30 maart 2023

InAudit Magazine

We leren het meest in interessante tijden

Met dank aan alle klanten en collega's die hebben meegewerkt, kunnen we u een magazine presenteren met veel inhoud. Onderwerpen als DORA, datakwaliteit, het interview met Jacob Iedema over informatie-beveiliging bij EOC en het artikel over security awareness geven een goed tijdsbeeld waarin we zien hoe zeer digitalisering ons dagelijks leven inmiddels beïnvloedt. Voor een kop boven dit voorwoord heb ik daarom ook maar even ChatGPT geraadpleegd.

Het is overigens niet alleen digitalisering dat ons leven interessant maakt. Nh1816 is met een ambitieus nieuwbouwproject bezig in 'ons dorp' Oudkarspel, maar realiseerde tegelijk het predicaat 'beste schadeverzekeraar particulier 2022' om de focus op de klant te onderstrepen. Ook als InAudit streven we naar een hoge waardering van onze klanten. De uitkomsten van de klantevaluatie 2022 voor onze interne audit dienstverlening onderstreept dat ook. Ook dit jaar waren onze klanten gemiddeld erg tevreden en tegelijk zijn ons weer een aantal mogelijkheden tot verbetering aangereikt, waarmee we aan de slag kunnen.

Menny en Floris hebben een voor verzekeraars interessant artikel geschreven over het essentiële onderscheid tussen schorsen en opschorten. Een verschil dat op het eerste gezicht triviaal lijkt, maar toch grote consequenties kan hebben. We hebben dit keer onze collega Daniël bereid gevonden om een inkijkje in zijn persoonlijke leven te geven. Om dan toch het bruggetje naar digitalisering te maken: als u nog goede podcast suggesties heeft, dan zijn die welkom (en niet alleen bij Daniël)!

Dat we binnen de wereld van de interne auditors steeds meer worden herkend door onze visie op informatiebeveiliging blijkt ook doordat we dit jaar opnieuw zijn uitgenodigd om de Cyberellende Pub Quiz op het jaarlijkse IIA congres te presenteren. Dankzij de hoge waardering mogen we ditmaal het internationale podium betreden om de quiz voor auditors uit de hele wereld te houden. Ondertussen zijn we ook aan de slag met DORA en zoeken we mogelijkheden om onze kennis op dit vlak met u te kunnen delen, mogelijk in de vorm van een kennisdag later dit jaar.

Na acht jaar klussen aan de datakwaliteit bij Nationale Nederlanden (en rechtsvoorgangers) is voor mij de tijd gekomen om afscheid te nemen van NN, maar gelukkig staan de eerste nieuwe klussen op het gebied van datakwaliteit alweer op het programma. Met name pensioenfondsen zullen als gevolg van de Wet Toekomst Pensioenen aan de slag moeten met het aantoonbaar maken van (de beheersing van) datakwaliteit. Op dat vlak werken we ook nauw samen met specialisten van Triple A.

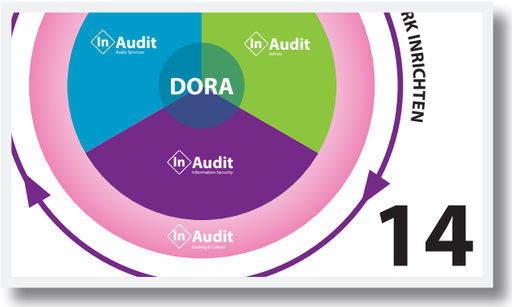
We zien ook dat de behoefte aan ondersteuning op het gebied van informatiebeveiliging snel toeneemt. Zelf geloven we erg in het concept van uitbesteding van de CISO-functie, omdat het voor veel kleinere en middelgrote organisaties moeilijk is om deze functie zinvol fulltime in te vullen. Niet alleen bij EOC werken we inmiddels op deze manier samen.

Ook de organisatie van InAudit zelf vraagt om de nodige aandacht. We willen een betrouwbare partner zijn om onze klanten goed te ondersteunen op het gebied van interne beheersing. Dit doen we niet alleen door van dag tot dag voor u bezig te zijn, maar ook door na te denken over de 'behoeften van morgen' en onze strategie daarin. Tegelijk willen we ook een goede werkgever zijn en daartoe hebben we in IJsselstein een tweede (samenwerk-)locatie geopend.

We hopen dat dit magazine ook voor u weer interessante inzichten oplevert!

Ronald van de Langenberg
Algemeen Directeur InAudit

Inhoud



Colofon

Uitgave: InAudit BV
Datum: 1 april 2023

Locaties:
Leuvenheim en IJsselstein

+31 (055) 303 25 97
info@inaudit.nl

www.inaudit.nl

Interview Rémon Chattellon Nh1816

“Een duurzame toekomst is iets van ons allemaal”, vindt Rémon Chattellon, financieel directeur bij Nh1816 Verzekeringen. Een uitspraak die past bij een coöperatieve verzekeraar, bij wie het draait om ‘samen’. Daarom werd in 1999 Stichting Goede Doelen opgericht.

In 2022 werden ze gekozen als beste schadeverzekeraar Particulier en wordt er een nieuw kantoorpand gebouwd. Tijd voor een interview dachten we.

Even voorstellen

Mijn naam is Rémon Chattellon en ik ben geboren in Gorinchem. Ik woon met mijn gezin in Heiloo en hou van uit eten gaan, mijn Green Egg en verre reizen maken. Aan de Universiteit van Amsterdam studeerde ik accountancy. Via verschillende rollen en organisaties kwam ik in 2009 terecht bij Nh1816 Verzekeringen als Manager Financiën. Nu ben ik een van de drie directieleden bij Nh1816. Mijn collega’s zwaaien dit jaar af en gaan met pensioen. Jammer, want we zijn een goed team. Tegelijkertijd kijk ik er naar uit om met een nieuwe collega-directeur ons mooie bedrijf te leiden.

De propositie van Nh1816

Onze roots liggen in Oudkarspel, aan de Dorpsstraat. Al ruim 200 jaar focust Nh1816 zich op particuliere schadeverzekeringen die we aanbieden via aangesloten adviseurs. Dat is een bewuste keuze. Net als de keuze om de telefoon persoonlijk op te nemen, zonder menu.
We blijven dicht bij onszelf, zijn informeel en laagdrempelig. Mede daarom geven verzekerden en aangesloten adviseurs ons gemiddeld een 9,1 voor service. Ook onze VerzekeringApp draagt daaraan bij. Het biedt gemak én overzicht. Vanuit de coöperatie Nh1816 zetten wij ons samen met local hero’s volop in voor diverse initiatieven die onze omgeving mooier maken. Bij Nh1816 vertrouwen wij op elkaar en de financieel adviseurs die met ons samenwerken. Wij werken samen aan begrijpelijke producten en voorwaarden. We zeggen wat we doen en doen wat we zeggen. Wij maken duidelijke keuzes en communiceren die in begrijpelijke taal.

“We zeggen wat we doen en doen wat we zeggen”

Nh1816 beste schadeverzekeraar Particulier 2022

Via het doorlopend PerformanceMonitor onderzoek van sectorexpert IG&H onder intermediairs in Nederland zijn we gekozen tot de beste schadeverzekeraar 2022. We zijn ontzettend trots dat de bij ons aangesloten adviseurs ons zo enorm waarderen. En dat ook laten blijken wanneer ze de vragenlijst invullen. We zetten ons elke dag in om de beste te zijn. Dat onze aangesloten adviseurs dat bevestigen met een gemiddelde score van 8.5 is de kroon op ons werk. Het bevestigt voor ons dat onze bewuste keuze om uitsluitend met adviseurs te werken nog steeds de juiste is.

Onze ambitie

De ontwikkelingen in de wereld, de pandemie, de klimaatverandering, ontwikkelingen rond duurzaam ondernemen, oorlog, het heeft allemaal invloed op onze dagelijkse praktijk. In sommige gevallen positief en in sommige gevallen negatief. De simpele som is hoe meer schade, hoe hoger de premie en andersom. Als verzekeringsbedrijf houden wij een gezonde premie-schade ratio aan. Maar we hebben ook duurzame ambities, die we met onze coöperatie en stichting tot uiting laten komen. Om samen goed te kunnen blijven doen voor onze omgeving is het belangrijk dat we financieel gezond zijn. Alle interne en externe ontwikkelingen die daar invloed op kunnen hebben volgen wij op de voet. Jaarlijks bekijken we ook of onze premies nog aansluiten bij de schadelast. Tijdens de pandemie was er bijvoorbeeld veel minder schade, logisch want er waren veel minder verplaatsingen.

Het gevolg was dat de door ons ingeschatte premie te hoog was. Een storm of overstroming zorgt voor het tegenovergestelde, dan moeten we veel schade betalen ten opzichte van de premie.

De oorlog met de inflatie als gevolg zorgden ervoor dat de hele keten onder druk is komen te staan. Iedereen heeft te maken met hogere kosten en die moeten worden doorberekend in de premie om financieel gezond te blijven. Dat is belangrijk voor ons verzekeringsbedrijf maar ook voor onze coöperatie, onze stichting, onze verzekerden, onze aangesloten adviseurs, onze leveranciers en onze medewerkers. Zodat we hopelijk nog heel veel jaar kunnen blijven doen waar we goed in zijn.

