Opwaarderingsverzoek en technische vragen m.b.t SB Voortgang Informatieveiligheid Privacy

Partij	Nr.	Vraag / Input	Antwoord / Reactie
VVD	1	**Opwaarderingsverzoek:** Waarom rapporteert de lijn niet over informatiebeveiliging & privacy, terwijl daar wel de verantwoordelijkheid is gelegd? Waarom is versterking van de governance van informatiebeveiliging & privacy langs managementcyclus is nog niet in gang gezet door het CMT?	De rapportage vanuit het programma IV&P is opgenomen in voortgangsrapportage (dashboard) BDV. Het is gedaan om de hoeveelheid aan rapportages op diverse bedrijfsvoering onderdelen te verminderen en om uniformiteit in de rapportages aan te brengen zodat de leesbaarheid verbetert. Rapportage vanuit de lijn vindt inderdaad nog niet plaats. Hier wordt inmiddels aan gewerkt, als onderdeel van de beweging Informatieveiligheid & Privacy te integreren in de CIO-Office en te borgen in de lijnorganisatie. Dit is dus juist nieuw t.o.v. eerdere situatie waar informatieveiligheid en privacy was belegd binnen het domein Bedrijfsvoering. Deze conclusie uit het Assessment IB 2021 dateert van enige tijd geleden. Inmiddels heeft het CMT het ambtelijk Actieplan IV&P vastgesteld. Hierin is, naast een aantal inhoudelijke prioriteiten op het gebied van informatieveiligheid & privacy, ten aanzien van het versterken van de governance het volgende besloten: 1. Het programma IV&P wordt onder aansturing gebracht van de CIO / het CIO-Office; 2. Informatieveiligheid & Privacy wordt als onderwerp opgenomen in de domein-informatieplannen met per domein een roadmap voor de komende 2 jaar; 3. Informatieveiligheid & privacy wordt opgenomen als onderwerp bij de managementgesprekken op ieder managementniveau en in de

		Wat gaat college doen aan gebrek aan ontoereikende inhoudelijke aansturing op het programma informatiebeveiligingsvraagstukken, zodat er zicht en grip op incidenten komt?	gesprekken met de medewerkers. 4. Er wordt nader uitgewerkt hoe invulling kan worden gegeven aan een Coördinator / Medewerker IV&P per organisatiedomein. Er is een kwartiermaker CIO-office aangesteld. Hij gaat zich onder meer bezig houden met het centraliseren van ICT-voorzieningen. Door de gedecentraliseerde inrichting van ICT is er nu nog te weinig overall overzicht op incidenten. Ook is er geen overzicht op de ICT-assets die gebruikt worden binnen de domeinen. Hierdoor is het proces om bij grotere incidenten snel de impact te kunnen inschatten en mitigerende maatregelen te kunnen nemen, te tijdrovend. Het inrichten en optuigen van een CIO-office is niet van vandaag tot morgen gebeurd. We gaan uit van een implementatieperiode van twee jaar.
ChristenUnie	2	**<u>Vragen:</u>** Hoewel er volgens de Statenbrief in de provinciale organisatie groei waarneembaar is, en een positieve ontwikkeling plaats vindt op het gebied van Informatieveiligheid en Privacy, baart het rapport van bevindingen 2021 ons zorgen. De basis is nog altijd niet op orde, met name wat de governance, de sturing, monitoring en borging betreft. Wat is de rol van afd CCO inzake het geconstateerde gebrek aan opvolging van de aanbevelingen uit de onderzoeken?	Wij betreuren ook dat de basis, met name ten aanzien van informatieveiligheid, nog niet goed op orde is. Dit zegt iets over de complexiteit van het onderwerp, maar betekent ook dat er nadrukkelijker op gestuurd moet worden. Een van de aanbevelingen betreft het volgen van de aanbevelingen en hoge risico's met actiemanagement en sturingsrapportage. De afdeling CCO faciliteert het actiemanagement en het rapporteren van de hoge risico's in de managementcyclus.
	3	In hoeverre is het bereiken van 'procesvolwassenheidsnivo 3' realistisch en haalbaar, wanneer uit de bevindingen blijkt dat er nog veel blokkades zijn die dat verhinderen?	CCO vindt dat procesvolwassenheidsniveau 3 realistisch en haalbaar is na het breed behalen van niveau 2, en het hangt af van de doortastendheid en het tempo waarmee de aanbevelingen worden opgevolgd.

