randstedelijke rekenkamer
flevoland | noord-holland | utrecht | zuid-holland

EINDRAPPORT

# Informatieveiligheid

Provincie Flevoland | juli 2016

# Voorwoord

'Aantal meldingen cyberaanvallen op overheid verdubbeld'

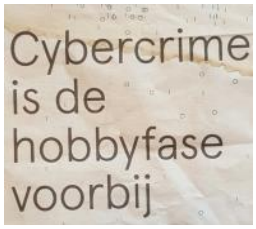
Het aantal gemelde cyberaanvallen op sites en systemen van de overheid is in de afgelopen twee jaar verdubbeld. Het Nationaal Cyber Security Centrum (NCSC) krijgt bijna dagelijks bericht over een aanval. Dat blijkt uit cijfers van het centrum die de Volkskrant heeft opgevraagd.

*Bron: Trouw.nl, 13 augustus 2015*

**Hackers dol op Nederland**

AMSTERDAM - Nederland is massaal het doelwit van spionage-activiteiten. De kraak bij het MH17-onderzoeksteam waar de uiterst geraffineerd opererende Russische cyber-spionagegroep Pawn Storm gevoelig bewijsmateriaal probeerde te ontfutselen, is het topje van de ijsberg.

*Bron: Telegraaf.nl, 25 oktober 2015*




*Bron: NRC, 19 september 2015*

**Gemeente Amersfoort lekt zorggegevens**

Door een blunder van de gemeente Amersfoort zijn de persoonsgegevens van 1000 tot 1500 inwoners die zorg ontvangen via de sociale wijkteams in verkeerde handen gevallen. Het gaat onder meer om BSN's, naam- en adresgegevens en omschrijving van (jeugd)zorg.

*Bron: Algemeen Dagblad, 9 mei 2016*


Gevaar van datalek collectief genegeerd

De put wordt meestal pas gedempt als het te laat is. Bedrijven en overheidsinstellingen lijken blind voor de beveiliging van hun gegevens.

Door Geerlof de Mooij Illustratie Claudie de Cleen

*Bron: De Volkskrant, 12 augustus 2015*

**Bedenk een slimmer wachtwoord dan 'dadada'**

wachtwoorden Zelfs de baas van Facebook heeft een slecht wachtwoord. Dom. Vorig week zijn er weer vele gehackt. Hoe wapen je je?

*Bron: NRC.nl, 13 juni 2016*

Een willekeurige selectie van krantenknipsels over informatieveiligheid gedurende ons onderzoek. Informatieveiligheid blijkt vaak pas urgentie te krijgen na een incident, zoals een datalek, cyberaanval of netwerkstoring. Zo hoorden we bijvoorbeeld in een interview dat voor dit onderzoek is gehouden: *"Een incident is goed voor de aandacht, maar dan graag bij de buren".*

Bij informatieveiligheid gaat het om de bescherming van informatie tegen dreigingen. Vaak wordt dit geassocieerd met nieuwe digitale dreigingen, zoals aanvallen door hackers, verlies van informatie door virussen of diefstal van wachtwoorden. Informatieveiligheid is echter van alle tijden. Het gaat erom dat informatie, zowel op papier als digitaal, alleen door de juiste personen is te zien en te gebruiken. Door de toenemende digitalisering is het risico van inbreuk op gegevens en/of verstoring van bedrijfsprocessen wel groter. Met de huidige smartphones is iedereen een James Bond geworden.

De Randstedelijke Rekenkamer heeft onderzocht of de vier Randstedelijke provincies de informatieveiligheid voldoende hebben gewaarborgd. Eén van de centrale bevindingen van het onderzoek is dat het gedrag van mensen een cruciale rol speelt. Met alleen technische maatregelen, zoals antivirusprogramma's of wachtwoordbeleid, kan informatieveiligheid maar gedeeltelijk worden bevorderd. Een strikt wachtwoordbeleid is bijvoorbeeld zinloos als wachtwoorden regelmatig worden gedeeld of op een zichtbare plek zijn opgeschreven. Niet iedereen is zich daarvan voldoende bewust.