“Samen doen we goed voor een ander”

Nieuw kantoorpand

We zijn een nieuw kantoorpand aan het bouwen. De bouw loopt op schema. De planning is dat we in de zomer 2024 kunnen verhuizen. Het pand is ontworpen door Piet Boon en wordt echt een groene campus. Elke keer dat ik op de bouwplaats kom sta ik weer versteld van hoe mooi het wordt. Er wordt hard gewerkt door bouwbedrijf de Geus en het vakwerk is goed zichtbaar.

Stichting Goede Doelen Nh1816

In 1999 heeft Nh1816 de Stichting Goede Doelen Nh1816 opgericht. En in 2013 de coöperatie waarmee onder andere maatschappelijk relevante projecten worden ondersteund. We vinden dit belangrijk, want een duurzame toekomst is iets van ons allemaal. De Stichting wil een bijdrage leveren aan maatschappelijk relevante projecten van organisaties en instanties (ANBI) die voor de financiering van hun activiteiten vaak niet of nauwelijks een beroep op subsidie of andere overheidssteun kunnen doen.

De coöperatie is dé schakel als het gaat om regionale en lokale goede doelen projecten. We werken actief samen met onze lokale adviseurs en klanten. In 2020/2021 stelde onze coöperatie bijvoorbeeld maar liefst 300.000 euro ter beschikking voor initiatieven die zich richtten op het verzachten van de negatieve effecten van de coronacrisis.

Heb je nog tips voor andere verzekeraars?

Daar kan ik kort over zijn. Blijf dicht bij jezelf en de klant. Maak duidelijke keuzes en werk met leveranciers en klanten die bij je passen.

Nh1816 Verzekeringen

www.nh1816.nl

Rémon Chattellon bij de ontwerpen van het nieuwe pand.

Schorsen en Opschorten van verzekeringen

Verzekeringen zijn er om te beschermen tegen onvoorziene gebeurtenissen en de (financiële) gevolgen hiervan. Soms is er aanleiding de dekking van een verzekering op te schorten of te schorsen. Hoewel deze termen vaak door elkaar worden gebruikt, zijn er belangrijke verschillen tussen het schorsen en opschorten van verzekeringen. Dit blijkt uit de Uitspraak van de Geschillencommissie Financiële Dienstverlening van KiFiD onder nummer 2022-0702 en datum uitspraak 18 augustus 2022.

Geschorst
Schorsen van een verzekering betekent dat de verzekering tijdelijk wordt stopgezet of geannuleerd, meestal op verzoek van de verzekerde. Dit kan om verschillende redenen gebeuren, zoals bijvoorbeeld wanneer de verzekerde tijdelijk geen gebruik maakt van zijn voertuig of wanneer hij of zij tijdelijk naar het buitenland verhuist. Tijdens de schorsingsperiode is er geen dekking en worden er geen premies betaald. De verzekering kan echter op elk gewenst moment opnieuw worden gestart.

Opgeschort
Opschorten van een verzekering daarentegen betekent dat de verzekering tijdelijk wordt onderbroken als gevolg van niet-betaling van premies of het niet voldoen aan andere voorwaarden in het contract. Dit kan bijvoorbeeld gebeuren als de verzekerde de premie niet op tijd betaalt of als niet wordt voldaan aan de veiligheidsvoorschriften die zijn opgesteld door de verzekeraar. Tijdens de opschortingsperiode blijft de verzekering bestaan, maar er is geen dekking, totdat aan de vereiste voorwaarden is voldaan en de premies zijn betaald.

Casus KiFiD uitspraak
In de uitspraak van KiFiD is er sprake van een ongevallen inzittendenverzekering/ schadeverzekering inzittenden. Wanneer nabestaanden een beroep op de verzekering doen, wijst de verzekeraar dekking af, omdat de overledene niet tijdig zijn premie zou hebben voldaan en daarom de dekking werd geschorst. Na uitblijving van betaling is vervolgens de verzekering beëindigd.

De situatie die ten grondslag ligt aan de niet-bindende uitspraak van de Commissie is de volgende. De verzekerde is door een ongeval met de auto in april 2020 aangetroffen. In juni 2020 is de verzekeraar door een gemachtigde geïnformeerd over het overlijden van de verzekerde. De gemachtigde verzoekt om de verzekering te beëindigen en doet gelijktijdig een beroep tot uitkering vanuit de ongevallenverzekering inzittenden en schadeverzekering inzittenden vanwege het overlijden.

De verzekeraar beëindigt, na ontvangst van de claim in juni 2020, met terugwerkende kracht, de verzekering per 1 mei 2020. Op 16 juni 2020 laat de verzekeraar per e-mail weten dat er sinds september 2019 een premieachterstand was en de getroffen betalingsregeling niet werd nagekomen. Als gevolg hiervan is de dekking van de verzekering op grond van artikel 5b van de algemene verzekeringsvoorwaarden per oktober 2019 geschorst. Daarna is de verzekering per 26 maart 2020 geroyeerd en het royement is onderbouwd met een brief van de RDW. De verzekeraar geeft aan dat er door het niet nakomen van de betalingsregeling geen recht op dekking is.

In september 2020 wordt een proces-verbaal overlegd waaruit blijkt dat de verzekerde in januari 2020 is overleden als gevolg van een eenzijdig ongeval, en pas in april 2020 is gevonden. Op het moment van overlijden was de verzekeringspolis geschorst en nog niet geroyeerd.

De KiFiD-uitspraak geeft inzicht in 1) of de schorsing rechtsgeldig was en 2) de verzekeraar daardoor geen uitkering is verschuldigd.

Wettelijke onderbouwing
In artikel 5 van de algemene voorwaarden is de bevoegdheid van de verzekeraar vastgelegd om een verzekering te schorsen wanneer de premie niet wordt betaald. Op grond van de wet zijn er aanvullende regels waaraan een verzekeraar zich dient te houden bij het beëindigen of schorsen van een verzekeringspolis of de dekking, te weten:
Artikel 7:934 Burgerlijk Wetboek (hierna: BW) bepaalt dat: "[h]et niet nakomen van de verplichting tot betaling van de vervolgpremie kan eerst leiden tot beëindiging of schorsing van de verzekeringsovereenkomst of de dekking, nadat de schuldenaar na de vervaldag onder vermelding van de gevolgen van het uitblijven van betaling vruchteloos is aangemaand tot betaling binnen een termijn van 14 dagen, aanvangende de dag na de aanmaning."

Uit artikel 7:943 lid 3 BW volgt dat artikel 7:934 BW van semi-dwingend recht is. Dit betekent dat niet ten nadele van de consument van dit artikel kan worden afgeweken. Als dus niet op de wettelijk voorgeschreven wijze is aangemaand, kan de schorsing of beëindiging van de dekking niet zijn ingetreden.

Artikel 7:934 BW vereist dat een aanmaning minimaal de volgende informatie moet bevatten:
1) een termijn van ten minste 14 dagen waarbinnen alsnog de premie moet worden voldaan;
2) wanneer de termijn van 14 dagen, ook wel respijttermijn genaamd, aanvangt; en
3) wat de gevolgen zijn wanneer niet binnen 14 dagen na aanvang van de termijn wordt betaald.

Vervolg casus
De verzekeraar heeft op 18 oktober 2019 een aanmaning gestuurd. Hierin staat:

"Wilt u het factuurbedrag binnen 15 dagen na ontvangst van deze aanmaning overmaken naar bankrekeningnummer [bankrekeningnummer verzekeraar] ten name van [naam verzekeraar]? Vergeet bij de betaling niet het factuurnummer te vermelden.
(….)

Als u de openstaande premie niet binnen de gestelde termijn voldoet, zullen wij uw verzekering opschorten conform de algemene verzekeringsvoorwaarden van uw schadeverzekering. Dat betekent dat u vanaf dat moment onverzekerd bent. In geval van schade zal dan niets worden uitgekeerd."

Besluit KiFiD
De commissie oordeelt dat de aanmaning tot betaling van de premie in de brief van 18 oktober 2018 niet voldoet aan artikel 7:934 BW en de dekking daarom niet rechtsgeldig is geschorst.

Weliswaar heeft de verzekeraar in die brief een betalingstermijn en een sanctie op het niet nakomen van de betaling genoemd, maar als sanctie is opschorten genoemd. Dat is niet hetzelfde als schorsen, de sanctie genoemd in art. 5 van de algemene verzekeringsvoorwaarden welke sanctie uiteindelijk ook door de verzekeraar is toegepast.

Bovendien heeft de verzekerde uitstel van betaling gekregen en had de verzekeraar na het uitblijven van betaling binnen de uitstteltermijn opnieuw de verzekerde moeten aanmanen tot betaling. Ook dit heeft de verzekeraar nagelaten. De verzekeraar had de verzekering dus niet mogen beëindigen.

Op basis van de uitspraak dient de verzekeraar:
- dekking te verlenen,
- het verzekerde bedrag bij overlijden op de ongevallen inzittendenverzekering, vermeerderd met de wettelijke rente, uit te keren;
- via de schadeverzekering inzittenden de door de gemachtigde opgevoerde, en niet door de verzekeraar betwiste, kosten te vergoeden.

De geclaimde pro memoriekosten zijn wel terecht afgewezen.

Menny Barendse &
Floris Stokkers

Security Awareness: waar mensen werken, ontstaan kwetsbaarheden

In dit artikel gaan wij in op het menselijk gedrag en leggen wij uit wat het belang van security awareness is als onderdeel van een effectief informatiebeveiligings-managementsysteem.

