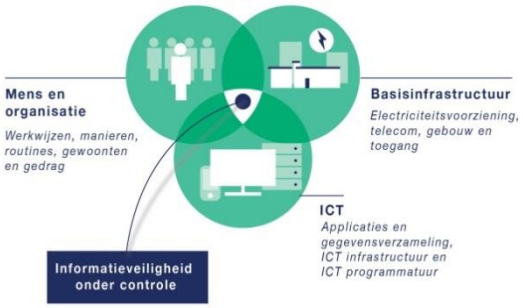
Informatieveiligheid

Provincie Zuid-Holland

Provincies zijn voor de uitvoering van hun taken steeds meer afhankelijk van informatiesystemen en informatiestromen. De veiligheid van informatie neemt dan ook een steeds belangrijker positie in. Informatieveiligheid houdt in dat informatie alleen door de juiste personen is te zien en te gebruiken. Ook dient informatie volledig, juist, actueel en op het juiste moment toegankelijk te zijn. Om informatieveiligheid te waarborgen, kunnen maatregelen worden genomen op de aandachtsgebieden Mens & Organisatie, ICT en basisinfrastructuur (zie afbeelding). Door deze maatregelen kunnen organisaties risico's voor informatieveiligheid tot een acceptabel niveau terugbrengen.



Met de ondertekening van het Convenant Interprovinciale Regulering Informatieveiligheid eind 2014 hebben de provincies kenbaar gemaakt de informatieveiligheid verder te willen optimaliseren en professionaliseren. De Randstedelijke Rekenkamer heeft onderzocht hoe de provincies zijn gevorderd met de borging van de informatieveiligheid.

Vraagstelling

Heeft de provincie Zuid-Holland de informatieveiligheid voldoende geborgd?

De centrale onderzoeksvraag is beantwoord aan de hand van de volgende vier deelvragen:

1. Heeft de provincie de sturing op en de verantwoordelijkheid voor informatieveiligheid goed verankerd?
2. Is het informatieveiligheidsbeleid in opzet, uitvoering én in resultaat adequaat?
3. Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?
4. Heeft de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?

Conclusies

De provincie heeft een aantal zaken op het gebied van informatieveiligheid goed geregeld. Zo heeft de provincie een informatieveiligheidsbeleid dat in opzet voldoet aan de eisen. Ook heeft de provincie het houden van toezicht op informatieveiligheid goed geregeld. Daarnaast zet de provincie sinds eind 2015 stappen in het systematisch integreren en monitoren van maatregelen, plannen en acties op het gebied van informatieveiligheid, door de implementatie van een Information Security Management System (ISMS). Hiermee wil de provincie meer structuur en transparantie aanbrengen in de activiteiten op het gebied van informatieveiligheid.
De provincie dient echter nog verschillende stappen te zetten om de informatieveiligheid voldoende te verankeren. Er zijn nog duidelijk aan te wijzen verbeterpunten, zoals de invulling van verantwoordelijkheden voor informatieveiligheid in de gehele organisatie en het versterken van het bewustzijn van medewerkers van het belang van informatieveiligheid. Hier wordt weinig sturing aangegeven. Een ander verbeterpunt is de uitvoering van maatregelen op het gebied van informatieveiligheid. De provincie heeft bijvoorbeeld nog niet voor alle bedrijfsprocessen bepaald of een risicoanalyse nodig is, waardoor niet voor alle bedrijfsprocessen duidelijk is welke risico's kunnen optreden.

De hoofdconclusie is gebaseerd op de volgende vier deelconclusies:

1. Er is weinig sturing gegeven aan de invulling van rollen en verantwoordelijkheden op het gebied van informatieveiligheid in de gehele organisatie. Ook is er weinig sturing gegeven aan het versterken van het bewustzijn van het belang van informatieveiligheid van medewerkers. Hierdoor wordt nog voornamelijk vanuit afdelingen binnen de directie Concernzaken invulling gegeven aan informatieveiligheid en is informatieveiligheid nog niet voldoende verankerd binnen de gehele organisatie.
2. Het informatieveiligheidsbeleid voldoet in opzet aan de eisen. Het is niet goed te beoordelen of de provincie de benodigde informatieveiligheidsmaatregelen uitvoert, omdat de provincie de uitvoering van de informatieveiligheidsmaatregelen niet coördineert of registreert en niet voor alle bedrijfsprocessen heeft bepaald of een risicoanalyse nodig is. Sinds eind 2015 zet de provincie stappen in het systematisch integreren en monitoren van maatregelen, plannen en acties op het gebied van informatieveiligheid, door de implementatie van een Information Security Management System (ISMS). Om te beoordelen of de informatie van de provincie in de praktijk voldoende beschermd is, is een test uitgevoerd. Daarbij is een aantal kwetsbaarheden met een groot risico ontdekt. Voor het merendeel van de kwetsbaarheden moeten nog maatregelen worden genomen om de kwetsbaarheden te verhelpen. Op basis van de test kan geen algemene uitspraak worden gedaan over de bescherming van de informatie van de provincie.
3. De provincie heeft nog niet voldoende aandacht voor de bewustwording van het belang van informatieveiligheid binnen de organisatie. Het voornemen om medewerkers bewust te maken van risico's op het gebied van informatieveiligheid bestaat sinds 2014. Dit voornemen is nog niet in actie omgezet.
4. De provincie heeft het houden van toezicht op informatieveiligheid goed geregeld. Er zijn diverse onafhankelijke onderzoeken uitgevoerd naar de stand van zaken van informatieveiligheid. De bevindingen zijn op managementniveau besproken en hebben tot vervolgacties geleid. De provincie heeft het afleggen van verantwoording over informatieveiligheid nog niet voldoende geregeld. Informatieveiligheid maakt nog geen onderdeel uit van de P&C-cyclus. Wel is in 2015 voor het eerst schriftelijk gerapporteerd over informatieveiligheid aan de directie. Ook heeft de provincie de zelfevaluatie over informatieveiligheid uitgevoerd.

Aanbevelingen

1. Vraag GS om ervoor te zorgen dat de rollen en verantwoordelijkheden op het gebied van informatieveiligheid in de gehele organisatie goed worden ingevuld.
2. Vraag GS om ervoor te zorgen dat er regelmatig en blijvend aandacht wordt besteed aan het bewustzijn van alle medewerkers van het belang van informatieveiligheid.
3. Spreek met GS af hoe u wordt geïnformeerd over de voortgang en resultaten bij het verbeteren van de informatieveiligheid, waaronder de implementatie van het Information Security Management System (ISMS).

Meer informatie

Dit onderzoek heeft geresulteerd in het rapport Informatieveiligheid en vindt u op onze website www.randstedelijke-rekenkamer.nl. Voor meer informatie kunt u zich wenden tot Ans Hoenderdos, info@randstedelijke-rekenkamer.nl tel. 020 58 18 585.