april 2024

InAudit Magazine

Met de poten in de modder

Zie ons daar staan bij de Eendenkooi in ’s-Hertogenbosch. Zo zie ik onszelf graag: handen uit de mouwen, poten in de modder. Maar dan met een stropdas of een mantelpakje ;-). Na het feestjaar waarin we ons 10-jarig bestaan op spectaculaire wijze vierden, zullen we dit jaar weer volop aan de bak moeten. Uiteraard willen we in 2024 weer ten minste net zo’n mooie score realiseren als de evaluatie van dit jaar, maar ook zullen de handen uit de mouwen moeten voor de onderwerpen die onze klanten bezighouden, zoals informatiebeveiliging (DORA) en duurzaamheid (CSRD).

In dit magazine
In deze editie van het InAudit Magazine komen beide onderwerpen ook nadrukkelijk aan de orde. We zijn erg blij met de bijdrage van Henk Cornelissen, duurzaamheidsmanager van Turien, maar ook met de inhoudelijke bijdragen van onze collega’s en het speciale inkijkje in het leven van Ricardo. Ook vieren we het eerste lustrum van de AVG-regelgeving met een goed voorstel om weer eens een check te doen of we nog steeds wel compliant zijn. Nieuwe regelgeving heeft immers ook de neiging om weer aan urgentie te verliezen zodra de implementatie achter de rug is. Tegelijk zien we de Autoriteit Persoonsgegevens ook steeds vaker kritisch naar het bedrijfsleven kijken en boetes opleggen.

DORA
Veel van onze klanten zijn inmiddels begonnen met de voorbereiding op DORA en dat is zeker verstandig. Er komt namelijk een hele set met gedetailleerde regelgeving op de sector af. Tegelijk moeten we dat ook nuchter en op basis van risicoanalyse benaderen. Het zal lang niet altijd mogelijk zijn om in januari 2025 helemaal compliant te zijn, maar de vraag is hoe erg dat zal zijn. De vraag is ook in hoeverre de toezichthouders AFM en DNB op koers liggen. DORA roept namelijk nog best de nodige vragen op als het gaat om de exacte invoering op onderdelen als de melding van ‘ernstige’ ICT-incidenten en de daarbij behorende templates, of de (technische) vastlegging van het informatieregister. Wie heeft het portal van DNB al op dit register durven zetten als rank 1 of 2 ICT dienstverlener?

Met de poten in de modder
Ook bij InAudit staan we met de spreekwoordelijke ‘poten in de modder’ als het gaat om DORA. We hebben mooie producten ontwikkeld om de gaps te analyseren, te oefenen met de voorgeschreven templates en voor het opzetten van het verplichte evaluatieverslag.

Met al deze werkzaamheden op het programma zijn we ook blij dat we ons weer hebben kunnen versterken met Sam, Quirien en Ruben (over Ruben in het volgende magazine meer). Het is ontzettend fijn om deze jonge enthousiaste collega’s in ons team te mogen verwelkomen. We wensen ze een mooie loopbaan toe. Interne beheersing is voor niemand een onderwerp waar je op de middelbare school van droomt, maar het is uiteindelijk wel belangrijk en als je er echt goed in wordt, ook nog best dynamisch en interessant.

Genoeg geschreven nu. Ik ga ook maar weer eens de handen uit de mouwen steken!

Ronald van de Langenberg
Algemeen Directeur InAudit

Inhoud

Colofon

Uitgave: InAudit BV
Datum: april 2024

Locaties:
Leuvenheim en IJsselstein

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

www.inaudit.nl

Interview Henk Cornelissen van Turien
De Duurzaamheidsmanager

Nieuwe tijden komen met nieuwe termen, zo hadden we al ‘bestuursschaamte’, ‘havermelkelite’ en ‘smoesflatie’, en nu valt de titel ‘duurzaamheidsmanager’ ook in te sturen aan het instituut voor de Nederlandse taal. Henk Cornelissen, de duurzaamheidsmanager van Turien, legt uit wat deze term nu precies inhoudt.

Ik ben Henk Cornelissen, en vorig jaar gepromoveerd aan de Universiteit van Manchester op het onderwerp klimaat wetenschap. Momenteel werk ik aan de duurzaamheidspropositie van Ansvar en Turien. Hierin proberen wij ons als Turien te onderscheiden op het gebied van ESG, zowel op ecologisch, sociaal als bestuurlijk gebied. Bijvoorbeeld middels duurzaam schadeherstel maar ook op andere zaken die mogelijk minder vanzelfsprekend zijn voor een schadeverzekeraar: op het moment dat je huis afbrandt is het essentieel dat je financieel gecompenseerd wordt, maar daarnaast is het in onze optiek ook van belang om op andere manieren ondersteuning te geven, door te inventariseren waar de verzekerde op dat moment behoefte aan heeft, bijvoorbeeld een psycholoog.

Hoe was het om naar Manchester te gaan voor je doctoraat?
Het was een hele leuke tijd, aan de andere kant zat ik na mijn eerste jaar alleen maar binnen vanwege de corona pandemie. Het veldwerk van mijn studie was in Marokko, in het eerste jaar ben ik daar twee keer geweest. Ik zou daar twee maanden gaan werken op de universiteit in Marrakesh om onderzoek te doen, maar dat ging niet door. Mijn bachelor heb ik gedaan aan de UVA, een future planet studie. Dit ervaarde ik als een soort voortgezet middelbaar onderwijs, het was een heel breed palet aan vakken: geschiedenis, aardrijkskunde, biologie, economie maar dan was alles gestoeld op sustainability.

In Manchester, kon ik een gaaf onderzoek gaan doen. Een Britse docent uit Manchester gaf het vak Paleo-ecologie, dat vond ik interessant en volgde ik als bijvak. Dat bleek mijn interessantste vak tijdens mijn bachelor. Voor dit vak heb ik destijds bodemonderzoek gedaan in Twente. Ik wilde graag door in dit onderwerp, en de docent gaf aan dat hij nog wel mensen kende in Bergen in Noorwegen, van daaruit ben ik als lab assistent gaan werken in onder andere Frankrijk, Australië, USA en Ecuador. Vervolgens kwam ik terug in Nederland en dacht ik: “Now what?” En toen kwam ik deze PhD tegen en ben ik deze gaan volgen.

Waar komt jouw interesse in duurzaamheid vandaan?
Ik ben kritisch onderlegd, ik ben een persoon die niet graag opgeeft én ik wil de wereld verbeteren op wat voor manier dan ook. Op die manier heb ik een natuurlijke affiniteit met het onderwerp duurzaamheid. Deze affiniteit wordt gevoed door mijn studieachtergrond, maar ook vanwege de sociale elementen. Tijdens mijn studie was de focus met name op de fysieke wereld, maar mijn interesse is nu meer gericht op de sociale kant van ESG. Ik zou het vreemd vinden als mensen niet geïnteresseerd zijn in duurzaamheid. In essentie ben ik er van overtuigd dat iedereen het beste wil voor de wereld en de toekomst, de mensen willen wel de wereld verbeteren maar willen zelf niet te veel offers brengen om dit te bereiken.

Hoe komt duurzaamheid als thema terug in jouw dagelijks leven?
Duurzaamheid is een container begrip dus ik zou het op veel manieren kunnen toelichten, ik probeer het zelf te volgen uit een definitie van de Verenigde Naties uit de vorige eeuw: Dat je je impact op de wereld tot het minimum behoud zodat je niet toekomstige generaties belast. Binnen mijn werk probeer ik het breder op te pakken.

Wellicht komt hier mijn sociale kritiek vandaan, momenteel gebruiken we 3,5 keer de carrying capacity van de wereld, dat is te veel. 3,5 meer dan de aarde aan kan. Ik rijd motor, ik beperk mij niet in wat ik eet, ik ga op vakantie maar ik probeer op andere vlakken wel een verschil te maken. Ik vind het altijd lastig dat wanneer je werkt in het discipline duurzaamheid dat de maatschappij verwacht dat je dan zelf roomser dan de paus bent. We moeten uitkijken dat inhoudelijke discussies en besluitvorming niet wordt vertroebeld door persoonlijke verwijten te maken. Het leuke aan mijn huidige functie vind ik dat ik sneller een verschil kan maken: wanneer je onderzoek doet word je betaald uit budgetten voor de wetenschap in een constante bureaucratische strijd. Een commercieel bedrijf is veel slagvaardiger en minder bureaucratisch, als binnen een bedrijf prioriteit wordt gegeven aan duurzaamheid kan je veel sneller stappen maken.