De meeste bedreigingen van informatiebeveiliging zijn gericht op het manipuleren van menselijk gedrag. Dit blijkt uit de social engineering-technieken die cybercriminelen toepassen om toegang te verkrijgen tot gevoelige informatie en -systemen. Een van de meest voorkomende technieken is phishing, waarbij cybercriminelen via een e-mail proberen om mensen te overtuigen om op een link te klikken of een bijlage te openen. Cybercriminelen proberen het gedrag van mensen te manipuleren door bijvoorbeeld een e-mail te gebruiken die eruitziet als een legitieme e-mail van een vertrouwde organisatie of door urgentie te creëren om snel te handelen.

Beweegredenen achter het klikken

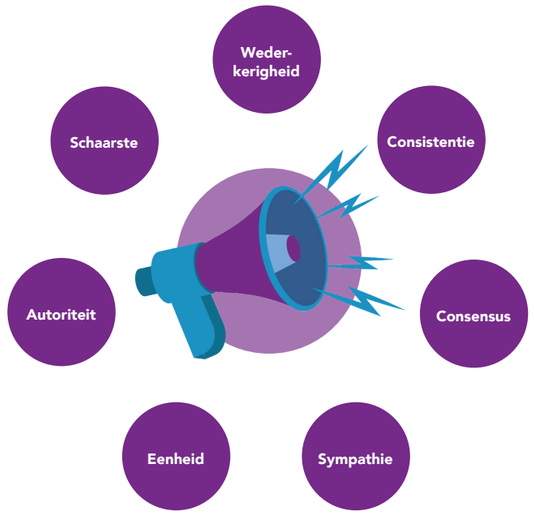
Maar waarom klikken er nog steeds mensen op links in phishing e-mails terwijl veel aandacht wordt besteed aan de risico's die hiermee gepaard gaan? En wat kunnen we eraan doen om dit te voorkomen? Veel keuzes die mensen maken zijn gebaseerd op emoties. Emoties kunnen de interpretatie van informatie en besluitvorming beïnvloeden. Als mensen tijdens het openen van een phishing e-mail niet anders denken dan dat het een 'echte' e-mail is en de inhoud automatisch vertrouwen, zal de kans groot zijn dat zij onbewust de phishinglink of bijlage openen. Dit is immers de makkelijkste weg. En hoewel er in toenemende aandacht voor het creëren van awareness voor dergelijke praktijken, lijkt het kiezen voor de makkelijkste weg ook vaak aan te sluiten bij de gewenste beleving van mensen, namelijk het handelen uit vertrouwen. Daarnaast kan het een trigger zijn om een phishing mail te openen omdat medewerkers een zekere urgentie ervaren; zij kunnen zich zorgen maken over het missen van belangrijke informatie en zouden daarom de phishinglink kunnen openen. Al is het alleen maar om het gevoel te krijgen dat zij niets missen; óók wanneer de klikker de mail niet helemaal vertrouwt.

Naast bovengenoemde redenen kan de druk van een groep, bijvoorbeeld van collega's of de verwachtingen van anderen, invloed hebben op het menselijk gedrag. Gedrag wordt in dit geval beïnvloed vanuit een sociaal perspectief. Sociale beïnvloeding wordt bewust ingezet bij het ontwerpen van phishing mails. Zo wordt zo'n mail vaak verstuurd uit naam van een collega of een bekende. Dit vergroot de kans dat op de mail geklikt wordt, bijvoorbeeld om niet onbeleefd gevonden te worden en uit betrokkenheid naar de betreffende collega.

Lang niet alle phishingmails zijn overigens zorgvuldig opgesteld en vormgegeven. Je kunt als kwaadwillende ook gewoon geluk hebben: er wordt uit automatisme of door slordig handelen heel vaak onbewust op een link geklikt, ondanks eenvoudig te herkennen punten die zo kenmerkend zijn voor een phishing e-mail.

De beïnvloedingsprincipes van Cialdini (zie afbeelding) helpen ons bij het inzichtelijk maken van hoe phishing e-mails werken en waarom mensen vaak in de val lopen. Een aantal van deze principes zijn:

- Consensus: phishing e-mails kunnen medewerkers proberen te overtuigen om op een link te klikken door het zo te laten lijken dat veel mensen dit eerder hebben gedaan;



De 7 beïnvloedingsprincipes van Cialdini

- Autoriteit: phishing e-mails kunnen verzonden worden uit de naam van een bedrijf met een bekende naam;
- Schaarste: phishing e-mails kunnen het gedrag van medewerkers manipuleren door te benadrukken dat de link voor een beperkte tijd toegankelijk is.

Security awareness beleid

Een cyberaanval kunnen wij niet voorkomen, we kunnen de kans daarop echter wel verkleinen door in te spelen op het menselijk gedrag. Dit vereist een combinatie van verschillende methodes.
Zo zou elke organisatie in onze ogen een security awareness campagne moeten ontwikkelen die past bij de organisatie en diens medewerkers (zie pagina 18 over de Pubquiz Cyberellende). Door regelmatig security trainingen te ontwikkelen en deze regelmatig op de agenda te zetten, wordt het veiligheidsbewustzijn van medewerkers vergroot. Het is het van belang dat alle medewerkers de trainingen volgen. Dit geldt uiteraard ook voor nieuwe medewerkers maar zeker ook voor het hoger management. De resultaten van deze trainingen kunnen vervolgens steeds weer worden geëvalueerd om te bepalen of deze effectief zijn en daadwerkelijk een bijdrage leveren aan het kennisniveau en de handelingsbekwaamheid van de medewerkers. De security trainingen bevatten informatie over alle soorten dreigingen waar de organisatie aan kan worden blootgesteld, waarvan de meest bekende voorbeelden phishing en social engineering technieken zijn. Door na afloop van de training de opgedane kennis te toetsen door een quiz of een game, kan een spelelement worden toegevoegd.

Ook het ontwikkelen van phishing simulaties kan bijdragen aan de kennis van de medewerkers. De phishing simulaties helpen de medewerkers om in staat te zijn phishing e-mails te herkennen en voorbereid te zijn in het geval dat er een echte phishing e-mail binnenkomt. Daarnaast kunnen phishingsimulaties medewerkers meer vertrouwen geven om een melding te maken als zij onverhoopt op een phishing e-mail hebben geklikt. De beleidslijnen en procedures die een organisatie hanteert zijn van belang om de juiste gedragscodes en richtlijnen te laten naleven. Door duidelijk beleid en heldere procedures op te stellen rond het veilig omgaan met (vertrouwelijke) informatie en het melden van incidenten, bied je duidelijkheid en handelingsperspectief.

Maar het is ook belangrijk dat medewerkers voldoende tijd (kunnen) nemen voor het lezen van hun e-mail om te voorkomen dat een medewerker haastig op een phishing link klikt. Het kan medewerkers helpen om hen er bewust van te maken dat het in dit licht zinvol kan zijn om een vast tijdstip aan te houden voor het controleren van en reageren op e-mails. Daarnaast is het verstandig om de resultaten van een phishing simulatie met de desbetreffende medewerker te bespreken. Daarbij geef je reflectie, maar ook laat je zien dat de organisatie belang hecht aan hetgeen wordt aangeboden.

Veiligheid op de werkvloer

De ervaren veiligheid op de werkvloer is een bepalende factor voor het gedrag en de ontwikkeling van medewerkers. Naast het herkennen van (cyber)dreigingen, is het van belang dat medewerkers deze melden aan de verantwoordelijke(n) en hierover openlijk durven te praten, zonder angst om te worden afgerekend. Dit zorgt ervoor dat als een dreiging daadwerkelijk plaatsvindt, bijvoorbeeld in de vorm van een phishinglink die wordt geopend door een medewerker, de medewerker dit durft te melden.

Vaak durven medewerkers in een onveilig werkklimaat niet aan te geven dat ze op een phishing link geklikt hebben of ze weten niet bij wie ze terecht kunnen op het moment dat er sprake is van een beveiligingsincident. Het niet weten of durven vertellen van de gebeurtenis draagt bij aan de afbreuk van het zelfvertrouwen van de medewerker. Deze kan zich schamen en zich zorgen maken over de gevolgen die zijn actie heeft voor de organisatie. Om te kunnen anticiperen op dergelijke incidenten is het belangrijk om medewerkers regelmatig te informeren over de procedures die zij moeten volgen wanneer zij te maken krijgen met een beveiligingsincident. Daarnaast is het belangrijk om een cultuur te ontwikkelen waarin medewerkers zich voldoende vertrouwd voelen om ook minder positieve zaken te delen met de organisatie. Dus: ontwikkel een degelijk awareness-programma. Het vroegtijdig op de radar hebben van dreigingen voorkomt immers verdere schade! We willen u daarbij graag helpen en ondersteunen.

Annebeth Groen, Frederike Gieles & Anna Navasardyan

Interview Jacob Iedema EOC Scheepsverzekeringen

Naast de reguliere audits via InAudit Audit Services kunnen we ook ondersteunen in informatiebeveiliging. Dit doen we via de de pijler Information Security.