Voor dit onderzoek is een documentenstudie gedaan en zijn interviews gehouden. Wij willen de experts en betrokken provincieambtenaren hartelijk danken voor hun bijdrage aan dit onderzoek. Het onderzoek is uitgevoerd door dr. Annalies Teernstra (onderzoeker), drs. Dharma Tjiam (onderzoeker) en dr. Jeroen van den Heuvel (projectleider tot april).

dr.ir. Ans Hoenderdos-Metselaar MBA
bestuurder/directeur Randstedelijke Rekenkamer

# Infographic

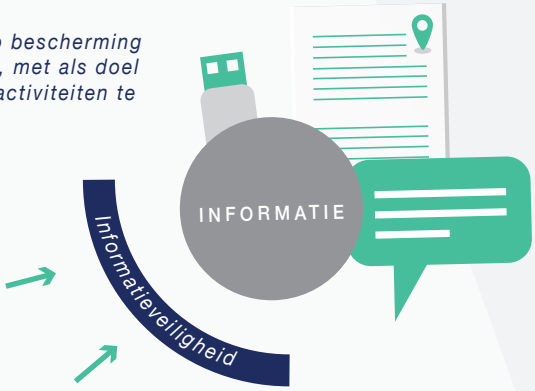
## Context

Informatieveiligheid is van alle tijden. Het is de ruggengraat van goed overheidsbeleid.

De mate van betrouw-baarheid, bruikbaarheid en toegankelijkheid van informatie is van invloed op een rechtmatige, doel-matige en doeltreffende overheid. Een goede sturing op informatie-veiligheid voorkomt schade die van invloed is op de kwaliteit van het functioneren van de provincie. In het digitale tijdperk is dat nog belangrijker.

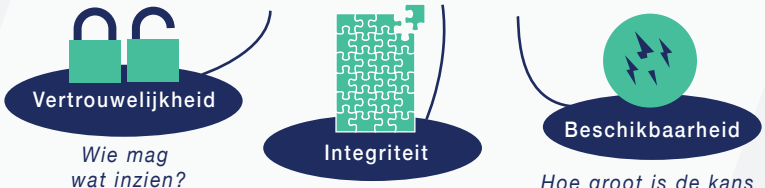
### 1. Wat is informatieveiligheid?

*Informatieveiligheid richt zich op bescherming van informatie tegen dreigingen, met als doel om de continuïteit van bedrijfsactiviteiten te waarborgen.*




*Als de informatieveiligheid onvoldoende is gewaar-borgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie.*

*Informatieveiligheid is te meten aan 3 aspecten:*




*Wie mag wat inzien?*

*Is de informatie juist, up-to-date en volledig?*

*Hoe groot is de kans dat een informatie-systeem uitvalt?*

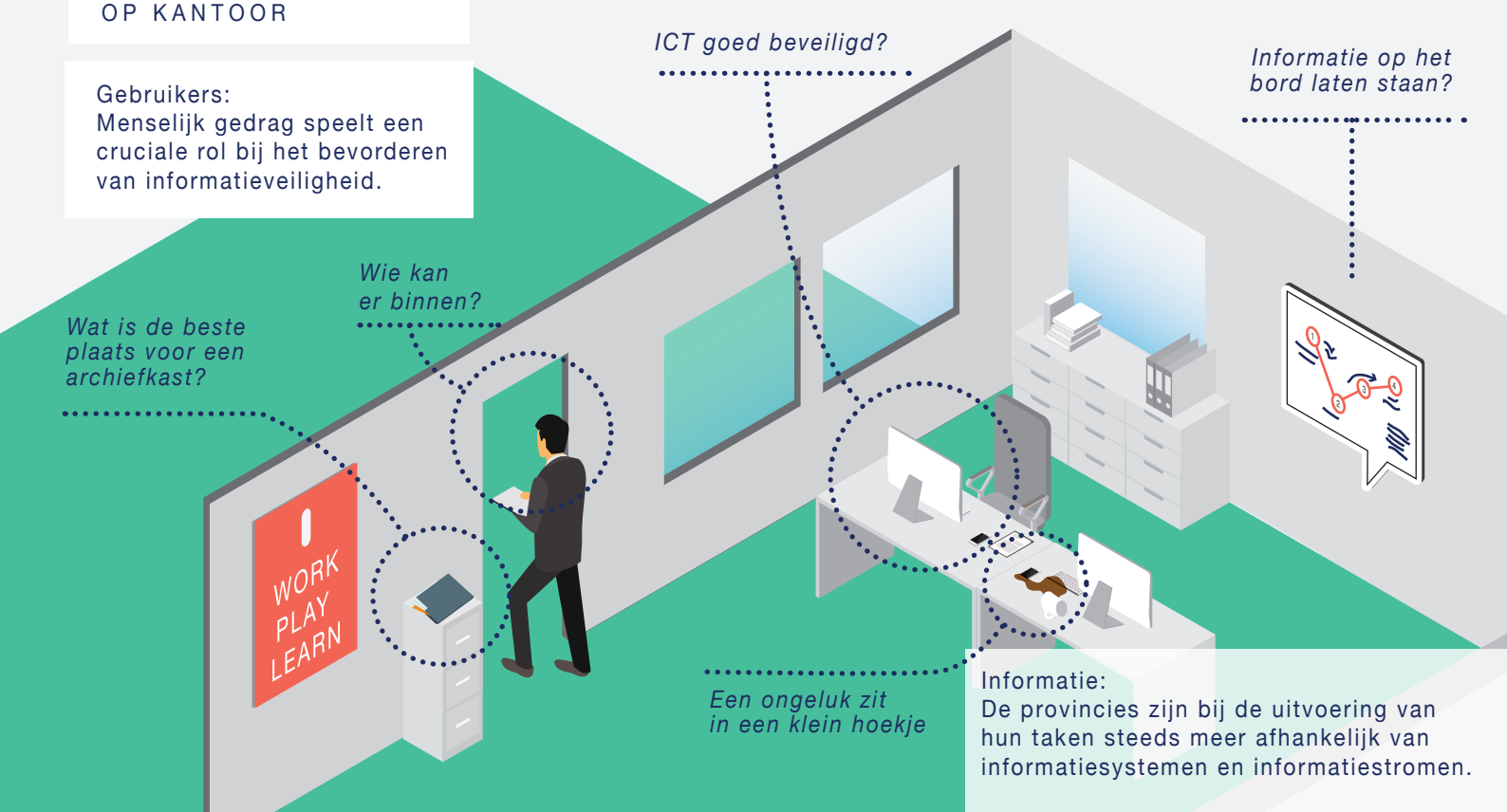
*Het doel van informatieveiligheid is om risico's tot een voor de provincie vastgesteld acceptabel niveau terug te brengen.*