Taken Duurzaamheidsmanager
Mijn taken splits ik op in drie hoofd onderwerpen:

- ESG verslaggeving CSRD boekjaar 2025 samen met een collega.
- Daarnaast ben ik onderdeel van het investmentcommitee, een vijfkoppig comité waarin we onze beleggingen monitoren en aansturen, daar houd ik zicht op de ESG kant van de beleggingen.
- Ook ben ik voorzitter van stuurgroep MVO. De directie heeft een deel van haar uitvoerende capaciteit uitbesteed aan stuurgroepen. Er zijn vier stuurgroepen: werkplezier, MVO, rendement en klanttevredenheid. Hiermee streven wij er naar om klanten en intermediairs van goede verzekeringsproducten te voorzien.

Middels deze stuurgroepen voeren wij een deel van de besluitvorming van de organisatie uit.

Stuurgroep MVO
Je zou mijn rol kunnen vergelijken met een tweede lijns manager, ik beoordeel en produceer beleidsstukken en werk veel samen met de risk manager en compliance officer. Er is geen duurzaamheidsafdeling binnen Turien, maar wij zijn wel het duurzaamheidsteam. Als voorzitter van de stuurgroep MVO heb ik daarmee een toegewijde leidinggevende functie. In deze stuurgroep zitten verschillende managers en de directie, maar ook een externe MVO adviseur die al sinds de jaren ’80 bezig is met verduurzaming als speerpunt toe te voegen aan verzekeringsproducten, dat vind ik erg inspirerend.

In deze stuurgroep bespreken we met name ESG. Hoe kunnen we ons ESG ready maken qua verslaggeving. Voor dit jaar is het onze hoofd-agenda om MVO-doelstellingen op te zetten voor de organisatie. We hebben momenteel nog geen zwaarwegende organisatiedoestellingen op het hoogste niveau, maar wel per afdeling. Er zijn 10 afdelingen en deze moeten elk jaar 5 doelstellingen vormen, voor 2024 is daar een kanttekening bij gekomen namelijk dat 1 van de 5 doelstellingen een MVO-doelstelling moet zijn, daardoor heeft elke afdeling nu een interne MVO doelstelling. Als stuurgroep monitoren wij dit, iedere maand komen wij bijeen en in de eerste helft van dit overleg nodigen wij een medewerker uit om toe te lichten hoe het gaat met deze doelstelling. Daarnaast zijn er elke maand actuele punten bijvoorbeeld een samenwerking met de Nederlandsche Reddingsmaatschappij in combinatie met onze scheepsverzekerings producten. Zo is ons bedrijf erg breed in de maatschappij en kan het op verschillende manieren aangevuld worden met MVO.

Een voorbeeld van zo’n actueel punt is het uitsluitingsbeleid op basis van verzekeringsproducten. De aansprakelijkheidsverzekering heeft een aanvullende module voor een controversiële

“momenteel gebruiken we 3,5 keer de carrying capacity van de wereld”

Vervolg pagina 5

activiteit aansprakelijkheid. In dit geval is het een klein deel van onze portefeuille dus we gaan kijken hoe we omgaan met deze clausule, hoe kunnen we dit beheerst gaan uitsluiten. Dit is een voorbeeld van moraliteit nu, maar we weten niet waar we in de toekomst ons morele kompas als samenleving op aanpassen. Nu is het een kleine impact, maar we moeten ook kijken als het gaat om producten die essentiëler zijn voor onze bedrijfsvoering, hoe we hier beheerst en duurzaam mee om gaan.

Huidige wet- en regelgeving CSRD?
Ik denk zelf dat de CSRD 20 jaar te laat komt, we vinden het allemaal heel normaal dat er financiële verslaggeving verplicht is, dat hoort zo, dat grote bedrijven transparant zijn, daar is iedereen het over eens. Nu komt daar niet financiële verslaggeving bij. Hoe is de verdeling van het salaris binnen het bedrijf? Hoe groot is de gender pay gap? Doe je aan charity? Dat lijkt mij relevante informatie voor de maatschappij om van grote bedrijven te weten.

De kanttekening is wel dat het voor het MKB een stuk lastiger/onmogelijke uitvoer is. Als je een ondernemer bent met twee man personeel dan kan je niet verwachten dat je aan dezelfde eisen kan voldoen als de grote bedrijven. Gelukkig zitten daar thresholds voor ingebouwd in de CSRD. Turien & Co is in mijn ogen precies groot genoeg om mee te doen aan de CSRD, Turien kan specialisten inhuren om dit uit te voeren en kan de informatie verzamelen die nodig is voor deze verslaggeving. Ik kan me voorstellen dat als je net de thresholds raakt dat het dan een stuk krapper wordt om aan de CSRD te voldoen. Je moet veel beleidsdocumenten aanpassen en veel expliciet maken.

Aan de andere kant blijf ik er bij dat de CSRD te laat komt. Misschien moeten de eisen geleidelijk omlaag gebracht worden zodat kleinere bedrijven meer tijd hebben om dit op te zetten. Daarentegen, misschien is de huidige shock approach wel goed voor de grote bedrijven, zij kunnen hun kop niet meer in het zand steken maar moeten echt aan de bak en transparant zijn. We moeten hier in Europa op een gepaste wijze transparant naar elkaar zijn, wij kunnen als Europa een duurzamere economie opzetten op deze manier. Mijn idealistische beeld is dat dit dan ook doorsijpelt naar andere werelddelen. Je ziet buiten Europa en Noord-Amerika steeds meer samenwerkingen als de EU opkomen tussen landen. Europa is een erg complex continent en hier werkt het, dus waarom daar niet? Natuurlijk zijn er in andere werelddelen andere duurzaamheidsvraagstukken die opgelost dienen te worden, maar transparant zijn over wat je doet kan altijd.

Een probleem dat ik zie in de CSRD is dat het met name gestoeld is op de productie van fysieke producten en daarmee wordt het voor een dienstensector lastiger om te voldoen en om transparant te zijn. Ik geloof dat er wel specifieke standaarden voor de financiële dienstverlening in ontwikkeling zijn maar pas in 2028 gepubliceerd zullen worden. Dit maakt het lastig voor (schade)verzekeraars om een verschil te kunnen maken. Toch willen wij als Turien proberen het traject te ondersteunen van een lineaire economie naar een circulaire economie. Schadeverzekeraars kunnen hier in mijn ogen een integrale rol in spelen.

Tijdens een eerder gesprek hadden wij het over de visie van beleggers op duurzaamheid en rendement, jouw visie hierop was voor mij een eye-opener. Kan je deze visie nog eens toelichten? Hoe kijk jij aan tegen investeren, rendement en duurzaamheid?
Het zijn twee belangrijke speerpunten die niet zonder elkaar kunnen. Het uitgangspunt van onze beleggingen is dat het duurzaam gebeurt. De hele reden dat je belegt is om je financiële rendement te verzekeren tegen waardebederving, dat gebeurt met elkaar en daarmee kan je in mijn visie rendement niet boven duurzaamheid plaatsen. Wanneer je niet duurzaam bent leen je van de toekomst, je maakt misbruik van grondstoffen om nu meer rendement te creëren terwijl een duurzame benadering van deze grondstoffen op de lange termijn meer rendement zou creëren en geen einde aan deze grondstoffen bewerkstelligt. Als Turien kiezen we daarom naast de gebruikelijke aandelenfondsen met een hoge duurzaamheidswaardering ook voor impact beleggen in wat wij noemen

TURIEN&CO
ASSURADEUREN

www.turien.nl

"onze rijkdom is gebaseerd op lenen van de toekomst"

een plastic-fonds. Van dit fonds zijn nog geen rendementen uit het verleden bekend maar het doel van dit fonds is om bedrijven te steunen die een verschil maken in de transitie om van fossiel plastic af te komen of het gebruik te beperken.

