit pittige jaren zijn, maar ook dat het een fase is die veel oplevert. Bovendien helpt het dat ik de studie samen met mijn collega Yorick Harmsen volg. Dat zorgt voor herkenning, wederzijds begrip en extra motivatie.

Wat heb je in deze periode vooral over jezelf geleerd?

Als ik terugkijk, is er één les die eruit springt: vaker nee zeggen. Niet omdat ik minder betrokken wil zijn, maar juist omdat enthousiasme er soms voor zorgt dat ik te veel tegelijk oppak. In de praktijk kosten dingen bijna altijd meer tijd dan je vooraf denkt. Wat klein lijkt, blijkt vaak groter zodra je erin zit.

Dat inzicht heeft mij geleerd om bewuster te kiezen. Niet alles wat interessant is, past ook op hetzelfde moment. Juist door selectiever te zijn, kan ik de dingen die ik wél doe beter uitvoeren en er meer plezier uit halen.

Tegelijk ben ik er ook trots op dat ik alles nog steeds draaiende houd. Werk, studie, vrijwilligerswerk en privé vragen allemaal energie. Dat is soms zwaar, maar het laat me ook zien dat ik veel aankan. Wat daarbij helpt, is het besef dat deze periode niet voor altijd zo intens blijft. Er is licht aan het einde van de tunnel, en dat vooruitzicht geeft energie om door te gaan.

Wat drijft je in alles wat je doet?

Mijn enthousiasme voor het vak. Ik kijk niet alleen naar wat een auditor doet, maar vooral naar wat een auditor kan betekenen. Die ontwikkelgerichte blik loopt als een rode draad door mijn werk, studie en nevenactiviteiten.

Tot slot: wat wil je andere young professionals meegeven?

Gewoon aansluiten. Voor iedereen die overweegt om actiever te worden binnen het vak, bijvoorbeeld via het IIA Young Professionals-netwerk, zou ik zeggen: doe mee. Je ontmoet mensen, leert nieuwe dingen en merkt vanzelf hoeveel energie het geeft om samen met anderen aan het vak te bouwen.

Voor mij zit de kracht juist in die combinatie van inhoud en ontmoeting. Je wordt er niet alleen beter van als professional, maar merkt ook dat je onderdeel bent van een bredere vakgemeenschap. En dat maakt het werk uiteindelijk niet alleen interessanter, maar ook leuker.

Afstudeerstage Integrale Veiligheidskunde

In februari ben ik, Hessel de Vrij, gestart met mijn afstudeerstage bij InAudit. Voor mijn opleiding Integrale Veiligheidskunde aan het Saxion moesten nog twee kerntaken worden afgerond: implementeren en evalueren. Binnen InAudit kreeg ik de kans om beide opdrachten in de praktijk uit te voeren, wat mij een volledig beeld heeft gegeven van informatiebeveiliging binnen een professionele organisatie.

Kerntaak Evalueren:

Interne ISO/IEC 27001:2022 audit

De eerste kerntaak was de interne ISO/IEC 27001:2022 audit. Mijn taak was om het Information Security Management System (ISMS) van InAudit objectief te beoordelen en te toetsen aan het internationale normenkader, niet alleen op papier, maar ook in de praktijk.

De eerste twee maanden heb ik mij hier intensief op gericht. Stap voor stap heb ik de hoofdstukken 4 t/m 10 en Annex A van de norm doorlopen in een werkprogramma, waarbij per norm is gekeken naar de opzet, het bestaan en de werking van de beheersmaatregelen binnen InAudit. Dit leverde een gestructureerd en volledig beeld op van hoe de organisatie voldoet aan de eisen van informatiebeveiliging.

Bijzonder leerzaam was de combinatie van zelfstandig werken en nauwe samenwerking met de

organisatie, waaronder de CISO, de ICT-manager en de directie. Gedurende het hele proces stond auditmanager Menny Barendse klaar om mee te denken, te reviewen en feedback te geven, waardoor ik mijn bevindingen steeds verder kon aanscherpen en onderbouwen.

Kerntaak Implementeren: Software beleid

Na de audit was het tijd voor de tweede kerntaak: implementeren. Waar de audit draaide om beoordelen, stond deze opdracht juist in het teken van verbeteren en veranderen.

Concreet heb ik een concept acquisitiebeleid opgesteld: een praktisch stappenplan voor de toekomstige aanschaf van nieuwe software, waarbij informatiebeveiliging een centrale rol speelt. Het doel is om meer structuur en bewustwording te creëren in de besluitvorming rondom nieuwe systemen, zodat keuzes niet alleen op functionaliteit worden gemaakt, maar ook op risico's en beveiligingseisen.

Als onderdeel van dit traject is een proof of concept aangeschaft, waarmee in de praktijk kon worden getest hoe een alternatief systeem functioneert binnen de bestaande processen. Dit gaf waardevolle inzichten in de haalbaarheid, gebruiksvriendelijkheid en de aansluiting op de eisen van InAudit. Tot slot heb ik uitgewerkt welke stappen, zowel technisch als organisatorisch, nodig zijn om een dergelijke verandering gestructureerd en gecontroleerd door te voeren.

Door beide opdrachten te combineren heb ik het volledige traject van informatiebeveiliging en procesverbetering van begin tot eind kunnen doorlopen.

Iedereen bedankt voor de fijne begeleiding!

Hessel de Vrij met zijn afstudeeropdracht.



We zijn er om u te helpen !



We zijn trots sponsor van The Powergirls, een team van hockeyvereniging BMHV uit Baarn.



www.inaudit.nl