*De maatregelen die genomen worden, moeten in verhouding staan tot de grootte van het risico.*

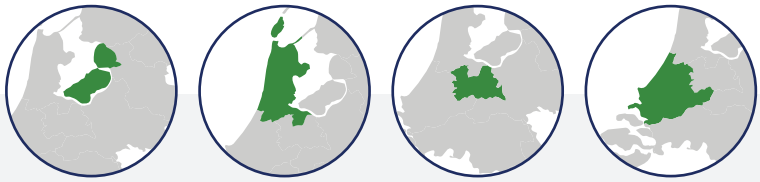
***100 procent veiligheid bestaat niet.***


### INFORMATIEVEILIGHEID OP KANTOOR

Gebruikers:
Menselijk gedrag speelt een cruciale rol bij het bevorderen van informatieveiligheid.



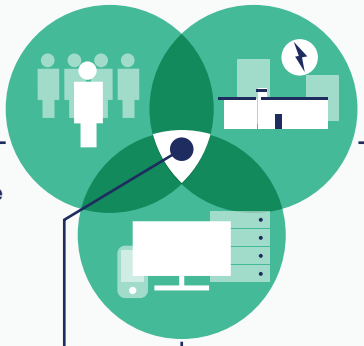

Informatie:
De provincies zijn bij de uitvoering van hun taken steeds meer afhankelijk van informatiesystemen en informatiestromen.



## 2. Waarop kan de Provincie sturen?

*Behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.*

*Aandachtsgebieden van informatieveiligheid:*



**Mens en organisatie**

*Werkwijzen, manieren, routines, gewoonten en gedrag*

**Basis-infrastructuur**

*Electriciteits-voorziening, telecom, gebouw en toegang*

**ICT**

*Applicaties en gegevensverzameling, ICT infrastructuur en ICT programmatuur*

**Informatieveiligheid onder controle**

## 3. Aan welke maatregelen moeten we denken?

*Voorbeelden van maatregelen die getroffen kunnen worden om de informatieveiligheid te waarborgen*

**Voorbeeld 1: Bedieningssysteem bruggen en sluizen**

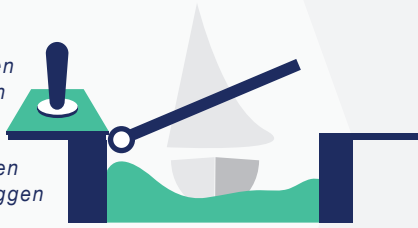
*Beschikbaarheid*

↓

*Planning werkzaamheden aan bedieningssysyteem*

↓

*In het pleziervaartseizoen optimale bediening bruggen*



**Voorbeeld 2: Fysieke toegangsbeveiliging**


*Spreek je onbekenden aan in gedeelten van gebouwen die alleen toegankelijk zijn voor medewerkers?*


## INFORMATIEVEILIGHEID ONDERWEG

Maatschappelijke verantwoordelijkheid: burgers, bedrijven en overheidspartners moeten erop kunnen rekenen dat de informatievoorziening betrouwbaar is en dat zorgvuldig wordt omgegaan met gegevens.