In mijn ogen moet de samenleving iets meer het besef hebben dat we niet daadwerkelijk de prijs betalen voor een product of belegging van wat het is. Bepaalde beleggingen of producten brengen meer schade toe aan de wereld dan wat jij als consument of belegger hier voor betaald. Met name in beleggingen omdat het in een koers naar voren komt, een bepaalde koers winst verhouding die uitdrukking geeft aan bijvoorbeeld 10 maal de verdiende winst in 1 jaar. Hierin zitten alleen financiële elementen verwerkt, maar niet de impact die een bedrijf heeft op de wereld. Ik hoop dat het CSRD hier een verschil in kan maken, grote bedrijven moeten hier aan gaan voldoen en daarmee wordt het transparanter wat hun impact op de wereld is. Doordat het in Europa is moeten de echt grote buitenlandse bedrijven ook hier aan gaan voldoen als zij hun dienstverlening in Europa willen voortzetten. Daarmee komt de werkelijke waarde van een product beter naar voren. Ik denk bijvoorbeeld ook dat wij in het westen denken dat wij heel rijk zijn. Ik denk van niet, onze rijkdom is gebaseerd op lenen van de toekomst, en op het rendement van onze nationale verledens.

Hoe kijk jij aan tegen 'duurzaamheidsdiscriminatie' middels bijvoorbeeld een lagere rente op de hypotheek voor mensen met een duurzamere woning?
Ik ben daar bekend mee, je maakt daar bepaalde zaken meer exclusief. In feite is het goedkoop om rijk te zijn. Het is bijvoorbeeld goedkoper om in één keer 36 rollen toiletpapier te kopen dan wanneer je elke keer 1 toiletrol moet kopen omdat je niet meer kan betalen op dat moment. Het is duur om arm te zijn, dit is een uitgangspunt van het (huidige) economische systeem. Dit trekt momenteel ook door naar financiële producten, bijvoorbeeld hogere subsidies, of wanneer je een bepaalde waarde van je huis hebt dan kan er een specialist langs komen op het gebied van duurzaamheid. Dit is een service naar onze klanten, ik vind dit bezwaarlijk maar de praktische limitatie is logisch, als je veel klanten hebt kan je niet bij eenieder langs gaan en de vermogende klanten kunnen hier makkelijker een verschil in maken en de insteek is nog steeds verduurzaming dus het effect is er. Dit zie je ook terug in de supermarkt, je hebt ook duurzamere geteelde bonen ten opzichte van gewone bonen. De gewone bonen zijn misschien te goedkoop als je kijkt naar de impact op de aarde, en de duurzame geteelde bonen hebben een echte prijs. De goedkope bonen worden misschien geproduceerd in lage lonen landen waar de arbeidsvoorwaarden minder zijn, of worden besproeid met in Europa verboden middelen en moeten verder vervoerd worden. De bonen zijn nog steeds goedkoper in prijs, maar de impact op de wereld niet.

Wil je nog iets kwijt buiten wat we reeds besproken hebben?
Wij als Turien benaderen duurzaamheid progressief, wij willen graag daadwerkelijk een verschil maken middels ons duurzaamheidsbeleid en de uitwerkingen daarvan. Wij zien duurzaamheid niet als compliance oefening maar als noodzaak voor de lange termijn en willen dit graag aan de maatschappij laten zien.

Wessel Westerveld MSc
Auditor en duurzaamheidscoördinator
06-21 62 77 50

De AVG heeft doorlopende aandacht nodig!

Sinds 25 mei 2018 geldt in de gehele EU dezelfde privacywetgeving: de Algemene verordening gegevensbescherming (AVG). Tijdens de uitvoering van auditwerkzaamheden bij onze klanten lopen we regelmatig tegen zaken aan die verbetering behoeven op het gebied van de bescherming van persoonsgegevens. Ook in de lokale en landelijke media lees je regelmatig dat onjuist met de gegevensbescherming wordt omgegaan. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de AVG. In de afgelopen maanden zijn meerdere organisaties door de AP gewezen op tekortkomingen als het gaat om de naleving hiervan. In sommige gevallen heeft dit zelfs geleid tot beboeting van deze organisaties.

Nieuwe uitdagingen door technologische ontwikkelingen

Recente technologische ontwikkelingen hebben ertoe geleidt dat organisaties (mogelijk onbedoeld) meer (persoons)gegevens verzamelen en verwerken, wat in strijd is met artikel 25 van de AVG (gericht op gegevensbescherming door ontwerp en standaardinstellingen). Om te voorkomen dat er niet meer persoonsgegevens worden verwerkt dan absoluut noodzakelijk voor het beoogde doel van de verwerking, horen we te streven naar minimale gegevensverwerking (dataminimalisatie). Met de opkomst van nieuwe technologieën, zoals kunstmatige intelligentie en algoritmes, is de discussie over gegevensbescherming en privacy verder aangewakkerd.

Voor 2024 heeft de AP, mede daarom, een aantal specifieke thema's centraal gesteld, waaronder:

- Algoritmes & AI;
- Big Tech;
- Vrijheid & veiligheid;
- Datahandel, en;
- Digitale overheid.

De AP stelt dat de huidige AVG-artikelen flexibel genoeg zijn om zich aan te passen aan de technologische veranderingen en een kader bieden voor gegevensbescherming in een meer digitale wereld. Maar, het is essentieel dat organisaties op de hoogte blijven van de prioriteiten van de toezichthouder, en anticiperen op ontwikkelingen die hun bedrijfsvoering en compliance met de AVG kunnen beïnvloeden.

Het waarborgen van AVG compliance

Het afschermen en beschermen van persoonsgegevens van klanten, relaties en personeelsleden is de verantwoordelijkheid van elke organisatie die deze persoonsgegevens nodig heeft voor haar bedrijfsvoering. Die verantwoordelijkheid is aanzienlijk want de privacy van personen moet maximaal geborgd zijn. Om de naleving van de AVG te borgen hebben organisaties actie ondernomen en beheersmaatregelen ingericht om bijvoorbeeld het risico op datalekken te verkleinen. Maar hoe weet een directie of bestuur van een organisatie dat de AVG vereisten juist en volledig zijn geïmplementeerd en ook als zodanig worden nageleefd?

Om hierbij te helpen hebben wij een aantal diensten en producten ontwikkeld die u ondersteunen bij het waarborgen van het juist en volledig naleven van de AVG:

- AVG Training: een korte stoomcursus AVG
- AVG Toolbox: een aantal gestandaardiseerde templates
- AVG Audit: een interne audit op de naleving van de AVG

AVG Training

Wat houdt de AVG in de praktijk nu eigenlijk in voor het dagelijkse werk? Wat mag wel, wat mag niet en wat mag alleen onder bepaalde voorwaarden? Hoe te handelen in bepaalde situaties? Onze AVG-stoomcursus biedt een overzicht van essentiële elementen in gegevensbescherming. Dit omvat de noodzaak van naleving van de AVG, die regels stelt voor de bescherming van persoonsgegevens. De cursus behandelt basisprincipes zoals het bepalen van het rechtmatig gebruik van gegevens, het minimaliseren van gegevensverzameling, het bijhouden van verwerkingsregisters, en verwerkersovereenkomsten. Ook worden de rechten van betrokkenen, bewaartermijnen, rollen van verwerkingsverantwoordelijken en verwerkers, en acties bij datalekken besproken, inclusief veelvoorkomende voorbeelden.

AVG Toolbox

De AVG stelt dat er meerdere vastleggingen moeten worden gedaan. Denk bijvoorbeeld aan het afsluiten van verwerkingsovereenkomsten met dienstverleners aan wie werkzaamheden zijn uitbesteed, het opzetten/ bijhouden van verschillende registers (zoals een verwerkings- en datalekregister) en het uitvoeren van een Data Protection Impact Assessment (DPIA). Wij kunnen u helpen door met u mee te kijken naar hoe u deze documenten heeft ingericht en/of gestandaardiseerde templates of tools aanbieden. Doordat we regelmatig de AVG-richtlijnen toetsen, zijn wij goed op de hoogte van de registraties die binnen organisaties moeten worden ingericht om juist en volledig te voldoen aan de AVG. Hiervoor hebben wij een toolbox ontwikkelt waar alle noodzakelijke documenten zoals de DPIA, verwerkingsregister en datalekregister in terug te vinden zijn. Door ons verwerkingsregister en datalekregister te gebruiken kunt u tijd en moeite besparen door een gestroomlijnde registratie en beheer van gegevensverwerkingen en incidenten/ datalekken. Het dashboard wat in het register te vinden is biedt u daarnaast ook de mogelijkheid voor monitoring, analyse en rapportage van trends, compliance management en getroffen maatregelen.

