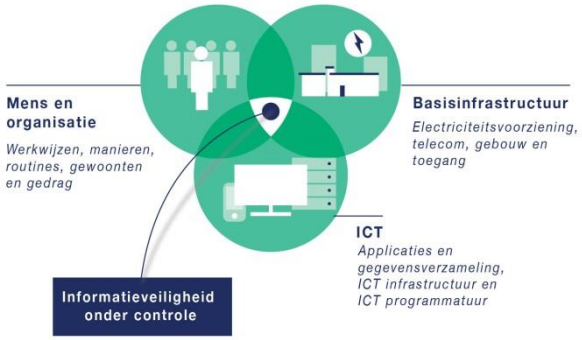
Informatieveiligheid

Provincie Noord-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 Noord-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 besteedt voldoende aandacht aan de bewustwording van het belang van informatieveiligheid binnen de organisatie. Ook heeft de provincie het toezicht op en de verantwoording over informatieveiligheid goed geregeld. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Er is wel verbetering mogelijk in de sturing op het tempo van de implementatie van de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid. Hoewel de provincie veel zaken heeft opgepakt, behoeft de organisatorische verankering en de planmatige aanpak van informatieveiligheid verbetering. Sinds 2016 zet de provincie hiertoe wel stappen. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te bevorderen. Het is bijvoorbeeld niet voor alle bedrijfsprocessen duidelijk welke informatieveiligheidsmaatregelen nodig zijn en de provincie heeft geen zicht of de maatregelen daadwerkelijk zijn uitgevoerd.

De hoofdconclusie is gebaseerd op de volgende vier deelconclusies:

1. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Zo zijn rollen en verantwoordelijkheden in 2012 vastgesteld. De sturing op het tempo van de besluitvorming en uitvoering ten aanzien van informatieveiligheid kan wel beter. De implementatie van de rollen en verantwoordelijkheden is vertraagd. Hoewel de provincie desondanks veel zaken heeft opgepakt, behoeft de organisatorische verankering en planmatige aanpak van informatieveiligheid verbetering. Sinds begin 2016 zet de provincie stappen met het beleggen van rollen en de invulling van verantwoordelijkheden op het gebied van informatieveiligheid.
2. Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. In 2016 dient een geactualiseerde versie van het informatieveiligheidsbeleid te worden vastgesteld. 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. In de provincie is geen test uitgevoerd of de informatie in de praktijk voldoende beschermd is.
3. De provincie heeft voldoende aandacht voor bewustwording van het belang van informatieveiligheid. De provincie heeft onafhankelijke onderzoeken laten verrichten die inzicht geven in de mate van bewustzijn van medewerkers van het belang van informatieveiligheid. De bevindingen van deze onderzoeken zijn gebruikt om het bewustzijn van medewerkers op het gebied van informatieveiligheid te vergroten. In 2015 was het bewustzijn van medewerkers verbeterd ten opzichte van 2013.
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 onder de aandacht gebracht van de directie en hebben tot vervolgacties geleid. Ook heeft de provincie het afleggen van verantwoording over informatieveiligheid goed geregeld. Informatieveiligheid maakt onderdeel uit van de ambtelijke P&C-cyclus en sinds 2016 ook van de bestuurlijke P&C-cyclus. De provincie heeft tevens de zelfevaluatie over informatieveiligheid uitgevoerd.

Aanbevelingen

1. Vraag GS om ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld, wordt gewerkt.
2. Vraag GS om ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld.
3. Vraag GS te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

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.