# Inhoudsopgave

# Conclusies en Aanbevelingen

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. Als de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. Provincies hebben hierin een maatschappelijke verantwoordelijkheid: burgers, bedrijven en overheidspartners moeten erop kunnen rekenen dat de informatievoorziening betrouwbaar is en dat zorgvuldig wordt omgegaan met gegevens. Bovendien kunnen inbreuken op informatieveiligheid leiden tot financiële en imagoschade.

Informatieveiligheid heeft betrekking op het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Dat wil zeggen dat informatie door de juiste personen is te zien en te gebruiken (vertrouwelijk), juist, volledig en actueel (integer/betrouwbaar) en toegankelijk is (beschikbaar). Om informatieveiligheid te waarborgen, kunnen maatregelen worden genomen op de aandachtsgebieden ICT, basisinfrastructuur en mens & organisatie. Bij ICT gaat het bijvoorbeeld om antivirusprogramma's, bij basisinfrastructuur om de toegangsbeveiliging van gebouwen en bij mens & organisatie om het creëren van bewustzijn bij medewerkers in hun eigen handelen ten aanzien van informatieveiligheid. Omdat 100 procent veiligheid niet bestaat, is het doel van informatieveiligheid risico's tot een acceptabel niveau terug te brengen.

Provincies richten zich al enige tijd op het bevorderen van informatieveiligheid. Zo heeft het Cibo[1] in 2010 de Interprovinciale Baseline Informatiebeveiliging (IBI) opgesteld. De IBI is het basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. In 2016 is deze baseline vernieuwd. Ook hebben alle provincies eind 2014 het Convenant Interprovinciale Regulering Informatieveiligheid ondertekend. Dit is een afsprakenkader waarmee provincies verantwoordelijkheid nemen voor het borgen van informatieveiligheid. Daarnaast had de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID)[2] als doel om informatieveiligheid gedurende twee jaar op de bestuurlijke agenda van alle overheidslagen te zetten. Begin 2015 heeft de Taskforce haar werkzaamheden beëindigd en overgedragen aan de betrokken (koepel)organisaties.

De ondertekening van het convenant en de beëindiging van de werkzaamheden van de Taskforce BID zijn voor de Rekenkamer aanleiding geweest om de informatieveiligheid van de provincie te onderzoeken. Het doel van het onderzoek is om inzichtelijk te maken of de informatieveiligheid van de provincie voldoende is geborgd.

**Centrale onderzoeksvraag**
Heeft de provincie Flevoland de informatieveiligheid voldoende geborgd?

**Conclusie**
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

[1] Het Centraal Informatiebeveiligingsoverleg (Cibo) is onderdeel van het IPO en is een platform waarin provincies de gezamenlijke ontwikkeling van informatieveiligheid vormgeven.
[2] In de Taskforce BID waren het Rijk, het IPO, de VNG en de Unie van Waterschappen vertegenwoordigd.

volledig geïmplementeerd. Ook zijn risicoanalyses om te bepalen of aanvullende maatregelen nodig zijn, slechts beperkt uitgevoerd.

De centrale onderzoeksvraag is beantwoord aan de hand van vier deelvragen. Hieronder is antwoord gegeven op de deelvragen in de vorm van deelconclusies en een toelichting daarop. De deelvragen hebben betrekking op de volgende onderwerpen: sturing en verantwoordelijkheid, informatieveiligheidsbeleid, bewustwording van informatieveiligheid en verantwoording en toezicht. Daarbij zijn per onderwerp, indien nodig, aanbevelingen opgenomen.

## Sturing & Verantwoordelijkheid

*1. Heeft de provincie de sturing op en de verantwoordelijkheid voor informatieveiligheid goed verankerd?*

**Deelconclusie 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.

**Toelichting**
Dat er wordt gestuurd op informatieveiligheid, blijkt uit besluiten over de aanpak van verschillende belangrijke zaken, bijvoorbeeld over de verbetering van de bewustwording in de organisatie van het belang van informatieveiligheid. Verder zijn verantwoordelijkheden, taken en bevoegdheden voor informatieveiligheid duidelijk toegekend aan bestaande functies of doelgroepen, en is er een opzet voor het eigenaarschap van processen en systemen. De eindverantwoordelijkheid voor informatieveiligheid berust bij de directie; de directie is in het algemeen ook goed betrokken (bevindingen 1 en 2).