AVG Audit

De interne audit zal u inzage geven in de naleving van de AVG-richtlijnen door het toetsen van de beleidsmatige uitgangspunten, de ingerichte procedures, beheersmaatregelen en vastleggingen. Dit doen we in een aantal stappen:

Stap 1:
We beoordelen of alle AVG-artikelen correct zijn vertaald naar beleid en procedures en dat informatie/ communicatie hierover voldoet aan de daaraan te gestelde eisen;

Stap 2:
We toetsen de (correcte) implementatie en naleving van beheersmaatregelen ter bescherming van de persoonsgegevens;

Stap 3:
We toetsen of bij onverhoopte datalekken (oneigenlijk of onbedoeld verspreiden van persoonsgegevens) de correcte procedures en communicatielijnen worden gevolgd, conform de AVG.

Na uitvoering van de interne audit zal de directie of bestuur van een organisatie meer inzicht hebben in de correcte en volledige implementatie en naleving van de AVG. Onze auditrapportages bevatten adviezen die u kunnen helpen om eventuele tekortkomingen te adresseren.

Veel organisaties hebben onvoldoende inzicht in hoeverre zij de AVG juist en volledig naleven of kunnen dit maar beperkt aantonen. Meer informatie over onze diensten kunt u vinden op onze website of neem contact met ons op.

Wij zijn er om u te helpen!

Sam Althoff
Sumeyya Demiroglu

DORA-Compliance met behulp van onze tools en oplossingen

InAudit begrijpt dat de naleving van de Digital Operational Resilience Act (DORA) veel tijd en inspanning van bedrijven vereist. Tijd die ze liever besteden aan andere belangrijke zaken. Om financiële instellingen te ondersteunen in hun DORA implementatieproces, heeft InAudit vier producten ontwikkeld. Deze oplossingen van InAudit zetten financiële instellingen op de fast track naar DORA-Compliance.

Onze 4 oplossingen:
1. Gap-analyse tool
2. Voorbeeld van het evaluatieverslag
3. Template voor ICT-incidentmelding
4. Template voor uitbesteding aan service-providers

1. Gap-analyse tool
Een van de ontwikkelde producten is de Gap-analyse tool. Deze tool is speciaal ontwikkeld om organisaties te helpen identificeren wat er tussen hun bestaande status en DORA-Compliance staat, en welke acties ze kunnen ondernemen om deze kloof te dichten. Met deze tool kunnen organisaties per DORA-wetsartikel en per lid een evaluatie uitvoeren, waarbij ze hun huidige nalevingsstatus kunnen beoordelen op gebieden zoals incident response, ICT-risicomanagement en operationele veerkracht. Door de resultaten te visualiseren in een overzichtelijk dashboard, kunnen bedrijven gericht sturing geven aan hun inspanningen en eventuele hiaten identificeren, prioriteren en aanpakken. Door de tool periodiek te updaten kan ook de voortgang worden bewaakt.

2. Evaluatieverslag
In DORA is opgenomen dat organisaties jaarlijks, én na een ernstig ICT-incident, een evaluatieverslag opstellen waarbij zij gedetailleerd alle gebeurtenissen en ontwikkelingen binnen het ICT-landschap vastleggen. Dit evaluatieverslag kan de toezichthouder opvragen. Wat er in het verslag moet worden vastgelegd en hoe dit vorm moet krijgen is door de ESA's gedetailleerd voorgeschreven in de Regulatory Technical Standards. Het betreft twee pagina's aan voorschriften waar dit verslag aan moet voldoen. Vanuit een blanco opzet uitwerken van een voorbeeldverslag kan tijdrovend zijn. Om dit alles te vergemakkelijken heeft InAudit op basis van de voorschriften een voorbeeldverslag

Sneak peek van het dashboard uit onze gap-analyse tool

opgesteld. Aan de hand van een fictieve entiteit bieden we een voorbeeld van hoe zo'n verslag er uit kan zien. Organisaties kunnen dit template gebruiken als inspiratie om aan de opgestelde voorschriften qua vorm en inhoud te voldoen. In plaats van zich door alle regelgeving heen te worstelen helpen we organisaties zo op weg. Door het door ons ontwikkelde template in de eigen context te brengen is al een belangrijk deel van het werk gedaan.

3. ICT-incidentmelding
De wettelijke norm om een ernstig ICT-incident te melden is binnen vier uur voor de eerste kennisgeving aan de toezichthouder. Om ervoor te zorgen dat organisaties zich tijdens deze vier uur kunnen focussen op het incident en niet op de vormvoorschriften van de kennisgeving, heeft InAudit een template gecreëerd, waarin alle te melden datavelden zijn opgenomen. Deze tool stelt organisaties in staat om te oefenen met het melden van ernstige ICT-gerelateerde incidenten conform de voorschriften van de ESA's. In het tool zitten verwijzingen naar de classificatie-criteria, drop-down menu's als het gaat om 'closed lists' en de toelichtingen zijn vertaald. Door te oefenen met dit tool, kan beter inzicht worden verkregen in welke informatie moet worden verzameld en gerapporteerd, wanneer een 'ernstig' ICT-incident zich voordoet.

4. Ketenpartners
Als het gaat om het onderdeel 'uitbesteding aan serviceproviders' gaat veel aandacht uit naar de toets en de update van de uitbestedingsovereenkomsten. Maar een ander belangrijk onderdeel is de verplichting om een 'informatieregister' bij te houden van alle serviceproviders. Daarbij gaat het niet alleen om de directe ICT-uitbestedingsrelaties, maar ook (als het belangrijke of kritieke processen betreft) om de onderaannemers van deze directe relaties en mogelijk zelfs de onderaannemers daarvan. De ESA's hebben het format daarvan gepubliceerd, maar wij hebben dat in een prettige layout gezet, verrijkt met toelichtingen, drop-down menu's en toelichtingen in het Nederlands. Op deze manier kom je wat gemakkelijker tot een eerste opzet. Vanaf het moment dat DORA van kracht is kan de toezichthouder dit register opvragen.

We zijn er om u te helpen!
Veel organisaties vliegen de DORA aan als een complianceproject vergelijkbaar met de invoering van de AVG. Daarvan heeft het ook zeker wel enkele kenmerken. Maar DORA gaat ook inhoudelijk over de inrichting van uw ICT-security management en daarin hebben we ook enige expertise opgebouwd. Met deze vier tools willen we u graag ondersteunen met uw implementatieproject.

InAudit Teamuitje Eendenkooi 12 maart 2024

Als Teamuitje wilden we ons dit jaar nuttig maken voor Stichting Eendenkooi Maaspoort. Een natuurhistorisch cultuurmonument in 's-Hertogenbosch. Sinds 2001 werken ze aan de restauratie en ontwikkeling van Eendenkooi Maaspoort en bevorderen er de biodiversiteit en stimuleren natuurontwikkeling. We hebben geholpen met het ruimen van zieke bomen in het stilte gebied.