	4	Kan (vanwege de urgentie op dit thema, en om druk op voortgang en verbetering te houden) het instrument van assesment naar het organisatiebrede beveiligingsnivo ook jaarlijks (ipv nu 2-jaarlijks) worden uitgevoerd? Dat zou onze fractie zeer wenselijk vinden.	Gezien de impact van het assessment op de organisatie in termen van auditlast en verwerking van aanbevelingen in de aanpak verwachten wij dat het jaarlijks uitvoeren van het assessment averechts werkt op de ontwikkeling. CCO verwacht meer effect van het volgen van de aanbevelingen, het betrekken van de hoge risico's in de managementcyclus en centrale sturing vanuit de CIO-office.
SGP	5	**<u>Opwaarderingsverzoek:</u>** In de SB over informatieveiligheid lezen we (opnieuw) dat de organisatie verrast is door een extern onderzoek naar de daadwerkelijke stand van zaken op het gebied van informatieveiligheid. In de SB over Woo wordt een optimistische stand van zaken geschetst over de haalbaarheid van de implementatie. Intussen gaat deze wet nog veel dieper de organisatie in (denk aan archivering in alle afdelingen). In hoeverre klopt dit optimisme en in hoeverre hebben wij grip op het onderwerp informatieveiligheid? Wij hameren hier al vanaf 2016 op en ieder jaar verschijnt er wel een extern rapport die bevestigt dat het allemaal minder rooskleurig is dan ons wordt voorgesteld.	De organisatie is niet zozeer verrast door het interne onderzoek. Wel is gesteld dat de organisatie verrast is door de conclusie van het onderzoek dat er, ondanks alle inspanningen, weinig aantoonbare groei is in de organisatie op het gebied van informatieveiligheid. Bij privacy is wel duidelijke een aantoonbare groei zichtbaar. Wij betreuren ook dat de basis, met name ten aanzien van informatieveiligheid, nog niet goed op orde is. Dit zegt iets over de complexiteit van het onderwerp, maar betekent ook dat er nadrukkelijker op gestuurd moet worden. Informatieveiligheid blijkt, niet alleen voor onze organisatie, een lastig onderwerp om aantoonbaar op te groeien. Bovendien is dit onderwerp sterk in ontwikkeling en blijkt het bijhouden van deze ontwikkeling en anticiperen hierop vanuit de organisatie veel inzet te vergen. Ondanks dat is ook in het rapport Assessment IB 2021 gesteld dat: *1. Er veel geïnvesteerd is in verbinding, het verbeteren van kennis en bewustwording. Dit wordt door de lijn ervaren en de bekendheid met het onderwerp en de spelers van IV&P is duidelijk gegroeid.* *2. In de afgelopen 2 jaar is het overkoepelende beleid voor informatiebeveiliging (IB) vernieuwd en zijn op verschillende onderwerpen specifieke beleidsuitwerkingen en richtlijnen opgesteld.* *3. Het programma de laatste maanden heeft gewerkt aan de versterking van de weerbaarheid door het opstellen van een incident*

			respons-plan, het organiseren van een crisisteam daarvoor ("CERT") en het oefenen met fictieve cyberaanvallen. *4. Het programma heeft de afgelopen periode ook gestaag gewerkt aan het in kaart brengen van IV&P-aspecten bij applicaties met het uitvoeren van korte scans ("BIA").* Het is van belang een reëel tijdpad te maken ten aanzien van de groei van informatieveiligheid binnen onze organisatie. Dit is vorm gegeven in het ambtelijk Actieplan IV&P dat onlangs door het CMT is vastgesteld. Daarnaast wordt het programma IV&P onder aansturing gebracht van het CIO-Office. Tenslotte is besloten ten aanzien van de governance en het integreren van informatieveiligheid & privacy in de organisatie een aantal veranderingen door te voeren.