Informatiebeveiliging is een essentieel onderdeel van de governance en het risicomanagement. Maar het is wel een onderdeel dat om specifieke kennis en deskundigheid vraagt. InAudit verzorgt de CISO-rol bij EOC Scheepsverzekeringen. We spreken met Jacob Iedema over de uitdagingen binnen EOC.

Even voorstellen
Mijn naam is Jacob Iedema, ICT Manager bij EOC Onderlinge Schepenverzekering u.a. in Meppel. Ik ben 56 jaar en woon met mijn gezin in Oudeschoot bij Heerenveen. In 2003 ben ik in dienst gekomen bij EOC en daarvoor heb ik meer dan 10 jaar op detacheringsbasis voor EOC gewerkt. In het begin was mijn functie software developer en later ben ik doorgegroeid naar ICT Manager.

Wie is EOC?
EOC is een Onderlinge Scheepsverzekeraar met ankers in de beroepsvaart, pleziervaart, charter- en passagiersvaart en wonen op het water. EOC heeft vestigingen in Meppel en Zwijndrecht waar we met ongeveer 85 collega's als stabiele, betrouwbare specialist onze leden en verzekerden terzijde staan met onze verzekeringen en deskundig advies.

Samen waken wij iedere dag over een behouden vaart voor al onze schippers, in zowel beroeps- als pleziervaart. Op ons kun je varen!

Wat maakt ons uniek:
- 24/7 bereikbaarheid bij schade en snelle afhandeling zodat de schipper zo snel mogelijk weer kan varen
- Geen callcenter en keuzemenu's: direct een duidelijk antwoord
- Totaalaanbod aan verzekeringen + aanvullende service speciaal voor schippers
- Eerlijke premies: EOC heeft geen winstoogmerk
- Schade-, inspectie- en certificeringsexperts in huis
- Betrokken medewerkers die vaak zelf uit de vaart komen en net zo van de vaart en het water houden als u.

Wat houdt ons bezig?
De energie transitie speelt ook in de scheepvaart een belangrijke rol. In de beroepsvaart zijn er veel innovaties op het gebied van elektrificatie, alternatieve krachtbronnen (bijv. waterstof), gebruik van zonnepanelen op schepen en semi-autonoom varen. Wij volgen deze actief om ervoor te zorgen dat we met onze kennis deze nieuwe risico's voor onze leden goed kunnen afdekken. Daarnaast geven wij advies over preventieve maatregelen om de kans op schade zo klein mogelijk te maken.

Mijn ervaringen in de verzekeringssector
Van de buitenkant wil nog wel eens een beeld ontstaan dat de verzekeringssector niet de meest spannende of uitdagende sector is op IT gebied. Ook ik wist niet precies wat ik moest verwachten toen ik voor het eerst voor EOC aan de slag ging. In de 30 jaar dat ik in de verzekeringssector als IT'er actief ben heeft het me echter geen moment verveeld. Het was, en is nog steeds, verrassend om te zien hoeveel vernieuwing en innovatie er plaatsvindt binnen EOC. Ontwikkelingen vinden plaats op uiteenlopende onderwerpen zoals verzekeringsproducten, klantbeleving, interne processen, digitalisering, cyber security, wet & regelgeving, etc. Het is geweldig om met ons hecht en gemotiveerd team van collega's te werken aan voortdurende vernieuwing en verbetering van onze organisatie. Daarbij komen zoveel ideeën uit de organisatie dat we deze goed moeten wegen en prioriteren om ze vervolgens in een roadmap te plaatsen. Voor de uitvoering, beheer en bewaking van trajecten maken we gebruik van de Obeya methode. Met Obeya maak je visueel zichtbaar waar de organisatie staat in de realisatie van haar doelen en strategie. Je zou natuurlijk verwachten dat dit allemaal digitaal staat, maar in dit geval zijn het ook fysieke white boards op een wand wat het heel overzichtelijk maakt en het personeel wordt op deze manier ook betrokken omdat ze er dagelijks langs lopen en kunnen zien waar we als organisatie mee bezig zijn en hoe de voortgang is.

"Samen waken wij iedere dag over een behouden vaart voor al onze schippers, in zowel beroeps- als pleziervaart"

Uitdagingen in de IT-sector
EOC is als verzekeraar een IT gedreven organisatie. Vrijwel alle processen leunen zwaar op IT oplossingen. Voor een deel hebben we te maken met dezelfde IT uitdagingen waar alle bedrijven mee te maken hebben. Wij hebben daarnaast echter te maken met een aantal aanvullende IT uitdagingen.

Niche markt
EOC beweegt zich in een niche markt namelijk het verzekeren van schepen in de plezier- en beroepsvaart. Het opereren in een niche markt brengt hele specifieke eisen en wensen met zich mee voor de IT systemen en met name de IT applicaties. Dit heeft er toe geleid dat we veel software die we gebruiken zelf ontwikkelen. Met een team van 6 developers en een business analist bouwen en onderhouden we deze applicaties. De uitdaging zit in het kunnen bijhouden van alle interne en externe ontwikkelingen en er gelijktijdig voor zorgen dat alle applicaties stabiel en soepel werken en meegroeien met ontwikkelingen binnen IT.

Cybersecurity
Eén van de grootste uitdagingen waar iedereen mee te maken heeft is cybersecurity. We werken voortdurend aan het controleren en verbeteren van de beveiliging van onze IT omgeving. Naast de gebruikelijke cybersecurity oplossingen zoals firewalls en antivirus oplossingen voeren we diverse andere activiteiten uit.

De Obeya methode

Vervolg Jacob Iedema
EOC Scheepsverzekeringen

We zijn aangesloten bij een Computer Emergency Response Team die ons informeren en adviseren over actuele cyberdreigingen. Elke maand krijgen onze medewerkers een cyber awareness training aangeboden. Periodiek voeren we PEN-testen uit om onze IT omgeving op kwetsbaarheden te testen. EOC heeft een informatiebeveiliging framework opgezet welke gebaseerd is op de good practice informatiebeveiliging van DNB. Met behulp van dit framework toetsen we ook zelf alle processen en geïmplementeerde maatregelen op het gebied van informatiebeveiliging.

Data gedreven organisatie en algoritmes
Data wordt steeds belangrijker in een organisatie. Niet alleen voor de dagelijkse operationele zaken, rapportages en analyses maar data is ook nodig voor je besluitvormingsproces. Algoritmes gaan binnen bedrijven een steeds grotere rol spelen en deze zijn weer afhankelijk van data. Met algoritmes kunnen systemen, op basis van een set instructies en data, keuzes maken die normaliter door medewerkers uitgevoerd worden. Dit alles vraagt een gedegen datastrategie en is een onderwerp waar we nu volop mee bezig zijn.

Samenwerking InAudit
We werken al vele jaren tot volle tevredenheid en plezier samen met InAudit. In de eerste plaats zijn dat uiteraard de reguliere audit werkzaamheden. Vanuit deze hoedanigheid kijkt InAudit ook met mij mee om de IT omgeving te beoordelen en te kijken of onze werkzaamheden worden uitgevoerd volgens de opgestelde processen. Dat is ook de reden dat we de samenwerking met InAudit hebben opgezocht bij het opstellen van ons informatiebeveiliging framework. Dit heeft geresulteerd in een framework waar zowel InAudit op kan steunen als EOC goed mee uit de voeten kan.

Sinds ruim een jaar huren we via InAudit een CISO in. In 2022 was dit Annebeth Groen en sinds januari is dat Jens Meuleman. De CISO ondersteunt ons 2 dagen in de week met alle cybersecurity gerelateerde onderwerpen. Ook is de CISO verantwoordelijk voor het controleren en beheren van ons informatiebeveiliging framework. Het inzetten van een CISO heeft er in geresulteerd dat cybersecurity onderwerpen niet naar de achtergrond verdwijnen maar voortdurend de aandacht krijgt die het moet hebben. Daarnaast geeft het mij als ICT Manager de ruimte om weer andere onderwerpen op te pakken. Een win-win situatie!

www.eoc.nl

Locatie IJsselstein

Sinds 1 januari 2023 hebben we naast ons hoofdkantoor in Leuvenheim nu ook een 2e locatie.

Samenwerken
In ons vak geldt goede samenwerking als voorwaarde voor het uitvoeren van kwalitatieve onderzoeken, niet alleen de samenwerking met u als klant, maar ook binnen het team. Onze medewerkers wonen verspreid over het hele land. Daardoor zijn ze vaak redelijk in de buurt van u, maar niet van elkaar. Daar hebben we verandering in gebracht.

Ten tijde van de corona-lockdowns hadden we geen keuze: vanuit eigen huis auditen. Dat was wennen voor iedereen, maar daar vonden we een goede modus in. Ook onze nieuwe collega's en klanten hebben we – op afstand – goed opgevangen. Maar ideaal was het niet. Nu we weer vrij kunnen bewegen, merken we dat we niet alleen u weer meer opzoeken, maar ook elkaar.

Locatie IJsselstein
Om hierbij de efficiëntie en effectiviteit van onze werkzaamheden te verhogen, hebben we een tweede locatie in IJsselstein geopend. Overleggen en afstemmingen gaan een stuk sneller en makkelijker. We merken dat ook het werkplezier hiermee stijgt.

Benieuwd naar een sfeerimpressie? Hierbij enkele foto's van onze nieuwe werkplek.

