Classificatie
AFM - Publiek

Reactie Consultatie Principes voor Informatiebeveiliging

Naam	**Bestuur NOREA (Nederlandse Orde van Register EDP auditors)**
Functie	NOREA is de beroepsgroep van IT-auditors. IT auditors houden toezicht op de kwaliteit, veiligheid en continuïteit van IT-systemen en IT-infrastructuren inclusief de bijbehorende (IT-)organisatie en processen. IT-auditing is in Nederland is een hoog ontwikkeld vakgebied doordat Nederland het enige land ter wereld is met een post-master IT-audit opleiding. In onze gedigitaliseerde wereld kennen IT-auditors drie aandachtsgebieden, te weten: Waarborgen van de continuïteit van IT om reputatieschade en verlies van omzet te voorkomen; Beheersen van (Cyber)risico's om betrouwbare gegevensverwerking te waarborgen; Beveiligen van het 'goud' (de data van een organisatie) en waarborgen dat deze data betrouwbaar blijft.
Naam instelling	**NOREA**
Datum	**24/6/2019**

1. Op welke punten kunt u zich vinden in de beleidsuiting Principes voor informatiebeveiliging?

De afhankelijkheid van technologie en van veilige en betrouwbare software wordt steeds groter. Privacy en online security zijn voorwaarden voor het online vertrouwen, economische groei en maatschappelijk welzijn.
Veel organisaties kunnen geen dag meer zonder IT, zonder in continuïteitsgevaar te komen. Hierdoor zijn de risico's sterk veranderd. Het risico van cybercrime wordt steeds groter en de gevolgen ervan steeds complexer. Een incident binnen een organisatie kan al snel economische en maatschappelijke gevolgen hebben voor alle organisaties in de online keten.

Daarom is het goed dat de AFM in haar rol als toezichthouder het initiatief heeft genomen om dit onderwerp onder de aandacht te brengen.

2. Op welke punten kunt u zich niet vinden in de beleidsuiting; voorziet u problemen en waarom?

NOREA begrijpt het initiatief, maar wil u erop wijzen dat het consultatiedocument nog diverse vaktechnische onduidelijkheden en omissies bevat. NOREA is van harte bereid om mee te denken en u hierbij te ondersteunen.

Uw keuze voor “principes” vinden wij een misleidende. De principes over informatiebeveiliging zijn als algemene uitgangspunten geformuleerd, maar zijn ook voorzien van een nadere toelichting wat lijkt op een nadere concretere invulling. Deze nadere invulling is niet langer principieel, maar wordt normerend gesteld zonder de norm te benoemen of uit te werken. Hier wordt onduidelijk, wat de doelstelling van uw consultatiedocument werkelijk is.
Het lijkt erop dat u ‘vriendelijk’ wil zijn voor de onder toezicht staande sector, maar hierdoor ontstaat juist meer onduidelijkheid.
NOREA stelt voor om op de volgende zaken nader met elkaar in overleg te treden:

- Doelstelling
- Scoping
- Normering
- Scoring
- Wijze van opvolging/controle door de AFM

Hieronder een aantal observaties:
De beleidsuiting omvat 12 principes die zijn opgesteld volgens internationaal geaccepteerde ICT-risk-managementraamwerken, zoals COBIT (COBIT 5, gepubliceerd door ISACA), National Institute of Standards and Technology Cybersecurity Framework (NIST) en richtlijnen van CPMI-IOSCO (Guidance on cyber resilience for financial market infrastructures) en het reeds bestaande toezicht op informatiebeveiliging door Nederlandse financiële ondernemingen.

- *Onduidelijk blijft welke overwegingen de AFM heeft gemaakt om te komen tot deze set van 12 principes en waarom afgeweken wordt van bestaande ICT-risk-managementraamwerken.*
- *De Nederlandsche Bank heeft onlangs een, met de AFM afgestemd, hernieuwd uitgebreid raamwerk gepubliceerd, dat al jaren bekendheid geniet onder de onder toezicht staande instellingen (Good Practice Informatiebeveiliging). Het is voor NOREA onduidelijk, waarom de AFM hiervan afwijkt.*

NBA en NOREA hebben begin dit jaar het volwassenheidsmodel informatiebeveiliging uitgebracht en NOREA heeft daarnaast een Cyber Security Assessment (CSA) ontwikkeld dat kan worden ingezet om te bepalen op welke onderdelen cyber risico’s bestaan en door middel van welke standaarden de te treffen acties kunnen worden opgepakt.

- *Wenselijk is dat de relatie met andere frameworks nadrukkelijk wordt aangegeven om zodoende ondernemingen eenvoudiger in staat te stellen om vast te stellen of zij aan de door de AFM gestelde principes voldoen*

De beleidsuitgangspunten zijn in het document nader toegelicht. Die toelichting gaat impliciet uit van een zekere omvang en volwassenheid van de onderneming; denk bijvoorbeeld aan ‘De

effectiviteit van deze maatregelen wordt periodiek getest'. Hiermee lijkt de AFM verder te gaan dan principes te benoemen maar ook voorschrijvend te zijn.