In de uitvoering is wel verbetering mogelijk. De managementlaag onder de directie is zich nog niet ten volle bewust van rollen en verantwoordelijkheden bij informatieveiligheid. Hierdoor is het eigenaarschap bij veel systemen nog niet belegd en bestaat ook terughoudendheid om dat eigenaarschap en de bijbehorende verantwoordelijkheid te aanvaarden. Verder zijn de controlerende rol, de beleidsrol en de uitvoerende rol bij informatieveiligheid niet goed gescheiden. Dit maakt onafhankelijke controle moeilijker (bevindingen 1 en 2). Uit het bestuurlijk wederhoor is gebleken dat de provincie naar aanleiding van deze conclusie van de Rekenkamer heeft besloten de controlerende rol beter te scheiden (zie verder de toelichting onder de aanbevelingen).

**Aanbevelingen**
1a. Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld.
1b. Vraag GS om u te informeren over de invulling van rollen en verantwoordelijkheden en de scheiding van functies bij informatieveiligheid.

De Rekenkamer heeft aanbeveling 1b aangepast naar aanleiding van het bestuurlijk wederhoor. De aanbeveling luidde eerst: ‘Vraag GS om de controlerende rol op informatieveiligheid gescheiden van de beleidsrol en de uitvoerende rol te positioneren.’ GS gaven in hun bestuurlijke reactie aan deze aanbeveling niet te kunnen onderschrijven, onder meer vanwege het besluit om de onafhankelijke onderzoeken naar informatieveiligheid onder verantwoordelijkheid van de concerncontroller te laten uitvoeren. Bij navraag is gebleken dat dit besluit op

29 juni 2016 door de directie is genomen naar aanleiding van het rapport van de Rekenkamer.[3] Hieruit blijkt dat de provincie alert is op mogelijkheden om de informatieveiligheid te verbeteren.

De Rekenkamer vindt het besluit om de onafhankelijke onderzoeken onder verantwoordelijkheid van de concerncontroller te laten uitvoeren, een goede stap om de controlerende rol bij informatieveiligheid meer gescheiden te positioneren. Om die reden hebben wij de oorspronkelijke aanbeveling 1b geschrapt. In de plaats daarvan is een nieuwe aanbeveling 1b gekomen, die is gericht op de informatie aan PS over de invulling van de rollen en verantwoordelijkheden bij informatieveiligheid en de inrichting van de functiescheiding. Dit kan in het kader van de al gebruikelijke bestuurlijke en ambtelijke P&C cyclus, waar het afleggen van verantwoording over informatieveiligheid deel van uitmaakt en die al goed is geregeld (zie deelconclusie 4).

### Informatieveiligheidsbeleid

2. *Is het informatieveiligheidsbeleid in opzet, uitvoering én in resultaat adequaat?*
   a. *Heeft de provincie een informatieveiligheidsbeleid opgesteld dat voldoet aan de daaraan te stellen eisen?*
   b. *Voert de provincie de benodigde informatieveiligheidsmaatregelen uit?*
   c. *Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?*

**Deelconclusie 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.

**Toelichting**
Het beleidsplan informatieveiligheidsbeleid van de provincie voldoet aan de eisen: het is in 2015 door de directie vastgesteld en noemt expliciet de Interprovinciale Baseline Informatiebeveiliging (IBI) als basis (bevinding 3).

In de IBI wordt onderscheid gemaakt tussen generieke en aanvullende informatieveiligheidsmaatregelen. Generieke maatregelen dienen altijd uitgevoerd te worden om aan het basisniveau voor informatieveiligheid te voldoen. Aanvullende maatregelen zijn alleen nodig als na een risicoanalyse blijkt dat een bepaald proces of systeem een hoger niveau van informatieveiligheid vraagt. Uit eigen controles van de provincie is gebleken dat ook bij kritieke systemen de generieke maatregelen doorgaans niet volledig geïmplementeerd zijn. De uitvoering van generieke maatregelen krijgt daarom prioriteit. Om dezelfde reden heeft de provincie, op een enkele uitzondering na, nog geen risicoanalyses uitgevoerd (bevinding 4 en 5).

De Rekenkamer heeft een praktijktest uitgevoerd bij de provincie (onderzoeksvraag 2c). In de test zijn drie belangrijke kwetsbaarheden met een groot risico gevonden. Deze kwetsbaarheden hebben betrekking op de mobiele apparaten iPhone en iPad. Zo bleken via één van de apps op de iPad documenten met vertrouwelijke informatie in te zien. De kwetsbaarheden die technisch oplosbaar zijn, zijn grotendeels verholpen. Een deel van

[3] Provincie Flevoland (2016), Conceptverslag directievergadering 29 juni 2016.

de kwetsbaarheden is echter gerelateerd aan het gedrag van medewerkers ten aanzien van informatieveiligheid (bevinding 6).

**Aanbevelingen**
2a. Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd.
2b. 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.