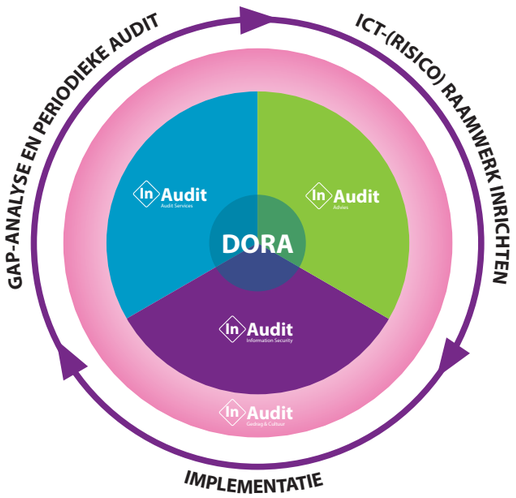
DORA
Digital Operational Resilience Act

Binnen de financiële sector is sprake van verregaande digitalisering en deze ontwikkeling blijft zich voortzetten. In combinatie met de grote hoeveelheid (persoonlijke) data en de ontwrichting van de samenleving bij omvangrijke verstoringen, zorgt dit ervoor dat het risico op cyberaanvallen in de financiële sector onverminderd hoog is. Om dit risico te beperken heeft de Europese Commissie een nieuwe verordening aangenomen, genaamd DORA (Digital Operational Resilience Act).

De DORA verordening moet de digitale weerbaarheid van de financiële sector in Europa versterken, zowel door de inzet van preventieve als correctieve maatregelen. Organisaties en hun IT-dienstverleners zouden cyberaanvallen en andere soorten IT-gerelateerde verstoringen en bedreigingen moeten kunnen weerstaan door het implementeren van best practices. DORA stelt eisen aan de financiële sector aan de hand van een vijftal pijlers, waaronder IT-incidentenbeheer, IT-risicomanagement en het periodiek testen van digitale weerbaarheid. Ook ligt er nadruk op de beheersing van IT-risico's bij uitbestedingen en op de uitwisseling van informatie binnen de sector en met de toezichthouders.

De DORA verordening is eind 2022 aangenomen en treedt vanaf 17 januari 2025 in werking. Dat betekent dat financiële entiteiten die binnen de reikwijdte van de verordening vallen nog twee jaar hebben om te voldoen aan de voorschriften.

Proces voorbereiding DORA



Bij InAudit verenigen wij onze verschillende expertises om bedrijven in de financiële sector, zoals dat van u, te helpen met het implementeren van DORA. Overigens is het ook voor organisaties buiten de scope van DORA verstandig om de weerbaarheid te verbeteren. In dit artikel geven wij per expertise aan hoe wij hieraan kunnen bijdragen.

Onze expertises:
- Audit Services,
- Information Security,
- Gedrag & Cultuur en
- Risicomanagement

Waar mogelijk bundelen wij onze krachten om u te helpen.

We kunnen ons voorstellen dat het ingewikkeld is om de vereisten die DORA stelt te vertalen naar uw organisatie. Neem gerust contact op met een van onze consultants voor een vrijblijvend gesprek.

Risicomanagement

De kern van DORA wordt gevormd door artikel 6: het kader voor ICT-risicobeheer. Financiële entiteiten moeten, als onderdeel van hun algemene risicobeheersysteem, beschikken over een solide, alomvattend en goed gedocumenteerd kader voor de beheersing van ICT-risico's. Dit betekent dat een entiteit strategieën, beleid, procedures, protocollen en instrumenten tot zijn beschikking heeft om informatie en ICT-activa te beschermen tegen ongeoorloofde toegang en gebruik. DORA schrijft vervolgens in gedetailleerde bewoordingen voor wat een financiële entiteit ingeregeld moet hebben. Die voorschriften eindigen niet bij de poorten van uw eigen organisatie, want u bent tevens verplicht het ICT-risico van uw IT-leveranciers te integreren in uw eigen kader voor ICT-risicobeheer. Het belang van adequaat uitbestedingsmanagement wordt met DORA wederom bevestigd.

Onze consultants van InAudit Advies hebben kennis van de DORA voorschriften en helpen u graag bij de naleving ervan. Dat kan via deeltrajecten, zoals de uitvoering van een gapanalyse of via de aanscherping van uw uitbestedingsbeleid en -regelingen, maar ook via integrale implementatietrajecten zodat uw kader voor ICT-risicobeheer op orde is, zowel in opzet als in werking. Uiteraard zoeken onze consultants daarbij naar een gezonde balans tussen proportionaliteit, best practices en uw eigen beleidslijnen.

Information Security

De doelstelling van DORA is het verhogen van de cyberweerbaarheid van (financiële) organisaties. Het managementsysteem dat u daarvoor inricht moet u ook implementeren, testen, monitoren en periodiek uitdagen op effectiviteit (en efficiency). Dit alles moet u ook aantoonbaar maken.

Het implementeren van cybersecuritymaatregelen vergt een nuchtere houding, een gezond verstand, maar vooral een hands-on aanpak. Daarin proberen onze consultants zich te onderscheiden. Met de kennis en ervaring die we opdoen bij vergelijkbare organisaties kunnen we zorgen voor effectieve voortgang, maar zijn we tevens een goed klankbord om 'lessons learned' te delen. We helpen u graag !

Audit Services

Vanuit InAudit Audit Services kunnen wij op verschillende momenten van de implementatie van de DORA-wetgeving met u meekijken. Allereerst kunnen wij voor u een gap-analyse uitvoeren. Dit stelt ons in staat om eventuele tekortkomingen te identificeren en voor u in kaart te brengen wat er moet gebeuren om te voldoen aan de vereisten vanuit DORA. Zo'n analyse geeft daarmee een helder inzicht in wat u te doen staat zodat u kunt prioriteren en plannen.

Naast bovengenoemde gap-analyse die vóór de inwerkingtreding van DORA kan worden uitgevoerd, staat uw auditteam paraat om de implementatie van DORA te toetsen. Ook hieraan verbinden we, zoals u van ons gewend bent, aanbevelingen die u kunt gebruiken om uw bedrijfsvoering in lijn te brengen met deze nieuwe regelgeving.

Gedrag & Cultuur

Ook vanuit Gedrag & Cultuur kunnen we op een aantal vlakken met u meedenken die in het kader van DORA belangrijk zijn. Zo legt DORA de nadruk op de inrichting van een aantal governance-aspecten. Hierbij is het zoals altijd van belang dat degenen die verantwoordelijk worden gemaakt voor, in dit geval bijvoorbeeld het ICT-risicobeheer ook daadwerkelijk deze rol op zich nemen. Hoe gaat u dit inbedden in de organisatie? En hoe zorgt u dat de verantwoordelijke deze rol ook werkelijk kan en gaat vervullen? Ditzelfde geldt ook voor het inrichten van het crisiscommunicatieplan dat van kracht wordt bij ernstige ICT-gerelateerde incidenten. En zo bevat DORA nog een aantal elementen waarbij het loont om hier goed over na te denken.

Artikel 13 van DORA gaat over voorschriften rond scholing en ontwikkeling; óók een onderwerp dat raakt aan Gedrag en Cultuur. Dit artikel schrijft onder meer voor dat organisaties bewustmakingsprogramma's moeten ontwikkelen voor álle werknemers. De mate van complexiteit van deze programma's moet passen bij het takenpakket van de betreffende personeelsleden. Dit geldt ook voor het hoger leidinggevend personeel. Hoe denkt u dit te gaan oppakken? Hoe gaat u dit opnemen in uw opleidings- en/of geschiktheidsplan? En waar let u op als u dit gaat uitbesteden? In bredere zin besteedt DORA sowieso veel aandacht aan het continu signaleren en benutten van verbeterpotentieel. En ook dit is een onderwerp waar het loont om met aandacht naar te kijken: hoe gaat u dit inrichten? Hoe zorgt u dat dit daadwerkelijk, tijdig en volledig gebeurt?

Wat kunnen wij vanuit InAudit voor u betekenen?

Wij helpen u graag met het in beeld brengen van de regelgeving, een plan van aanpak en de bemensing om snel voortgang te realiseren.

Wij kunnen u ondersteunen bij het aanscherpen en structureren van de beleidsmatige opzet, zodat deze in lijn is met de vereisten vanuit DORA.

Wij kunnen u adviseren over het implementeren van dit beleid zodat compliance met DORA aantoonbaar is. Oók als het gaat om het aantoonbaar in control zijn wat betreft door u uitbestede werkzaamheden.

Wij kunnen u ondersteunen bij het rapporteren over ICT-gerelateerde incidenten. U kunt dan denken aan advies over het vormgeven van een beoordelingsformulier om ICT-gerelateerde incidenten te categoriseren. Wij kunnen u ook helpen bij het opstellen van een rapportageformat.

Wij kunnen een readiness-assessment of gap-analyse voor u uitvoeren.

Wij kunnen u adviseren over het organiseren van een PEN-test, en/of het laten uitvoeren hiervan binnen uw gehele uitbestedingsketen.

Wij kunnen met u meedenken over het inrichten van awareness-programma's en opleidingsprogramma's.

Wij kunnen u adviseren over het optimaal benutten van verbeterpotentieel.

Team DORA

Vragen of wilt u meer informatie? Neem gerust even contact met ons op. We denken graag met u mee.