- *Hoewel de principes geldend zijn voor alle ondernemingen kan de nadere invulling hiervan afhankelijk zijn van de aard en omvang van de onderneming alsmede haar volwassenheidniveau. Wenselijk is dat helderheid wordt gecreëerd over de niveaus en periodiciteit van toetsing.*
- *Een goed gebruik is om in het kader van informatiebeveiliging nadere beheersingsdoelstellingen te formuleren die vervolgens nader uitgewerkt kunnen worden in beheersingsmaatregelen. Wenselijk is dat de principes daarom worden vertaald naar beheersingsdoelstellingen.*

De Plan – Do – Check – Act cyclus, gebruikelijk in besturing van ondernemingen (en standaard opgenomen in bijvoorbeeld ISO-normeringen) is onvoldoende aanwezig in het document.

Het verschil tussen gegevensverwerking en gegevensverstrekking is onvoldoende duidelijk. De focus op 'data' apart van 'informatie' is niet helder.

Op het gebied van principe 10 en 11 (Keten en Uitbesteding) is onduidelijk wat de AFM verwacht van de onder toezicht staande instelling. Er zit een grens (zowel fysiek als logisch) aan de verantwoordelijkheid van een instelling in de keten. Ook kan er sprake zijn van een hybride situatie (uitbesteding als keten of keten als uitbesteding) die verder niet wordt uitgewerkt.

- *Een verdere verduidelijking, ook van de rol van de AFM in deze ketens, is noodzakelijk voor een helder begrip en de reikwijdte van beheersing in de keten.*

NOREA onderkent dat verschillende ondernemingen op verschillende wijze omgaan met informatiebeveiliging en hierbij een verschillend niveau van volwassenheid hebben bereikt. Het toepassen van een volwassenheidsmodel in plaats van het schetsen van (minimale) vereisten omtrent informatiebeveiliging kan behulpzaam zijn in het meten en verbeteren van informatiebeveiliging. (zie ook: https://www.accountant.nl/nieuws/2018/10/nba-model-informatiebeveiliging-basis-plan-van-aanpak-jenv/)

In de Principes wordt geen melding gemaakt van het continuïteitsrisico dat organisaties lopen indien informatiebeveiliging niet op orde is. Denk maar aan het risico van platleggen van een organisatie indien het getroffen wordt door een geslaagde cyberaanval. Veel organisaties kunnen inmiddels geen dag zonder ICT zonder risico te lopen in deconfiture te geraken.

- *Het opnemen van het principe "continuïteit" is noodzakelijk.*

3. Wat is uw voorstel om verbeteringen aan te brengen?

Zie 2.

Daarnaast heeft NOREA de volgende tekstuele suggesties:

blz 4, punt 1.1, 4e regel: spatie tussen "financiële" en "dienstverleners"

blz 5, punt 2, 2e alinea, 2e regel: na "vertrouwelijk" invoegen "met"

blz 8, punt 4.1, laatste alinea, 1e regel: na "ervoor dat" schrappen "zij"

blz 11, punt 5.1, 3e alinea, 2e regel: "cyberraamwerken" wijzigen in "cybersecurityraamwerken"

blz 11, voetnoot 7, 3e regel: "verantwoordelijke" wijzigen in "verantwoorde"

blz 12, punt 5.3, 2e alinea, laatste regel: moet de laatste zin van deze alinea niet verhuizen naar punt 5.4? Daar wordt gesproken over "security by design" en daar gaat ook die laatste zin van de 2e alinea van 5.3 over

blz 13, 4e alinea, 2e regel: "informatie" wijzigen in "ICT-assets, inclusief fysieke locaties" (zie blz 8, punt 4.1, 5e alinea)

blz 13, 5e alinea, 1e regel: aan einde toevoegen "overige"

blz 13, punt 5.5, 3e alinea, 3e regel: aan einde toevoegen: "overige"

blz 15, punt 7.1, 2e alinea, 5e regel: "cybertesten" wijzigen in "cybersecuritytesten"

blz 18, bij bullit financiële dienstverlener: na haakje openen invoegen "voor"

Tot slot:

NOREA juicht uw aandacht voor informatiebeveiliging toe en biedt u van harte aan om hierover samen met u en desgewenst De Nederlandsche Bank nader verder te spreken.

De AFM ontvangt uw reactie graag voor **25 juni 2019**. U kunt uw reactie en/of eventuele vragen sturen naar het e-mailadres: consultatieprincipes@afm.nl.

Na sluiting van de consultatieperiode verwerkt de AFM de reacties in een definitieve versie van de Principes voor informatiebeveiliging. Deze publiceert de AFM, samen met een feedback statement op haar website.