## Bewustwording van informatieveiligheid

3. *Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?*

**Deelconclusie 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.

**Toelichting**
De provincie heeft eind 2012 in de nota Informatie in Beweging het voornemen voor een bewustwordingsprogramma opgenomen. Dit leidde tot het opstellen van een projectplan bewustwording informatieveiligheid in 2014. Dit projectplan is eind 2015 uitgewerkt in een activiteitenplan. De eerste activiteiten zijn begin 2016 gestart (bevinding 7).

**Geen aanbevelingen**

## Verantwoording & Toezicht

4. *Heeft de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?*

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

**Toelichting**
In 2014/2015 heeft de provincie vier onafhankelijke onderzoeken naar de stand van zaken bij informatieveiligheid laten uitvoeren, waaronder drie penetratietesten (o.a. op de bediening van bruggen en sluizen) De bevindingen van deze onderzoeken hebben geleid tot verbeteracties die ook worden gemonitord (bevinding 9).

Voor wat betreft de bestuurlijke P&C cyclus is een korte toelichting over informatieveiligheid opgenomen in de programmabegroting 2016 en in de jaarstukken 2014. Informatieveiligheid is ook onderdeel van de ambtelijke

P&C cyclus. Het werkplan Informatisering en Automatisering (I&A) wordt gemonitord (bevinding 8). De provincie heeft in 2014 en 2015 de interprovinciale monitor zelfevaluatie over informatieveiligheid uitgevoerd. Aan de hand van deze monitor zijn de belangrijkste risico's benoemd en maatregelen geformuleerd. Deze maatregelen zijn opgenomen in het Werkplan I&A (bevinding 10).

**Geen aanbevelingen**

# Reactie Gedeputeerde Staten

PROVINCIE FLEVOLAND

Postbus 55
8200 AB Lelystad

*Telefoon*
(0320)-265265
*Fax*
(0320)-265260
*E-mail*
provincie@Flevoland.nl
*Website*
www.flevoland.nl

Randstedelijke Rekenkamer
Mevrouw Dr. Ir. A.W.C. Hoenderdos-Metselaar
Teleportboulevard 110
1043 EJ AMSTERDAM

*Verzenddatum* — 6 JULI 2016
*Bijlagen*
*Uw kenmerk*
*Ons kenmerk* 1929867

*Onderwerp*
Bestuurlijke reactie Informatieveiligheid

Geachte mevrouw Hoenderdos,

U heeft ons op 17 juni jongstleden de bestuurlijke nota Informatieveiligheid in concept toegezonden. Graag maken we van de gelegenheid gebruik om daarop in het kader van het bestuurlijk wederhoor te reageren.

**Algemeen**
Eind augustus 2015 is de opzet voor dit onderzoek gepubliceerd. In de maanden die daarop volgden is intensief met de ambtelijke organisatie gesproken, merendeels met de medewerker belast met informatieveiligheid. Het onderzoeksproces hebben wij als zorgvuldig ervaren en dat geldt ook voor de test van de mobile devices. In de uitvoering van uw onderzoek herkennen wij de aanpak uit uw onderzoeksopzet. Uw aanbevelingen zijn via Provinciale Staten (PS) aan ons gericht en wij gaan daarom hieronder daar op in.

Het onderzoek is gelijktijdig uitgevoerd in de vier provincies waar de Randstedelijke Rekenkamer werkzaam is. Wij hadden op basis van de laatste zin van hoofdstuk 6 Werkwijze van uw onderzoeksopzet verwacht dat het eindrapport op een aantal onderdelen een provincievergelijking zou bevatten. Deze interprovinciale vergelijking zouden we gebruiken bij onze doorontwikkeling.

**Ontwikkeling**
De rekenkamer constateert dat de provincie veel aandacht besteed aan informatieveiligheid. Wij vinden het prettig dat de onderzoekers dit hebben geconcludeerd. De laatste jaren zijn we er in geslaagd om informatieveiligheid op een hoger plan te brengen. Onze risico-georiënteerde aanpak heeft aantoonbaar geleid tot een structurele verbetering van de informatieveiligheid. Inmiddels hebben andere provincies onze aanpak overgenomen. Onze directie bepaalt en monitort de activiteiten die daarvoor worden uitgevoerd.

**Conclusies en aanbevelingen**
De hoofdvraag die u heeft gesteld is in hoeverre de provincie Flevoland de informatieveiligheid voldoende heeft geborgd. In onze directie is recent over het rapport gesproken.