Frederike Gieles
Senior Auditor en
Consultant Gedrag & Cultuur
06-11 09 69 89

Annebeth Groen
Auditor en CISO
06-25 10 55 45

Niels Bokkers
Senior Risk Consultant
06-15 43 67 74

Robert Verweij
Auditmanager Audit Services
06-25 29 69 67

Ronald van de Langenberg
Algemeen Directeur InAudit
06-24 48 68 92

De wereld van … Daniël Tiemstra

Wie zijn nu de mensen van InAudit. Elke keer laten wij je kennismaken met één van onze collega's in de rubriek 'De wereld van…'. Deze keer leer je Daniël Tiemstra beter kennen. We stelden hem de volgende vragen.

Wie is Daniël Tiemstra?
Ik ben 30 jaar oud en woon samen met mijn vrouw Monica en dochter Lucia (8 maanden) in Leerdam. Sinds april 2022 werk ik als auditor bij InAudit.

Waar ben jij opgegroeid?
Ik ben opgegroeid in Sprang-Capelle, een mooi Brabants dorpje. Gemoedelijk en gezellig, het bourgondische leven heb ik daar leren waarderen. Na de middelbare school ben ik in Rotterdam gaan studeren en daar gelijk op mijn 18e gaan wonen. Ik heb daar 10 jaar gewoond. Met de huizenprijzen is het wat makkelijker om niet in de stad te gaan wonen, maar de reuring mis ik nog wel.

Wat is je leukste schoolherinnering?
Onder het mom van een eindexamenboek hebben we docenten een enquête in laten vullen met daarin de vraag: 'Waar zou je 's nachts voor wakker gemaakt willen worden?' Daar werd vaak iets ingevuld als een Bossche bol of een speciaal biertje. Met 3 vrienden zijn we vervolgens diep in de nacht als examenstunt met al die dingen bij de docenten thuis langs geweest. Leverde mooie taferelen, met grotendeels leuke reacties, op (en een paar slaapkoppen). In die tijd stonden docentenadressen nog in de schoolgids en was er nog geen AVG en privacy bewustzijn.

Vertel eens over je eerste baan?
Voor InAudit heb ik ruim zes jaar gewerkt voor een ander auditbureau. Het betrof een certificerende instelling die hoofdzakelijk ISO-certificeringen (o.a. ISO27001) uitvoert. Ik was daar als auditor en projectleider hoofdzakelijk actief voor de toetsing van het dealernetwerk zoals dealercontracten en importeursvereisten van een aantal automerken.

Van welke hobby krijg jij energie?
We hebben thuis een hele uitgebreide spelletjeskast. De laatste jaren zijn er heel veel nieuwe leuke spellen op de markt gekomen. Met vrienden of familie brengen we zo graag een zondag door, super gezellig. Schaken is ook een hobby van mij.

Verliefd, verloofd of getrouwd?
Vorig jaar maart ben ik getrouwd met Monica. We hebben een schitterende dag gehad met een mooi feest.

Wat is je favoriete vakantiebestemming?
De laatste 5 jaar heb ik een aantal mooie vakanties gehad, bijvoorbeeld een aantal weken backpacken in Georgië en het jaar daarna in Colombia. In beide vakanties waren de hoogtepunten de meerdaagse trektochten door de bergen. Nu met een kleine wordt het een uitdaging om dat vorm te geven, maar daar zijn we hard over aan het nadenken.

Wat is je favoriete muziek/liedje?
Onderweg naar klanten door het hele land breng ik best wat tijd door in de auto. Wanneer er muziek op staat is mijn smaak vrij breed; van Bach tot Metallica of The War on Drugs. Tegenwoordig luister ik voornamelijk podcasts; informatief, verhalen of actualiteiten. Mocht iemand tips hebben laat het me weten.

Daniël Tiemstra

Pubquiz Cyberellende

Op een leuke interactieve manier brengt Ronald van de Langenberg al jaren informatiebeveiliging bij onze medewerkers onder de aandacht. Op het IIA congres 2022 werd de pubquiz gewaardeerd met een 8,2. Dit jaar in juli zal de pubquiz daarom op de IIA International Conference 2023 worden herhaald.

Maandelijkse Pubquiz bij InAudit
Sinds een lange tijd is de Pubquiz Cyberellende vast onderdeel van onze maandelijkse Vaktechnische Overleggen. Om een goede, brede basis te bieden en op de hoogte te zijn van relevante ontwikkelingen op het gebied van informatiebeveiliging, worden elementen thematisch behandeld. Zo behandelen we interne vraagstukken, maar ook relevante ontwikkelingen voor onze klanten. En dit vindt niet plaats in de vorm van een presentatie, maar in een interactieve pubquiz. En hoewel 'meedoen is belangrijker dan winnen' de hoofdgedachte is, eindigen onze collega's maar al te graag met een topscore.

IIA Congres juni 2022
Sinds 2021 zijn wij als partner verbonden aan het IIA, onze beroepsgroep. Samen met de partners ondersteunen wij de organisatie om het auditvak verder te ontwikkelen.

Onze intern zeer gewaardeerde Pubquiz Cyberellende sloot daarom goed aan om te presenteren tijdens het IIA Congres. Op een vrolijke, interactieve manier zijn in een hoog tempo onderwerpen voorbij gekomen, variërend van 'vormen van malware', 'wat doet de overheid', tot aan 'hacker films' en 'recente hacks'. De pubquiz is goed ontvangen en werd in de evaluatie met een 8,2 boven het gemiddelde van alle presentaties beoordeeld. De pubquiz werd ervaren als 'waardevol' en 'actief'.

International Conference 2023
Dit jaar pakken we het nog groter aan. We zijn uitgenodigd om op de IIA International Conference 2023 te spreken. En hoewel de internationale markt niet direct onze focus heeft, is het natuurlijk een eer om onze inzichten met een breed internationaal publiek te delen.

Klantevalutie 2022

Hoe ervaren onze klanten de interne audit dienstverlening van InAudit Audit Services (verder genoemd InAudit)? Om hierachter te komen vragen wij onze klanten, jaarlijks een evaluatieformulier in te vullen. Op dit formulier geven onze klanten aan hoe zij onze dienstverlening waarderen.

Daarbij is niet alleen het oordeel over de inhoudelijke kwaliteit van belang, maar ook de waardering van het samenwerkingsproces. Door meer inzicht te krijgen in de waardering van de gehele dienstverlening kan InAudit zich continu blijven ontwikkelen en haar werkwijze aanpassen om beter aan te sluiten bij de wensen van onze klanten.

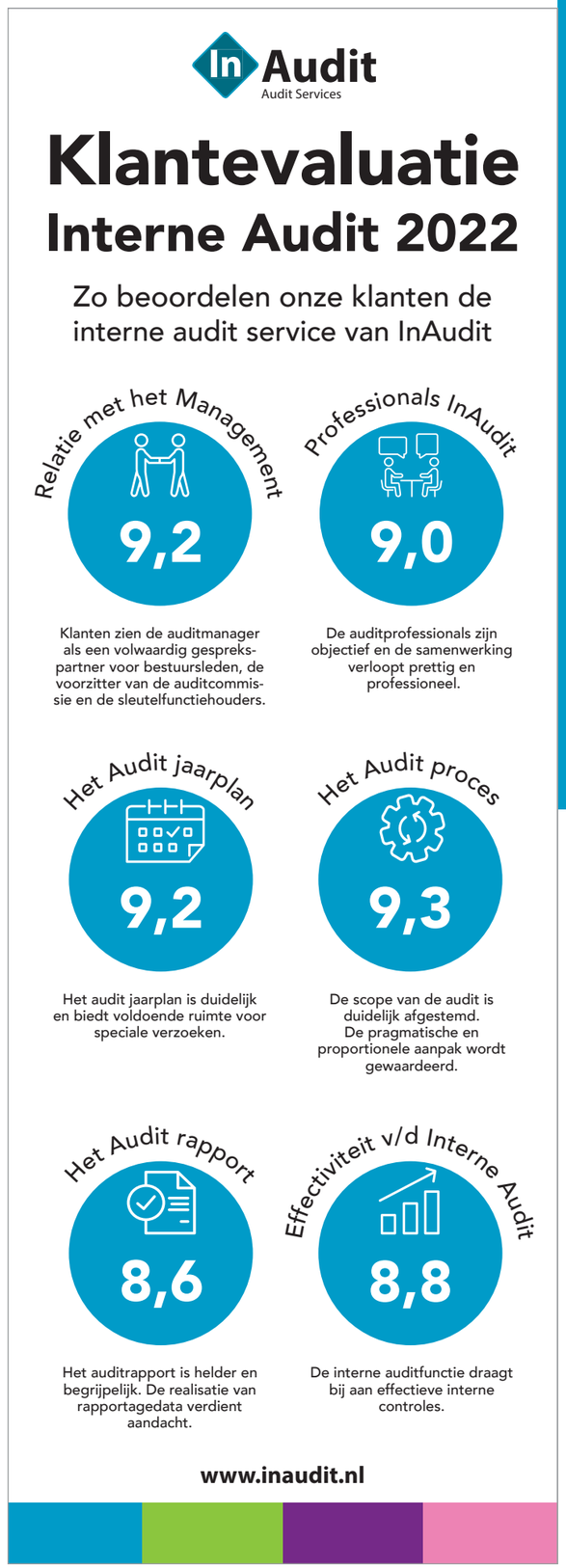
De uitkomst
Vorig jaar waren we zeer tevreden over de uitslag van de klantevaluatie met een gemiddelde waardering van een 9,4. Dit jaar is de uitkomst nog steeds boven onze verwachting met een 9,0. Een mooie waardering voor het werk van onze collega's, maar wat ons betreft blijft het daar niet bij. Ook in 2023 willen wij ons blijven ontwikkelen.