De evolutie van cyberweerbaarheid:

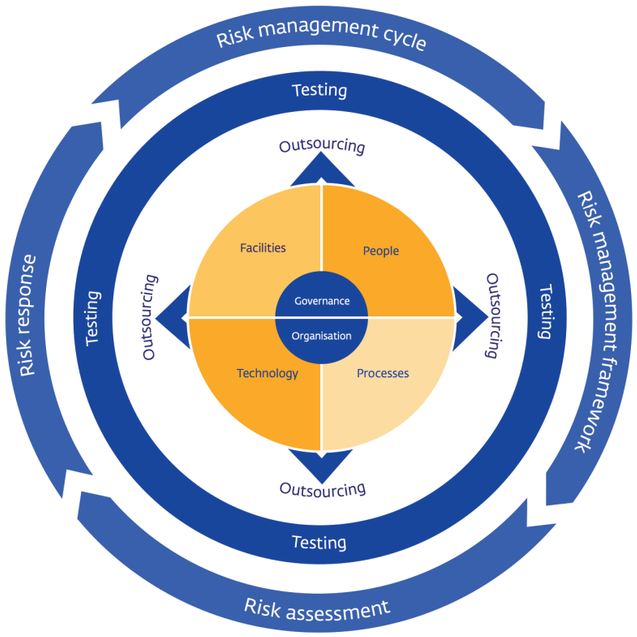
DNB's Good Practice Informatiebeveiliging 2023

De cybercrime industrie wordt steeds professioneler en dat leidt tot toenemende dreigingen. Financiële instellingen zullen hun weerbaarheid voortdurend moeten verbeteren. De Nederlandsche Bank (DNB) speelt een belangrijke rol bij deze bescherming, door het opstellen van Good Practices voor informatiebeveiliging. De Good Practice uit 2019/2020 is in 2023 bijgewerkt en reflecteert de toenemede eisen aan het ICT-risico raamwerk. Dit artikel duikt in de belangrijkste veranderingen en hun impact op de financiële sector.

Van compliance naar weerbaarheid
De nieuwste update laat zien hoe financiële instellingen zich bewust moeten worden hoe groot de risico's en dreigingen zijn. De invoering van de Digital Operational Resilience Act (DORA), die de cyberweerbaarheid van de financiële sector beoogt te verhogen, is door DNB aangegrepen om heldere handvaten en beheersmaatregelen te geven aan financiële instellingen.

Het belang van continue aandacht
DNB benadrukt dat informatiebeveiliging en cybersecurity permanente aandacht vereisen, vooral ook op strategisch en bestuurlijk niveau. De Good Practice 2023 is een reflectie van deze behoefte en biedt de financiële sector de handvatten om niet alleen te voldoen aan de wettelijke bepalingen, maar ook om proactief te reageren op het constant veranderende dreigingslandschap.

Ontwerpen van Information Security Management Systeem
Voor het inrichten van een Information Security Management Systeem (ISMS) is de Good Practice Informatiebeveiliging 2023 (GP IB 2023) van DNB een effectieve manier om het proces rond informatiebeveiliging te structureren, monitoren en versterken. Op basis van de 58 controls kan je als organisatie een risicoanalyse, beleid en beheersmaatregelen implementeren. De Good Practice geeft de juiste basis voor een algeheel ISMS, in onze opinie beter dan de DORA (dat veel focus op een beperkt aantal onderwerpen legt).



De visuele weergave van de focusgebieden van informatiebeveiliging, de onderlinge relaties en de inbedding in het risicobeheer is (afgezien van de kleurstelling) ongewijzigd ten opzichte van de 2019 versie.

Nieuwe en relevantste wijzigingen

De Good Practice Informatiebeveiliging 2023 introduceert belangrijke wijzigingen die een robuust fundament leggen voor financiële instellingen om de voortdurende dreigingen in kaart te brengen:

- **Strategie ICT-risicobeheer:** Nadruk op een digitale operationele weerbaarheid strategie op korte, middellange, en lange termijn, die richting geeft aan het (ICT) Risk Management Framework inclusief het beheer over derde partijen.
- **Risico-gebaseerd:** Aandacht voor een risico-gebaseerde invulling per control. Hierdoor kunnen instellingen steeds verdergaand maatwerk toepassen ten aanzien van de inrichting en implementatie van hun specifieke informatiebeveiligingsmaatregelen.
- **Business Impact Analyse:** Het belang van het uitvoeren van een business impact analyse wordt benadrukt, om de blootstelling aan ernstige bedrijfsstoringen en de potentiële gevolgen daarvan beter te kunnen inschatten.
- **Bestuurlijke betrokkenheid:** De gewenste rol van het bestuur is explicieter gemaakt, inclusief het ontwikkelen en bijhouden van relevante kennis en opleidingen door bestuursleden en sleutelfunctiehouders.
- **Uitbestedingsketen:** Extra aandacht voor (kritieke) uitbestedingen wordt aangekaart. Meer voorbeelden en normen om te zorgen dat financiële instellingen een gestructureerd en overzichtelijk uitbestedingsproces inrichten.

DORA vs Good Practice
Hoewel de implementatie van de GP IB 2023 van DNB een sterke basis legt voor het verbeteren van de cyberweerbaarheid, is het voldoen aan de Good Practice niet voldoende om ook gereed te zijn voor DORA. DORA is namelijk meer rule-based en gedetailleerder. DORA heeft een bredere reikwijdte en bevat specifieke vereisten die niet volledig worden gedekt door de controls van DNB. Daarom moeten financiële instellingen aanvullende maatregelen nemen om volledig aan DORA te voldoen, boven op de richtlijnen van de Good Practice.

Conclusie
Met de GP IB 2023 zet DNB een belangrijke stap vooruit in de bescherming van de financiele sector tegen cyberdreigingen. De update is een erkenning van de noodzaak voor financiële instellingen om hun cyberweerbaarheid continu te evalueren en te versterken in reactie op een steeds veranderend dreigingslandschap. Het is een oproep aan alle financiële instellingen om hun beleid en procedures rond informatiebeveiliging te herzien en te versterken. Dit is essentieel om niet alleen te voldoen aan de wettelijke vereisten maar ook om een stap voor te blijven in de voortdurende strijd tegen cyberdreigingen.

Hoewel de Good Practice Informatiebeveiliging 2023 van DNB financiële instellingen een sterke basis biedt voor informatiebeveiliging en de bevordering van cyberweerbaarheid, moeten instellingen zich ook direct richten op de vereisten van DORA om te zorgen voor volledige compliance met deze Europese wetgeving.
Het is belangrijk dat financiële instellingen zich bewust zijn van en actief werken aan het voldoen aan beide sets van richtlijnen om hun cyberweerbaarheid te maximaliseren.

De wereld van … Ricardo Henriques

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 Ricardo Henriques beter kennen. We stelden hem de volgende vragen.

Wie ben ik?
Ik ben 53 lentes jong en ben samen met Maria en mijn dochter Alexandra. We wonen in "de stad achter de duinen" met onze trouwe viervoeter Beau.
We zijn een leuke combinatie: Ik ben tweede generatie Portugees en Maria heeft haar roots in Friesland. Alexandra is daarmee een Portugees-Friese mix.

Waar ben ik opgegroeid?
Ik zag voor het eerst het levenslicht in Voorburg. In de randgemeente van Den Haag ben ik opgegroeid samen met mijn jongere zus en ouders. Tot mijn 12e jaar heb ik gewoond in Voorburg en daarna ben ik met mijn familie verhuisd naar Leidschendam (ook een randgemeente van Den Haag).

Mijn middelbare school (VWO/ Atheneum) heb ik afgerond aan het Veurs College in Leidschendam. Naast mijn middelbare school heb ik in Den Haag ook de Portugese school gevolgd. Op deze school waren de lessen voornamelijk gericht op de Portugese taal (schrijven en lezen) en de Portugese geschiedenis. Ik ben dus volledig tweetalig.

En toen verder?
Na het afronden van mijn middelbare school wilde ik wel verder leren. Maar wat? Ik heb verschillende zaken overwogen: Vertaler of journalist, gezien mijn tweetaligheid. Maar ik vond ook economie en wiskunde A leuk. Uiteindelijk heb ik besloten de opleiding Accountancy aan de Haagse Hogeschool te volgen. Ik had op dat moment geen idee wat ik met die studie wilde doen.

De stageperiode in het 4de jaar van de HBO opleiding bracht daar verandering in: In het tweede jaar heb ik twee maanden stage gelopen bij PWC. Dat vond ik eigenlijk niet zo heel leuk (veel cijfertjes en jaarrekeningen), maar de stage bij de interne controle afdeling van ABN AMRO in Den Haag vond ik wel heel leuk.

De start van mijn carrière?
De stage bij de Interne Audit afdeling van ABN AMRO in Den Haag is de springplak geweest voor mijn 15-jarige carrière bij ABN AMRO. Ik ben begonnen bij het controleren van de processen bij de verschillende bankkantoren. Daar waren er in die tijd heel veel van.