*Inlichtingen bij*
drs. G. de Vos

*Doorkiesnummer*
0320 265759

*Bezoekadres*
Visarenddreef 1
Lelystad

*Bij het provinciehuis is het aantal parkeerplaatsen voor bezoekers (ingang Visarenddreef) beperkt. In de omgeving van het provinciehuis bevindt zich een aantal parkeergarages. Vanwege de ligging naast het NS-station is het provinciehuis uitstekend bereikbaar met het openbaar vervoer. Meer informatie over de bereikbaarheid vindt u op onze website www.flevoland.nl.*

| | Conclusies en aanbevelingen | Bestuurlijke reactie |
|---|---|---|
| Conclusie | De provincie Flevoland 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. | Wij stemmen met grote tevredenheid met deze conclusie in. Onze inspanningen van vooral de laatste jaren hebben goede resultaten opgeleverd. Onze insteek daarbij is met name een risicogeoriënteerde aanpak geweest. Sinds de twaalf provincies gezamenlijk een ambitie hebben geformuleerd en onderschreven, hebben wij daaraan in onze organisatie structureel aandacht gegeven. En ook in de recent vastgestelde Meerjarenaanpak Bedrijfsvoering is informatieveiligheid een cruciaal element. |
| Deelconclusie 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. | Deze conclusie onderschrijven wij. deels, aangezien deze verdeling in het informatieveiligheidsbeleid is vastgelegd |
| Aanbeveling 1a | Vraag GS om ervoor te zorgen dat rollen en verantwoordelijkheden bij informatieveiligheid door de gehele organisatie goed worden ingevuld. | De aanbeveling pakken wij risico-georiënteerd op, waarbij we de tien meest kritische systemen eerst ter hand nemen. Het eigenaarschap van de systemen met bijbehorende rollen en verantwoordelijkheden wordt aan de hand van een PDCA-aanpak op voldoende niveau gebracht. |
| Aanbeveling 1b | Vraag GS om de controlerende rol op informatieveiligheid gescheiden van de beleidsrol en de uitvoerende rol te positioneren. | Deze aanbeveling kunnen wij niet onderschrijven. Bij het vaststellen van het informatiebeveiligingsbeleid in mei 2015 is bepaald dat de directie verantwoordelijk is voor het vaststellen van het beleid. Het voorbereiden en toetsen van het beleid zijn belegd bij de adviseur informatieveiligheid. Het uitvoeren en verbeteren ligt bij de afdelingshoofden / systeemeigenaren. |

| | | |
|---|---|---|
| | | in het kader van de ontwikkeling van informatievoorziening is besloten om de controlerende rol - met name de tweejaarlijkse onafhankelijke toetsen -onder de verantwoordelijkheid van de concerncontroller te brengen. Wij vinden dat hiermee een juiste invulling was gegeven aan functiescheiding en dat het nu nog verder verbeterd is. |
| Deelconclusie 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.<br><br>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. | Deze conclusie onderschrijven wij |
| Aanbeveling 2a | Vraag GS om te bewaken dat alle generieke maatregelen voor informatieveiligheid zo snel mogelijk worden uitgevoerd. | Wij hebben alle geïdentificeerde maatregelen geïnventariseerd en geprioriteerd voor de komende vier jaar. De maatregelen met een hoog risico worden in 2016 gemitigeerd. Alle maatregelen met een midden risico zijn eind 2017 in uitvoering. Vervolgens kan een onafhankelijke toets bepalen of de directie een zogenaamde "in control"-verklaring kan afgeven. De uitvoering van de door de directie vastgestelde verbeteracties wordt maandelijks gemonitord en gerapporteerd aan de IT-Raad. |
| Aanbeveling 2b | Vraag GS om te bewaken dat voor alle processen en systemen wordt bepaald of | De inventarisatie van de systemen wordt in juli 2016 afgerond. |

| | | |
|---|---|---|
| | een risicoanalyse nodig is, dat deze risicoanalyses worden uitgevoerd en dat aanvullende maatregelen die daaruit voortkomen, worden uitgevoerd. | Elke systeemeigenaar gaat vervolgens indien relevant een Afhankelijkheids- en Kwetsbaarheidsanalyse uitvoeren. Alle uitkomsten worden door de adviseur Informatieveiligheid gebundeld en ter goedkeuring voorgelegd aan de directie. Dit besluit bevat ook de keuze voor de tien meest kritische systemen van de provincie. Het uitvoeren van risicoanalyses op processen is inmiddels interprovinciaal ingebracht bij het Strategische Overleg, maar is daar vooralsnog niet opgepakt. We hebben hierbij voorgesteld om de tien meest kritische processen van de provincies vast te stellen. |
| Deelconclusie 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. | Wij stemmen met deze conclusie in en zijn ons ervan bewust dat in de organisatie structureel aandacht nodig is voor informatieveiligheid. |
| Deelconclusie 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 ambtelijk P&C cyclus. Verder gebruikt de provincie de interprovinciale monitor zelfevaluatie om de voortgang bij informatieveiligheid te volgen. | Deze conclusie onderschrijven wij. |

Het onderwerp gaat over de kwaliteit van de informatieveiligheid in de organisatie. Onze organisatie is daar intensief mee bezig. Ook in het kader van de Meerjarenaanpak bedrijfsvoering komt het aan de orde. We zijn dan ook geïnteresseerd in de behandeling van dit onderzoek in de staten en zien wij deze met vertrouwen tegemoet.