Zo geven wij het realiseren van de afgesproken planning meer aandacht. De aangereikte verbeterpunten bespreken wij in ons maandelijks vaktechnisch overleg, alsook met de individueel betrokken auditors. Daarbij wordt per klant bekeken welke verbeteringen wenselijk zijn. In de infographic hiernaast kunt u in de scores zien per onderdeel.

En verder...
Het jaar 2022 is een mooi jaar geweest. Een jaar dat we ons 10-jarig jubileum hebben gevierd met ons team. Het landelijke personeelstekort speelt ook bij ons en dat gaf soms wat druk op de bezetting. In april 2022 is Daniël Tiemstra gestart als auditor en in september mochten we Jens Meuleman en Wessel Westerveld verwelkomen als junior auditor.

Concluderend kunnen we vaststellen dat 2022 in meerdere opzichten een goed jaar is geweest, zowel voor u als voor ons. Wij willen u hier hartelijk voor bedanken en gaan aan de slag met de uitdagingen die dit jaar voor ons staan.

Wij bedanken u nogmaals voor uw feedback.



Meer focus met de A3 methodiek

InAudit gebruikt de A3 methodiek om meer focus aan te brengen in de organisatie. We hebben met de A3 methodiek een nuttig management tool dat ons helpt om onze plannen en ambities inzichtelijk te maken evenals de realisatie daarvan.

InAudit en de A3 methodiek

InAudit is de afgelopen jaren sterk gegroeid op meerdere vlakken. Zo hebben we ons klantenbestand substantieel zien groeien, hebben we meerdere nieuwe collega's mogen verwelkomen, zijn we actief op meerdere markten en bieden we meerdere producten aan vanuit onze diverse expertises.

In het tweede halfjaar van 2022 hebben we de behoefte besproken om onze strategische uitgangspunten specifieker te benoemen en gewenste doelen meer gestructureerd te managen. We zijn daarom op zoek gegaan naar een middel dat ons hierbij helpt. Na afweging van verschillende methodieken zijn we uitgekomen op de A3 methodiek.

Voor de pijlers Audit services en Gedrag & Cultuur hebben we inmiddels een A3 opgesteld. De plannen hebben onderlinge samenhang, zodat de gezamenlijke richting wordt ondersteund. Bij het opstellen van deze A3 plannen hebben de algemene uitgangspunten van InAudit overall als basis gediend zoals onze missie:

Wij zijn er om u te helpen!

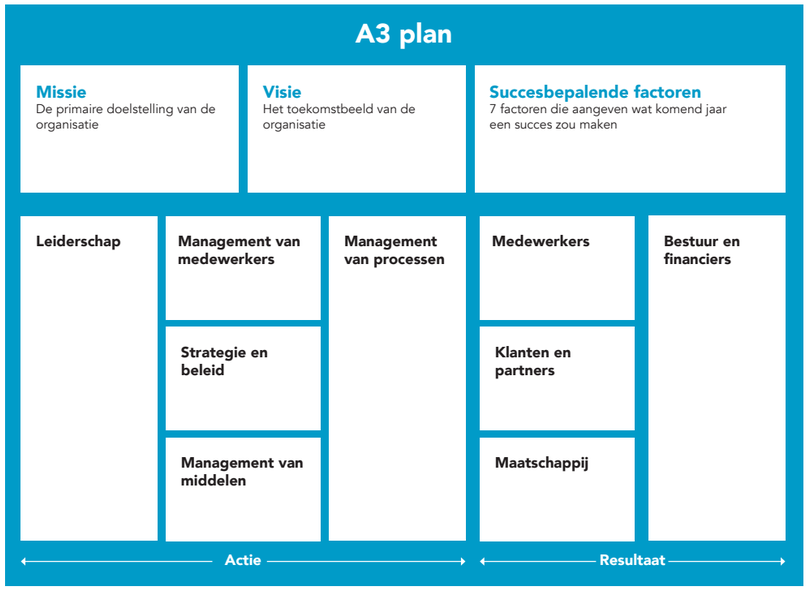
Structurele aanpak

Door de structurele aanpak die de A3 methodiek nastreeft zijn we binnen Audit Services 'gedwongen' om heel concreet na te denken over wie we nu zijn en willen zijn, hoe we dit (willen) uitdragen en waar we eigenlijk naartoe willen, met wie en met welke producten.

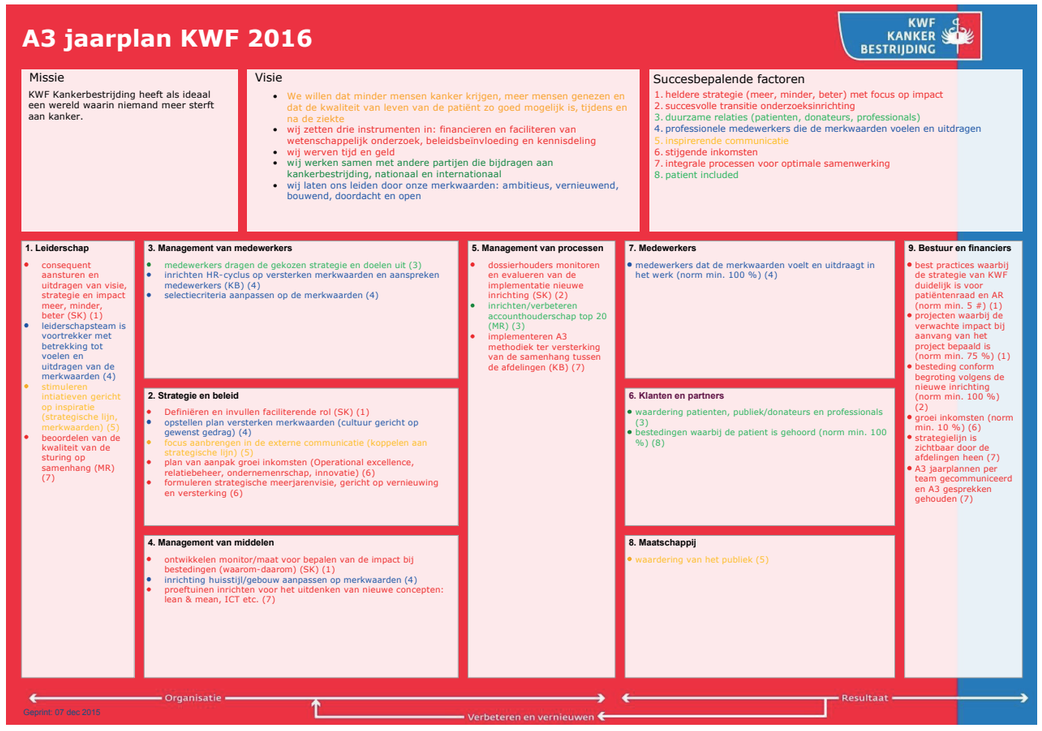
In 2023 blijven we samen met alle collega's van Audit Services het A3 plan monitoren en waar nodig bijsturen.

Meer focus, minder papier

De A3 methodiek is ongeveer 12 jaar geleden ontwikkeld bij de Dienst Justitiële Inrichtingen (DJI) in samenwerking met TNO Management Consultants, nu RONT Management Consultants. Inmiddels werken honderden organisaties met de A3 methodiek. De A3 methodiek wordt toegepast bij organisaties die de sturing willen verbeteren. Niet door middel van omvangrijke planningssystemen, maar door de nadruk te leggen op het opstellen van een overzichtelijk plan (op één A3), het houden van periodieke gesprekken over dat plan én het verzamelen van relevante sturingsinformatie over de voortgang en over de effecten.



De verdeling van het A3 plan in Resultaat gebieden en Actie gebieden.



Een voorbeeld van het A3 plan van KWF

De A3 methodiek maakt gebruik van het INK Managementmodel, dat al vele jaren wordt toegepast bij het beoordelen en verbeteren van organisaties. In de A3 methodiek is vanuit die achtergrond een set van tools ontwikkeld om de daadwerkelijke sturing op verbetering en vernieuwing te ondersteunen. En het werkt! Organisaties die de A3 methodiek toepassen zijn enthousiast over de werking en bij audits wordt herkend dat de Plan-Do-Check-Act cyclus op beleidsniveau wordt gesloten. En wie wil dat niet!

De kernbeloften van de A3 methodiek zijn:

- richting,
- consistentie,
- focus,
- feedback,
- en commitment.

Dat is vooral zichtbaar als organisaties niet alleen het A3 (jaar)plan maken maar er ook daadwerkelijk mee sturen. De A3 gesprekken in teams en het contact tussen manager met zijn of haar leidinggevende zijn cruciaal. Zij vormen een belangrijke pijler van de methodiek. Door in een A3 plan de nadruk te leggen op die onderwerpen waar de organisatie op wil verbeteren, versterken of vernieuwen blijft een plan slank en overzichtelijk.