Ik heb in die eerste periode van mijn carrière in het kantorennet van ABN AMRO mooie dingen meegemaakt: aanwezig zijn bij het tellen van meer dan 1 miljoen valuta, aanwezig zijn bij de opening van bankkluisjes die verjaard waren maar ook overval (preventie)trainingen volgen (voor het geval dat).

Vervolgens heb ik de overstap gemaakt naar Group Audit van ABN AMRO waar ik zowel nationaal als internationaal veel bijzondere dingen heb gezien en meegemaakt. Veel in Brazilië geweest (voordeel van mijn tweetaligheid), de diamanten business van ABN AMRO leren kennen en op dealingroom audits uitgevoerd. Dit zijn wel dingen die ik niet zal vergeten.

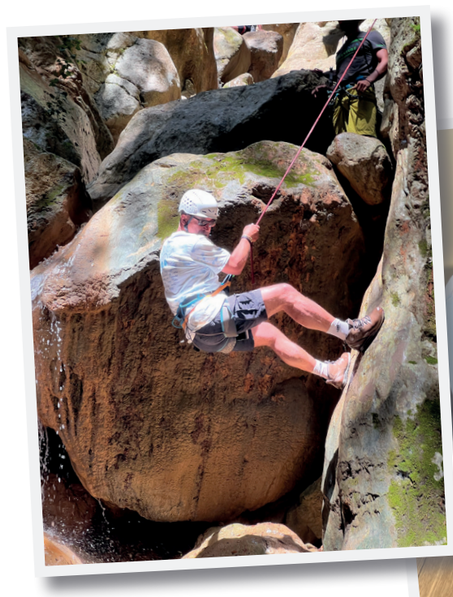
Na 15 jaar heb ik mijn carrière voorgezet bij MN: een van de grotere pensioenuitvoerders in Nederland. Hier ben ik het interne audit vak op het gebied van Vermogensbeheer gaan verkennen en later heb ik uitgebreide ervaring opgedaan in de rol van directeur Risk Management.

En nu?
Ik ben al sinds november 2017 trots onderdeel van InAudit. Ik heb veel plezier met mijn collega's (wat er steeds meer worden) en ik heb ook mijn vaktechnische uitdaging nog door steeds nieuwe onderwerpen en nieuwe sectoren te mogen bedienen vanuit de interne audit functie.

Niks anders?
Jawel! Ik ben op mijn 8ste gaan voetballen en ben eigenlijk mijn hele leven al vrij sportief. In het begin kon ik er eigenlijk niks van, maar vanaf mijn 14e ben ik toch wel in de wat hogere jeugdelftallen gaan voetballen. Ik ben tot mijn 45ste blijven voetballen, maar vanaf mijn 21ste heb ik het hoge niveau losgelaten. Ik vond andere dingen ook leuk: stappen met vrienden, veel en lang op vakantie gaan naar Portugal, de wereld wat verkennen en misschien wel een gezinnetje starten.

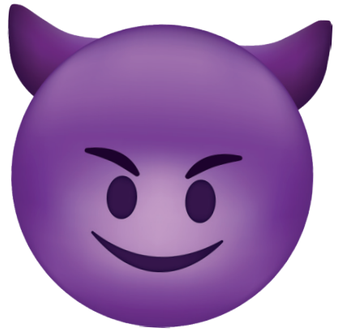
Mijn dochter hockeyt bij onze locale club HCWV (Hockey Club Wateringseveld) in Den Haag vanaf haar zesde. Eigenlijk ben ik toen vanuit een vrijwilligersrol ingestroomd in het trainers- en coach vak. Ik heb zelfs een trainingscursus gevolgd. Ik heb zes jaar mijn dochters team getraind en gecoacht en geef nu training aan Dames 2 van HCWV en assisteer bij Dames 1 van DSHC (Delftse Studenten Hockey Club). Hartikke leuk. Zelfs zo leuk dat ik zelf ook ben gaan Trimhockeyen (doordeweeks voor 35+).

Later als je groot bent?
Ik kijk stiekem wel naar later, maar ik geniet nu van mijn gezin en mijn leven. We hebben alle drie dezelfde instelling: als het minimaal kan dan doen we het. Uitgangspunt is elk jaar op een plek te komen waar we nog nooit zijn geweest. Zo hebben we een prachtige ervaring gehad op de Azoren, waar we mooie natuur hebben gezien en een hele dag op zee hebben doorgebracht en verschillende soorten dolfijnen en walwissen hebben gespot.
Het liefste wil ik binnenkort gaan genieten van de Portugese kust en leuke dingen doen met Maria zonder werk gerelateerde verplichtingen. Wellicht dat Alexandra meegaat…. En anders komen wij regelmatig naar Nederland terug….



DORA en haar duiveltjes

Waarschijnlijk heeft u het zelf ook wel eens ervaren: "The devil is in the detail". Bij de implementatie van DORA is het niet anders. Betrekkelijk eenvoudige acties als 'informeer de toezichthouder bij ernstige ICT-incidenten' wordt al snel een hele opgave als de Europese regelgevers daar standaarden voor gaan ontwikkelen. In dit artikel gaan we u helpen door u een eerste rondleiding te geven langs de 'regulatory technical standards' en de andere detaillering van de DORA.



Regulatory en Implementing Technical Standards
Op verschillende plaatsen in de DORA-verordening staat dat de Europese Commissie de bevoegdheid krijgt om de voorstellen voor 'technische reguleringsnormen' vast te stellen. Daarmee wordt verder invulling gegeven aan de regelgeving. Bij de implementatie van de DORA is het dus zinvol om deze technische uitwerking er meteen bij te pakken en mee te nemen in het plan van aanpak.

Deze technische standaarden verschijnen in drie vormen namelijk:
- 'regulatory technical standards' (RTS),
- de 'implementing technical standards' (ITS),
- Guidelines (in het Nederlands vertaald als 'richtsnoeren').

Over het algemeen geldt dat de RTS wat concreter is dan de DORA verordening zelf en de ITS is doorgaans erg voorschrijvend qua detail.

Bij de DORA horen tien aanvullende documenten (RTS, ITS en Guidelines). Deze zijn verschenen in twee sets, namelijk fase 1 en fase 2. Zolang deze regelgeving nog de status consultatie heeft, zijn de teksten alleen in het Engels beschikbaar. Bij de definitieve vaststelling verschijnen de documenten in het Nederlands. Maar u kunt er in de voorbereiding nu al mee aan de slag en wij zetten alvast wat aandachtspunten voor u op een rijtje.

Fase 1: de voorstellen aan de Europese Commissie
In de eerste fase zijn vier documenten geconsulteerd. De consultatiefase is inmiddels beëindigd en de geconsulteerde documenten zijn thans als voorstel gepresenteerd aan de Europese Commissie. Het betreft de volgende vier documenten:
1. Draft RTS on the ICT Risk Management Framework and on Simplified ICT Risk Mgt Framework;
2. Draft RTS on the classification of major incidents and significant cyber threats;
3. Draft RTS to specify the policy on ICT services supporting critical or important functions;
4. Draft ITS on the Register of Information.

Fase 2: in consultatie
In de tweede fase worden zes documenten geconsulteerd. De consultatiefase is inmiddels gestart en deze loopt tot 4 maart 2024. Uiterlijk 17 juli moeten deze voorstellen, na verwerking van de feedback uit de consultatie, worden gepresenteerd aan de Europese Commissie. Het betreft de volgende zes documenten:
5. Draft RTS on subcontracting ICT services supporting critical or important functions;
6. Draft joint guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents;
7. Draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities
8. A: Draft RTS on the content of the notification and reports for major incidents;
   B: Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident;
9. Draft joint guidelines on the oversight cooperation and information exchange;
10. Draft RTS specifying elements related to threat led penetration tests.

We hebben deze documenten doorgenomen. Het gaat te ver om alles te bespreken, want het zijn stevige documenten met veel details. Hierbij een overzicht met een korte toelichting. Elk document bevat tevens de link naar de EBA-website.

1. Draft RTS on the ICT Risk Management Framework and on Simplified ICT Risk Mgt Framework
Deze technische standaard heeft betrekking op de eerste pijler en is vrij omvangrijk. Een proportionele benadering is wellicht mogelijk en de RTS biedt ook een onderdeel (titel 2) over een vereenvoudigde aanpak, maar voor de meeste organisaties zullen de voorschriften van titel 1 gelden.

