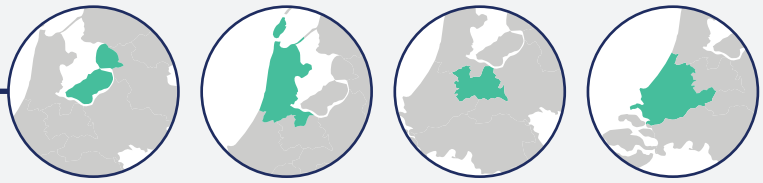
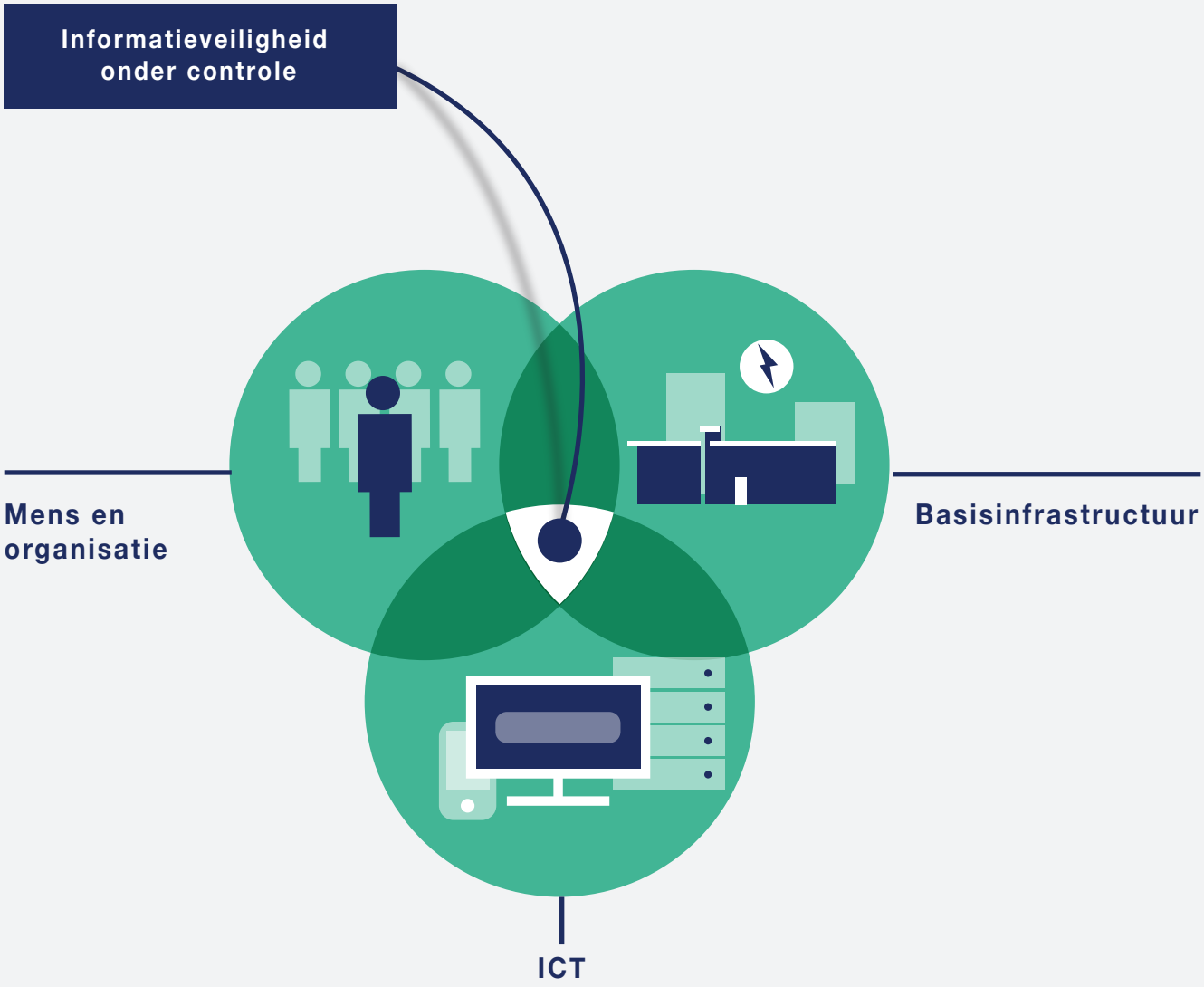
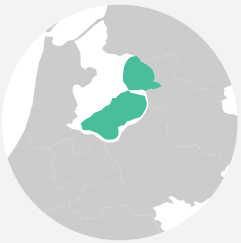
Provincievergelijking