Je stelt een A3 plan op met het MT, met het team of een delegatie daarvan. Nooit in je eentje achter het bureau. Tijdens het opstellen van het A3 plan stem je af wat je bedoelt met belangrijke beleidsonderwerpen of onderwerpen die je wilt verbeteren. Je werkt met elkaar die prioriteiten uit in resultaten en acties, zie afbeelding op pagina 20.

Plan-Do-Check-Act cyclus

Nieuwgierig naar de methodiek: lees meer op www.a3plan.nl.

Datakwaliteit en de Wet Toekomst Pensioenen

Beheersing van de datakwaliteit staat bij veel organisaties op de agenda, maar bij weinig organisaties is de urgentie zo hoog als bij pensioenfondsen die in het kader van de WTP het transitieproces willen ingaan. De risico's zijn namelijk aanzienlijk indien na de transitie blijkt dat de datakwaliteit onvoldoende werd beheerst. Dat geldt uiteraard voor de deelnemers, maar ook voor de fondsbestuurders. Tel daarbij op de enorme complexiteit van veel pensioenregelingen, alle uitzonderingen en historische data, alle veranderingen in de uitvoering en dan is het duidelijk: de sector staat voor een grote uitdaging !

Risicobeheersing

Pensioenfondsen die willen besluiten om in te varen moeten aantoonbaar documenteren dat ze alles hebben gedaan om eventuele problemen in de datakwaliteit in beeld te hebben en op te lossen. Om pensioenfondsen en pensioenuitvoerders hierbij een normenkader te geven, heeft de Pensioenfederatie in oktober 2022 een 'Kader Datakwaliteit' gepubliceerd. Dat kader beschrijft 5 fasen die het pensioenfonds moet doorlopen om tot een verantwoord besluit tot invaren te komen. Dat besluit zelf is fase 6.

Omvangrijk project

Van de 6 fasen die het Kader Datakwaliteit beschrijft zijn met name fase 2 en 3 behoorlijk omvangrijk, vooral omdat de fondsen veel moeten analyseren en documenteren. Bovendien zal het proces niet helemaal lineair zijn. Analyses moeten zo nu en dan opnieuw met nieuwe kennis worden uitgevoerd. Een blik op de (Excel) bijlage A6 laat een lijst met meer dan 60 KDI's (key data items) zien en pakweg 20 kolommen met daarin inhoudelijke beoordelingen. Alleen dat levert al pakweg 1200 cellen op die moeten worden gedocumenteerd. Overigens zouden we niemand willen adviseren om dit in Excel te gaan bijhouden. In fase 5 gaat een externe accountant, voorafgaand aan de besluitvorming, op basis van een vooraf gedefinieerd programma, deze werkzaamheden beoordelen.

Oud nieuws ?

Nu is dit niet de eerste keer dat van pensioenfondsen wordt verlangd dat zij naar de datakwaliteit gaan kijken. Maar ook daarin schuilt een risico, namelijk de gedachte dat we het nu wel weten. De scherpte is wellicht wat weggezakt. In 2022 voerde DNB een sectorbrede analyse [1] uit, waaruit onder meer naar voren kwam dat bij een derde tot de helft van de pensioenfondsen het datakwaliteitbeleid niet op orde was (verouderd of niet aanwezig). Verder werden de vastgelegde beheersmaatregelen veelal niet (volledig) uitgevoerd. Een proces gericht op voortdurende verbetering was vaak niet meer onderhouden en bij driekwart van de onderzochte pensioenfondsen had de interne auditfunctie geen recent onderzoek gedaan naar de (beheersing van) datakwaliteit. Er zijn dus genoeg aanwijzingen om te vrezen dat de urgentie om te blijven investeren in datakwaliteit in de loop der jaren is weggezakt.

Optrekken met de pensioenuitvoerders

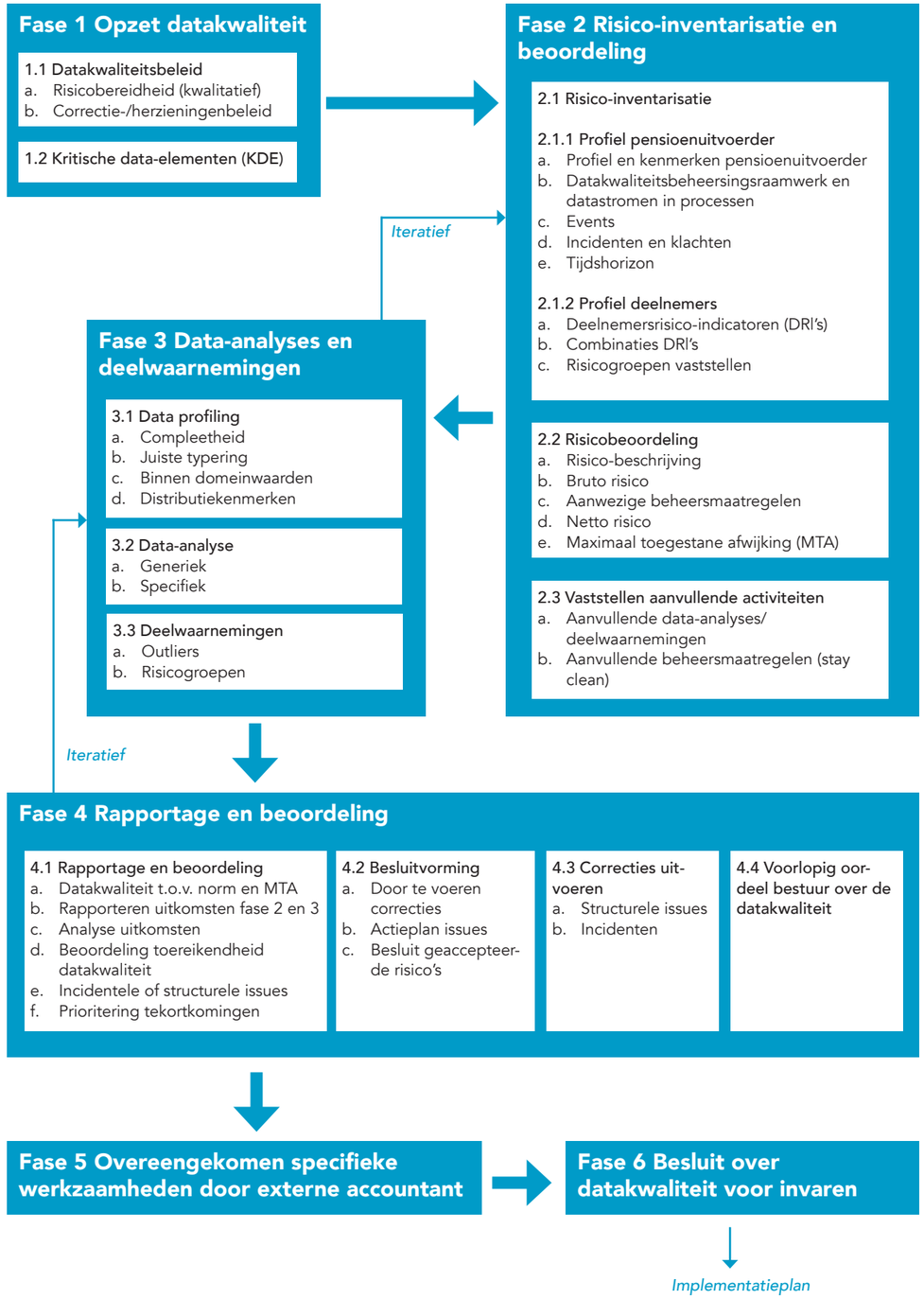
Voor veel kleinere fondsen geldt dat de uitvoering is uitbesteed. Als het gaat om de datakwaliteit zullen ze dus moeten samenwerken met deze uitvoerders. Daarin schuilt echter ook enig risico. Uiteraard zijn de pensioenuitvoerders nu al druk doende om faciliteiten te creëren voor hun klanten om de benodigde werkzaamheden uit te voeren. Maar projecten hebben nogal de neiging om uit te lopen en de vraag is of er niet een enorme piekbelasting gaat ontstaan als alle fondsen tegelijk aan de slag gaan. Uitvoerders moeten namelijk tegelijk ook nieuwe IT systemen gaan ontwikkelen en uitrollen en de beschikbaarheid van data-engineers is niet onbeperkt. Naast de risico's bij de uitvoerders kun je je daarnaast ook nog afvragen of accountants, IT auditors, data-analisten en andere deskundigen de vraag wel aan zullen kunnen.

Wat kan InAudit voor u betekenen ?

In haar recente nieuwsbericht van 16 februari 2023 [2] pleit DNB voor een tijdige start met de werkzaamheden op het gebied van datakwaliteit. InAudit kan u daarbij helpen. Dat kan zowel in de rol van interne auditor ('readiness audits', 'gap-analyses' en beoordeling van de beheersing van de datakwaliteit), maar vanuit InAudit Advies ook in adviserende of ondersteunende rollen. Daarbij werken we samen met Triple A op projectbasis, maar ook op kennisevents zoals de door InAudit georganiseerde bijeenkomst op 1 november 2022 in Burgers Zoo.

1 https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/highlights-uitvraag-niet-financiele-risico-s-2022-pensioenfondsen/

2 https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/transitienieuws-datakwaliteit-tijdig-beginnen-cruciaal/



Ronald van de Langenberg

Algemeen Directeur InAudit

06-24 48 68 92

We zijn er om u te helpen !

In Audit
10 jaar

www.inaudit.nl