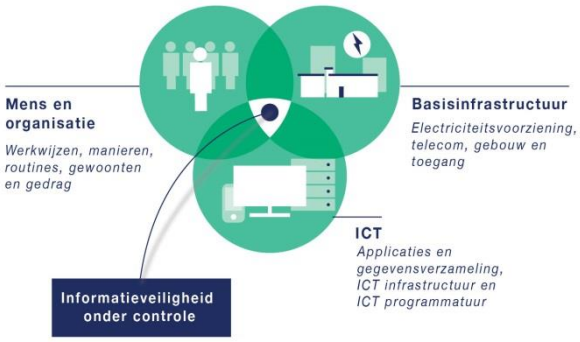
Informatieveiligheid

Provincie Flevoland

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 Flevoland 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 stuurt voldoende op informatieveiligheid. Er zijn goede aanzetten voor de verdeling van verantwoordelijkheden en er is voldoende aandacht voor toezicht op en verantwoording over informatieveiligheid. Ook worden sinds eind 2015 acties ondernomen om het bewustzijn voor informatieveiligheid te vergroten. De invulling van verantwoordelijkheden in de praktijk behoeft nog wel verbetering. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te verbeteren. Generieke maatregelen zijn nog niet volledig geïmplementeerd. Ook zijn risicoanalyses om te bepalen of aanvullende maatregelen nodig zijn, slechts beperkt uitgevoerd.

De hoofdconclusie is gebaseerd op de volgende vier deelconclusies:

1. Verantwoordelijkheden zijn over het geheel genomen goed verdeeld, met een duidelijke rol voor de directie. Verder is een opzet gemaakt voor de toedeling van het eigenaarschap van informatiesystemen. De invulling van verantwoordelijkheden voor informatieveiligheid in de managementlaag onder de directie behoeft nog wel verbetering. Verder is de controlerende rol bij informatieveiligheid niet goed gescheiden van de beleidsrol en de uitvoerende rol.
2. Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. De provincie heeft de benodigde informatieveiligheidsmaatregelen nog niet allemaal uitgevoerd. Er moeten nog generieke informatieveiligheidsmaatregelen worden uitgevoerd, ook bij kritieke systemen. Risicoanalyses om te bepalen voor welke systemen en processen aanvullende maatregelen nodig zijn, zijn slechts in beperkte mate gedaan. 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 hoog risico ontdekt. Voor zover deze kwetsbaarheden technisch van aard zijn, zijn deze grotendeels verholpen. Op basis van de test kan overigens geen algemene uitspraak worden gedaan over de bescherming van de informatie van de provincie.
3. Binnen de provincie bestaat sinds eind 2015 voldoende aandacht voor bewustwording van het belang van informatieveiligheid. Het voornemen om meer aandacht te geven aan bewustwording bestaat sinds eind 2012, maar het duurde tot eind 2015 voordat dit voornemen in actie is 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 hebben geleid tot vervolgacties ter verbetering van de informatieveiligheid. Het afleggen van verantwoording over informatieveiligheid in de provincie is eveneens goed geregeld. Informatieveiligheid maakt deel uit van zowel de bestuurlijke als de ambtelijke P&C cyclus. Verder gebruikt de provincie de interprovinciale monitor zelfevaluatie om de voortgang bij informatieveiligheid te volgen.

Aanbevelingen

1. a. Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld.
   b. Vraag GS om u te informeren over de invulling van rollen en verantwoordelijkheden en de scheiding van functies bij informatieveiligheid.
2. a. Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd.
   b. Vraag GS om te bewaken dat voor alle processen en systemen wordt bepaald of een risicoanalyse nodig is, dat deze risicoanalyses worden uitgevoerd en dat aanvullende maatregelen die daaruit voortkomen worden uitgevoerd.

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.