De belangrijkste conclusies per provincie op een rij:



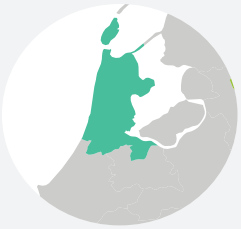


De Conclusies



FLEVOLAND

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.



NOORD-HOLLAND

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 informatie-veiligheid. 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.

UTRECHT

Tot eind 2015 is er ondanks verschillende kritische signalen te weinig gestuurd op de realisatie van acties om de informatieveiligheid te verbeteren. Het gaat dan onder meer om een goede verdeling van verantwoordelijkheden en het vergroten van het bewustzijn voor informatieveiligheid. Hierdoor is weinig tot geen voortgang geboekt bij zaken die belangrijk zijn voor informatieveiligheid, zoals de uitvoering van risicoanalyses. Sinds eind 2015 is de provincie actiever in de verbetering van informatieveiligheid. De eerste stappen bij de invulling van rollen en verantwoordelijkheden zijn gezet. Er komt ook nieuw informatie-veiligheidsbeleid, waaraan voor het eerst ook een plan van aanpak wordt gekoppeld.

ZUID-HOLLAND

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 risico-analyse nodig is, waardoor niet voor alle bedrijfsprocessen duidelijk is welke risico's kunnen optreden.

Deelconclusie 1

Sturing en verantwoordelijkheid

Flevoland

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.

Utrecht

Tot eind 2015 is er te weinig gestuurd op informatieveiligheid. Op verschillende zaken die belangrijk zijn voor de verbetering van de informatieveiligheid, is weinig tot geen voortgang geboekt. Zo was de verdeling van verantwoordelijkheden voor informatieveiligheid lange tijd alleen op papier goed uitgewerkt.
Vanaf eind 2015 heeft de provincie de eerste stappen gezet om meer sturing te geven op informatieveiligheid. Er is een begin gemaakt met de toedeling van verantwoordelijkheden. Verder zijn de vaststelling van nieuw informatieveiligheidsbeleid en een bijbehorend plan van aanpak voorzien in juni 2016.

Noord-Holland

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.

Zuid-Holland

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.

Deelconclusie 2

Beleid en normenkader

Flevoland

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.

Utrecht

Het in 2015 opgestelde informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. Dit beleid wordt echter niet uitgevoerd, omdat de provincie van plan is om in juni 2016 een geactualiseerde versie van het informatieveiligheidsbeleid, met daaraan gekoppeld een plan van aanpak, vast te stellen. Het is niet goed te beoordelen of de provincie de benodigde informatieveiligheidsmaatregelen uitvoert, want een systeem dat hier inzicht in moet geven, is nog niet goed geïmplementeerd. Om te beoordelen of de informatie van de provincie voldoende beschermd is, is een test uitgevoerd. Daarbij is een aantal kwetsbaarheden met een hoog, maar niet direct kritiek risico ontdekt. Ook is geconstateerd dat de provincie onvoldoende monitort of er indicaties zijn voor ongeoorloofde toegang tot provinciale systemen. Op basis van de test kan overigens geen algemene uitspraak worden gedaan.