De kern van de RTS is opgedeeld in vijf hoofdstukken: (1) Governance, (2) Human resources en logische toegangsbeveiliging, (3) ICT incidentmanagement, (4) ICT Business Continuity en (5) Review rapportage.

Het eerste hoofdstuk is omvangrijk en de volledige implementatie zal een flinke klus zijn die mogelijk ook niet in 2024 kan worden afgerond. Onze visie is dat het goed is om hier te denken in termen van stapsgewijze toenemende volwassenheid door middel van de PDCA-aanpak. De hoofdstukken die volgen betreffen onderwerpen die ook op basis van het Good Practice document al zijn ingericht. Maar de regels zijn wel gedetailleerder dan het Good Practice document dat in beginsel meer principle based is.

Een belangrijk sluitstuk van deze RTS is hoofdstuk 5, het jaarlijkse evaluatierapport. De RTS schrijft de vorm en inhoud voor en daarin komen alle onderdelen van het ICT risicobeheer wel in terug. De toezichthouder mag dit document opvragen en onze verwachting is dat u er rekening mee moet houden dat de toezichthouder dat ook gaat doen.

Dit document zal zich nog gaan ontwikkelen en mogelijk gaan toezichthouders ook terugkoppeling en wellicht nog wat guidance geven over hun verwachtingen. Eenvoudig beginnen is een goed idee, maar met 12 verplichte onderdelen bent u al snel onderweg richting een stevig rapport. Sommige elementen zijn overigens erg eenvoudig, zoals de datum van goedkeuring van het rapport. Andere elementen zijn omvangrijk, zoals een omschrijving van alle genomen maatregelen om de geconstateerde zwaktes en tekortkomingen op te lossen.

Naar onze verwachting zal de implementatie van deze standaard een behoorlijke klus worden, maar naar onze inschatting kan dit ook gefaseerd worden opgepakt.

2. Draft RTS on the classification of major incidents and significant cyber threats
Deze technische standaard heeft betrekking op de tweede pijler van DORA. Een belangrijk onderdeel van deze tweede pijler is dat u onderscheid moet gaan maken tussen:
- (gewone) ICT-incidenten en ernstige ICT-incidenten en
- (gewone) cyberdreigingen en significante cyberdreigingen.

Ernstige ICT-incidenten moeten (onverwijld) worden gemeld bij de bevoegde autoriteit en significante cyberdreigingen op vrijwillige basis. Deze technische standaard gaat met name in op de criteria om ICT-incidenten en Cyberdreigingen als "ernstig" of "significant" te classificeren. Daarvoor worden zeven criteria uitgewerkt waarbij deels kwalitatieve criteria worden meegegeven, maar deels ook heel concrete kwantitatieve criteria, zoals bijvoorbeeld voor de economische impact (> €100.000), de duur van het incident (24 uur) of de downtime van kritische of belangrijke systemen (2 uur).

Deze RTS biedt een nadere uitwerking van de criteria en hoe deze onderling moeten worden gewogen om te kunnen concluderen of er sprake is van een ernstig ICT-incident dat moet worden gemeld.

De wijze waarop moet worden gemeld is uitgewerkt in een separate RTS en ITS (zie document 8). In dat document worden ook de tijdslijnen en de inhoud van de rapportage toegelicht.

Op zichzelf zijn de regels best concreet en duidelijk, maar pas als je aan de slag gaat, bijvoorbeeld in een door InAudit gefaciliteerde workshop, blijkt pas echt hoe lastig het zal zijn en welke voorbereidingen je moet treffen om te voorkomen dat je in tijden van grote stress (als gevolg van een ernstig ICT-incident) het wiel moet gaan uitvinden. Naar onze verwachting zijn workshops en 'table top exercises' de beste methode om deze regelgeving eigen te maken.

3. Draft RTS to specify the policy on ICT services supporting critical or important functions
Deze technische standaard heeft betrekking op de vierde pijler van DORA en gaat over de risicobeheersing met betrekking tot ICT-serviceproviders. De vierde pijler van DORA is een hele pittige opgave die zich ook nog eens lastig laat plannen omdat medewerking van leveranciers nodig zal zijn. Ook is er nog best wel wat onduidelijkheid over de mate waarin je mag steunen op de 'oversight' werkzaamheden van de grote 'third-party providers'. Als individuele verzekeraar zal het namelijk lastig onderhandelen zijn met Microsoft, Google of AWS.
Inhoudelijk bestaat deze RTS op zichzelf eigenlijk maar uit tien artikelen, waarbij het met name gaat over de risico-analyse rondom uitbesteding van ICT diensten, due diligence vooraf, contractuele bepalingen en de monitoring. Uit dit RTS volgt wel dat het wellicht zinvol is om het ICT-uitbestedingsbeleid als separaat beleidsdocument uit te werken. Hierdoor voorkom je dat het reguliere uitbestedingsbeleid te zeer wordt belast met ICT-specifieke vereisten.

Vervolg pagina 19

Naar onze verwachting is de invoering van deze RTS een logisch en samenhangend onderdeel van de werkzaamheden van hoofdstuk vijf van de DORA verordening zelf. In dit document wordt op het eerste gezicht weinig extra complexiteit toegevoegd.

4. Draft ITS on the Register of Information

Ook het informatieregister is onderdeel van de vierde pijler. Op zichzelf klinkt het heel logisch: namelijk een overzicht van ICT serviceproviders, de dienstverlening en het soort contracten. Toch zijn de ESA's erin geslaagd om er een complex geheel van te maken. Probeer het zelf maar eens.

Een lastig onderdeel is dat het informatieregister meerdere lagen kan hebben. Als er belangrijke of kritieke functies worden uitbesteed kan het zijn dat ook de serviceprovider van de serviceprovider van de serviceprovider moet worden gerapporteerd, ergo twee of drie lagen diep. Binnen InAudit hebben we een Excel tool (pagina 11 punt 4 in dit magazine) gemaakt waarin we alle informatie bij elkaar hebben gebracht en u op een iets vriendelijkere wijze proberen naar de juiste invulling te leiden met vertalingen, drop down menu's en instructies.

Het informatieregister moet er in beginsel liggen als DORA van kracht wordt op 17 januari 2025. De bevoegde autoriteiten mogen het ook opvragen en onze verwachting is ook dat dit misschien al in 2025 zal gebeuren. Dit kan dus uitdrukkelijk niet worden uitgesteld naar 2025.

Onze verwachting is dat de eerste invulling van deze templates erg zal tegenvallen. Neem hier voldoende tijd voor, of overweeg een door InAudit gefaciliteerde workshop.

5. Draft RTS on subcontracting ICT services supporting critical or important functions

Waar document 3 gaat over het beleid met betrekking tot ICT uitbesteding, gaat het in dit document met name over de vraag: "Mag je deze (kritieke of belangrijke) functie eigenlijk wel uitbesteden?" Het document kent eigenlijk maar 8 artikelen en is daarom vrij overzichtelijk. Het centrale artikel van de RTS is artikel 4 waarin een soort checklist-achtige opsomming wordt gegeven van de specifieke eisen waaraan de SLA met de serviceprovider moet voldoen. Uiteraard beschrijft deze RTS ook de verplichting om de risico's te analyseren, maatregelen te treffen om de naleving te bewaken en om de overeenkomst te beëindigen bij materiële veranderingen.

Net zoals document 3 is dit RTS een logisch en integraal onderdeel van de implementatie van de op zichzelf lastige vierde pijler over ICT-risicomanagement over uitbestedingen.

6. Draft joint guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

Zowel in het evaluatieverslag over het boekjaar (zie document 1) als in de meldingen van 'ernstige ICT-incidenten' moet de (geschatte) schade als gevolg van ICT incidenten worden gerapporteerd. Deze kosten kunnen op verschillende manieren worden bepaald en de vraag zal vaak zijn of kosten nu incident-gerelateerd zijn of wellicht gewoon 'vervroegde investeringen' danwel 'achterstallig onderhoud'. Ook het toerekenen van schades aan een boekjaar (afgrenzen) kan wellicht complexiteit geven. Deze guidelines geven daartoe nadere duiding. Ook wordt een template meegegeven (pagina 16 van deze RTS) van de te rapporteren (geschatte) schade in het boekjaar.

