Tweede voortgangsrapportage 202

Behandeling in DB dd. 9 december 2021

Uitvoeringsorganisatie van en voor
Ouder-Amstel, Diemen en Uithoorn

de risico's en de beheersmaatregelen. Dit jaar zal het VIC-team de proceseigenaren verder ondersteunen bij het in de lijn brengen van de interne controles waarbij ook de nodige aandacht besteed zal worden aan het vastleggen van de interne controles. Daarmee komt het VIC-team ook steeds beter in positie om de eigenlijke taak uit te voeren, namelijk het controleren van de lijncontroles. De verwachting is dat in 2022 voor vrijwel alle processen de interne controle in de lijn belegd is. Dit betekent dat het VIC-team dit jaar voor een groot deel nog de interne controles zal uitvoeren. De accountants van zowel Duo+ en de DUO-gemeenten hebben aangegeven dat de kwaliteit van de controles die door het VIC team uitgevoerd zijn over 2020 voldoende was om als accountant daarop te kunnen steunen. Het VIC team zal er alles aan doen om deze lijn naar de komende jaren door te trekken.

3.2.2 Informatieveiligheid

BIO

In de vorige versie van deze voortgangrapportage werd stil gestaan bij de instemming van het Duo+ bestuur op het nieuwe Strategisch Informatieveiligheidsbeleid 2020-2023, gebaseerd op de Baseline voor Overheidsinstellingen en de BIO. In navolging van dit beleid is de staf afdeling van Duo+ - onderdeel informatieveiligheid - uitgebreid met de functie van Privacy Officer (2 FTE). Het is de bedoeling dat deze functie de verbindende schakel gaat vormen tussen de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO) en de contactpersonen van de afdelingen / teams. Door deze bundeling van expertise zullen de verplichte invoering van de te nemen AVG- & BIO-maatregelen voor de desbetreffende afdelingen / teams en voor de DUO-organisaties in zijn geheel een betere voortgang van de uitvoering van dit beleid moeten geven.

Door deze uitbreiding van het team informatieveiligheid bij Staf Duo+ is het bijvoorbeeld mogelijk om met een gerichtere aanpak te werken aan voorlichting over 'houding en gedrag' rondom informatieveiligheid van medewerkers en bestuurders. In de veranderende wereld van 'gijzelsoftware, hacking, phishing' en andere ICT informatie risico's zijn helaas ook al verschillende andere (gemeentelijke) overheidsinstellingen slachtoffer geworden. Aan het team de taak om deze risico's zoveel als mogelijk in te perken. Een voorbeeld van een dergelijke bewustwording onder medewerkers, bestuurders en ook raadsleden is een recentelijk in scene gezette phishing actie. Het is de bedoeling om in overleg met de verschillende afdelingen / teams de resultaten hiervan in de werkoverleggen of weekstarts te gaan bespreken. Er zullen nog meerdere van dit soort acties volgen.

ENSIA (Eenduidige Normatiek Single Information Audit)

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over de informatieveiligheid.
Het betreft een verantwoordingssystematiek ten aanzien van de Basisregistratie Personen (BRP), de Paspoortuitvoeringsregeling (PUN), de Digitale persoonsidentificatie (DigiD), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Deze afzonderlijke, zogenoemde verticale verantwoording, geschiedt aan landelijke partners (zoals Logius, het BKWI en de Autoriteit Persoonsbescherming) en de ministeries die een rol hebben in het toezicht op informatieveiligheid.