Noord-Holland

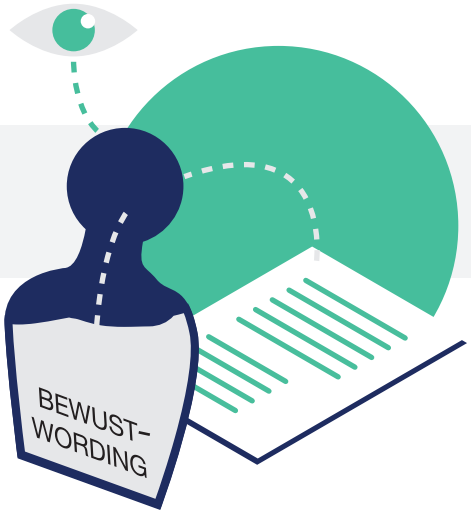
Het informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. In 2016 dient een geactualiseerde versie van het informatieveiligheidsbeleid te worden vastgesteld. Het is niet goed te beoordelen of de provincie de benodigde informatieveiligheidsmaatregelen uitvoert, omdat de provincie de uitvoering van de informatieveiligheidsmaatregelen niet coördineert of registreert en niet voor alle bedrijfsprocessen heeft bepaald of een risicoanalyse nodig is. In deze provincie is geen test uitgevoerd of de informatie in de praktijk voldoende beschermd is.

Zuid-Holland

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.

Deelconclusie 3

Bewustwording



Flevoland

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.

Utrecht

De provincie heeft tot eind 2015 nog onvoldoende aandacht gehad voor de bewustwording van het belang van informatie-veiligheid; er is slechts een beperkt aantal acties ondernomen om dit bewustzijn te vergroten. De provincie heeft wel in 2015 een mystery guest-onderzoek laten uitvoeren om het bewustzijn van informatieveiligheid te meten. Uit dit onderzoek en uit verschillende andere onderzoeken blijkt dat het bewustzijn van informatieveiligheid in de organisatie nog duidelijk verbeterd kan worden. Het vergroten van het bewustzijn in de provinciale organisatie van het belang van informatieveiligheid is een speerpunt van het plan van aanpak, dat in juni 2016 vastgesteld moet worden.

Noord-Holland

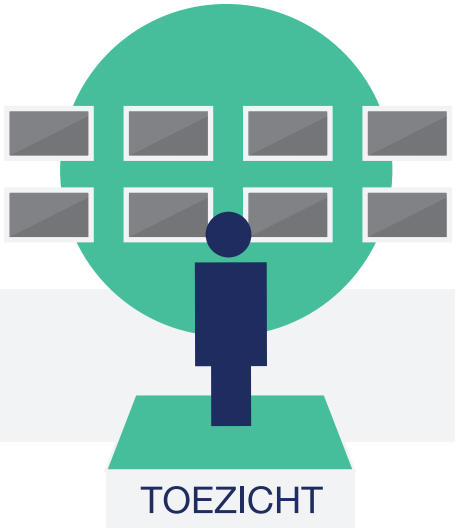
De provincie heeft voldoende aandacht voor bewust-wording van het belang van informatieveiligheid. De provincie heeft onafhankelijke onderzoeken laten verrichten die inzicht geven in de mate van bewustzijn van medewerkers van het belang van informatieveiligheid. De bevindingen van deze onderzoeken zijn 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.

Zuid-Holland

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.

Deelconclusie 4

Verantwoording en toezicht



Flevoland

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 ambtelijk P&C cyclus. Verder gebruikt de provincie de interprovinciale monitor zelfevaluatie om de voortgang bij informatieveiligheid te volgen.

Noord-Holland

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.

Utrecht

De provincie had het houden van toezicht op informatieveiligheid tot medio 2015 nog niet voldoende geregeld. Er zijn diverse onafhankelijke onderzoeken uitgevoerd naar de stand van zaken van informatieveiligheid. Echter, slechts de onderzoeken vanaf medio 2015 leidden tot vervolgacties. Het afleggen van verantwoording over informatieveiligheid in de provincie is nog niet voldoende geregeld. Informatieveiligheid maakt nog geen deel uit van de P&C-cyclus. Er is wel een jaarlijkse zelfevaluatie over informatieveiligheid uitgevoerd, maar die wordt niet gebruikt voor verantwoording of sturing.

Zuid-Holland

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.