Deze RTS moet zeker enige aandacht krijgen. Mogelijk zal iedere organisatie hier ook zelf weer vuistregels voor ontwikkelen, maar op zichzelf lijken deze guidelines niet erg complex.

7. Draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities

Terwijl wij meestal spreken over 'vijf pijlers' spreken de toezichthouders meestal over zes focus areas. Het verschil is het 'oversight' kader. Daarin worden de bevoegdheden van de bevoegde autoriteiten vastgelegd met betrekking tot het (rechtstreekse) toezicht op ICT-serviceproviders.

Wij hebben ons hier vooralsnog niet nader in verdiept omdat we ervan uitgaan dat dit niet tot werkzaamheden voor financiële instellingen zal leiden.

De 5 pijlers van DORA

8. A: Draft RTS on the content of the notification and reports for major incidents
B: Draft ITS on the standard forms, templates and procedures for financial entities to report a major incident

Bij de tweede pijler van DORA horen twee documenten, namelijk de RTS die gaat over de classificatie van incidenten en cyberdreigingen (document 2) en een RTS (en ITS) die gaat over de tijdslijnen en de inhoud van de melding van ICT-incidenten (document 8).

Document 8 bestaat uit twee delen, namelijk een RTS en een ITS. De ITS betreft een gedetailleerde uitwerking van de te rapporteren velden in de vier templates die van toepassing worden op de incidentenrapportage aan de bevoegde autoriteiten, inclusief data glossary etc.

Het informeren van de autoriteiten over ernstige ICT-incidenten vindt plaats met drie verschillende rapportages (en templates):

- Eerste kennisgeving: Deze moet plaatsvinden binnen vier uur na het classificeren van het incident als 'ernstig', maar niet later dan 24 uur na eerste vaststelling. De classificatie moet dus min of meer binnen 20 uur zijn afgerond.
- Tussentijds verslag: Zodra de situatie is teruggekeerd naar normaal, maar anders na 72 uur na classificatie als 'ernstig'.
- Eindverslag: Niet later dan één maand na classificatie, maar als het incident dan nog niet gesloten is, dan de dag na de definitieve afwikkeling van het incident.

Voor de drie verschillende verslagen zijn afzonderlijke templates gedefinieerd. Deze zijn in de ITS uitgewerkt. Om deze templates te kunnen invullen moet u in uw incidentenproces heel wat informatie vastleggen. Zo moet u bijvoorbeeld na afloop rapporteren over de totale kosten van het incident. Ook daar bestaan weer guidelines voor (document 6).

Binnen InAudit hebben we een Excel tool (pagina 11 punt 3 in dit magazine) ontwikkeld waarmee kan worden geoefend om op tijd te zijn voorbereid op deze meldingsplicht. In geval van ernstige ICT incidenten is het namelijk geen goed moment om die last er ook nog bij te krijgen. Ons advies is om hiertoe één of meerdere workshops te plannen zodat er een goed draaiboek ligt en er alvast enige bekendheid zal zijn met betrekking tot alle vragen en bepalingen en hetgeen rondom het incident moet worden vastgelegd.

9. Draft joint guidelines on the oversight cooperation and information exchange

Net als document 7 gaat ook dit document over de samenwerking tussen bevoegde autoriteiten als het gaat om het toezicht op met name serviceproviders. Dit document biedt een wettelijk kader om informatie te delen. Verder beschouwen wij dit niet als een document waarmee financiële instellingen aan de slag moeten gaan.

10. Draft RTS specifying elements related to threat led penetration tests

De 'threat led penetration test' (TLPT) is een belangrijk onderdeel van de derde pijler van DORA. Bevoegde autoriteiten kunnen daarin een belangrijke rol spelen als het gaat om validatie van de scope vooraf en het delen van de uitkomsten achteraf. Eisen worden gesteld aan diverse elementen, waaronder ook expliciet de testers. In het RTS wordt dit allemaal netjes uitgewerkt met onder andere ook een duiding van de 'red, white and blue teams' in het TLPT proces.

Maar voordat we enthousiast de diepte ingaan maakt artikel 2 duidelijk dat deze verplichting voor veel financiële instellingen niet zal gelden. Voor verzekeraars bijvoorbeeld gaat het om organisaties met meer dan €500 miljoen premievolume. Hoewel we graag onze enthousiaste beschouwing over de verschillende fases van het TLPT willen delen, kunnen we dat wellicht beter alleen doen met de organisaties die het betreft. Voor de meeste organisaties kan invoering van de TLPT en deze RTS achterwege blijven, al is het opdoen van inspiratie voor het reguliere pentest programma geen slecht idee.

We zijn er om u te helpen!

De hele stapel regelgeving (DORA plus tien RTS/ITS documenten) is een hele klus. Zelfs als u redelijk goed bent ingevoerd is het wellicht zinvol om te kunnen sparren. Binnen InAudit hebben we tools en workshops ontwikkeld die u wellicht op een efficiënte wijze op weg kunnen helpen. Daarover hebben we ook een artikel opgesteld. Dat vindt u op pagina 10. Verder houden we u graag op de hoogte via de themapagina op onze website. Maar u mag natuurlijk ook gewoon bellen!

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

Even voorstellen ... Nieuwe collega's

We hebben begin dit jaar een paar nieuwe collega's mogen verwelkomen. We stellen ze hier even aan u voor.

Quirien Slaghekke

Hi! Ik ben Quirien Slaghekke en in januari van dit jaar als junior internal auditor begonnen bij InAudit. Ik studeerde af aan de Hogeschool van Utrecht, waar ik Commerciële Economie met de studierichting Marketing heb gestudeerd. Mijn studie heeft ervoor gezorgd dat ik bij alle facetten van het opzetten van een nieuw (bedrijfs) concept betrokken ben geweest.

Na mijn studententijd in het mooie Utrecht ben ik teruggegaan naar mijn roots, Twente. En heb ik, voordat ik bij InAudit kwam werken, een klein jaar in de onderwijslogistiek gewerkt. Als consultant ben ik op detacheringsbasis werkzaam geweest bij diverse onderwijsinstellingen door heel Nederland. Dit in de rol van procescoördinator bij de HAN en als Key User van de evaluatietool Evalytics aan de Technische Universiteit van Eindhoven.

Door de jaren heen, maar vooral in de laatste opdracht werd ik enthousiast van het evalueren en het continu verbeteren van bedrijfsprocessen. Dit heeft ervoor gezorgd dat ik de overstap heb gemaakt naar het audit vak. Ik kijk daarom enorm uit om de aankomende jaren bij InAudit bedrijfsprocessen en producten te evalueren en te auditen.

Sam Althoff

Ik ben Sam Althoff en sinds januari ben ik werkzaam als junior auditor bij InAudit. Hiervoor heb ik mijn diploma voor de Master International Business Administration behaald aan de Universiteit Twente, waar ik mij heb gespecialiseerd in HRM en Change Management. De afgelopen twee maanden ben ik voor het eerst aan de slag gegaan binnen het audit vak. Ik heb in die tijd alvast kennis mogen maken met een aantal van mijn klanten door daar op locatie langs te komen, audits op te starten en interviews te doen.

Met mijn achtergrond en persoonlijke visie streef ik naar voortdurende verbetering. Binnen mijzelf en voor de klant. Wat dit vak voor mij zo interessant maakt is dat het mij de mogelijkheid biedt om bij veel verschillende organisaties en bedrijfsprocessen te kijken hoe dit georganiseerd is. Hier mag ik dan vervolgens ook nog mijn onderzoek vaardigheden op los laten. Het contact met de klant, verdiepen in nieuwe onderwerpen en organisaties voorzien van advies geeft mij veel energie.

Ik kijk met interesse uit naar het komend jaar, waar mijn werkzaamheden en rol binnen InAudit steeds meer vorm zullen krijgen.

Klanten evaluatie 2023

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 9,0. Dit jaar is de uitkomst nog steeds boven onze verwachting met een 8,9. Een mooie waardering voor het werk van onze collega's, maar wat ons betreft blijft het daar niet bij. Ook in 2024 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 2023 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.

Concluderend kunnen we vaststellen dat 2023 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.

We zijn er om u te helpen !

In Audit

www.inaudit.nl