Hoogachtend,

Gedeputeerde Staten van Flevoland,
de secretaris, de voorzitter,

mr. drs T. van der Wal L. Verbeek

# Nawoord Rekenkamer

De Rekenkamer dankt GS voor hun reactie. Wij zijn verheugd dat het college het grootste deel van de conclusies en aanbevelingen onderschrijft.

Tot nu toe was het gebruikelijk dat de Rekenkamer alleen via het nawoord op de bestuurlijke reactie van GS inging. Bij dit onderzoek hebben wij een andere lijn gevolgd. Wij hebben contact opgenomen met de directie om na te gaan waarom de provincie een aanbeveling over het meer onafhankelijk positioneren van de controlerende rol bij informatieveiligheid niet onderschreef. Het bleek dat deze aanbeveling van de Rekenkamer voor de provincie aanleiding was om de onafhankelijke controlerende rol te versterken.

De Rekenkamer vindt dat de provincie met dit besluit onze oorspronkelijke aanbeveling (het betreft aanbeveling 1b) op een goede manier uitvoert. Daarom hebben wij deze aanbeveling vervangen door een nieuwe aanbeveling, die is gericht op de informatie aan PS over de invulling van rollen en verantwoordelijkheden bij informatieveiligheid en de inrichting van de functiescheiding. In de conclusies en aanbevelingen lichten we deze aanpassing inhoudelijk toe. Tot slot willen wij onze waardering uitspreken voor de directie en de contactpersonen van de provincie voor de medewerking gedurende dit onderzoek. In het bijzonder hebben we door hen de conclusies en aanbevelingen kunnen laten aansluiten bij de meest recente besluiten, zodat er een zo actueel mogelijk rapport ligt voor PS.

De behandeling van het rapport in PS zien we met belangstelling tegemoet.

# | 1 | Inleiding

## 1.1 Aanleiding

*De overheid en informatieveiligheid*

We leven in een tijd die wordt gekarakteriseerd door het opkomen van de informatiesamenleving. Dit betekent dat onze activiteiten meer en meer zijn georganiseerd in informatienetwerken, worden geconcentreerd rondom informatieverwerking en zijn gebaseerd op informatietechnologie.[4] Ook voor provincies geldt dat zij voor de uitvoering van hun primaire taken steeds meer afhankelijk zijn van informatiesystemen en informatiestromen. Digitale veiligheid neemt dan ook een steeds belangrijker positie in.[5] Overheden hebben hierin een maatschappelijke verantwoordelijkheid: burgers, bedrijven en overheidspartners moeten erop kunnen rekenen dat de informatievoorziening betrouwbaar is en dat zorgvuldig wordt omgegaan met gegevens. Een betrouwbare informatievoorziening is van essentieel belang voor het functioneren van de processen van de overheid.[6] Daarnaast kunnen inbreuken op digitale veiligheid leiden tot financiële en imagoschade.[7] Uit onderzoek blijkt echter dat de helft van alle digitale inbraakpogingen vaak pas na maanden wordt ontdekt.[8] Daarnaast toonden onder meer het DigiNotar-incident en Lektober (2011) en het Dorifel-virus (2012) aan dat de digitale omgeving van overheden een aantal kwetsbaarheden bevatte en de informatieveiligheid tekortschoot.[9] Mede naar aanleiding van bovenstaande ontwikkelingen zijn er verschillende initiatieven genomen om de informatieveiligheid van overheden te verbeteren. Deze initiatieven richten zich niet alleen op de digitale veiligheid, maar ook op de fysieke veiligheid en het gedrag van mensen ten aanzien van informatieveiligheid (zie Figuur 1).


**Figuur 1 Bewustwordingscampagne iBewustzijn Overheid[10] (Bron: iBewustzijn Overheid, 2015)**

[4] Castells (1996), The Information Age: Economy, Society, and Culture.
[5] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt.
[6] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging.
[7] Rekenkamer Den Haag (2014), Digitale Veiligheid.
[8] FOX-IT (2015), www.fox-it.nl.
[9] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
[10] iBewustzijn Overheid is een ondersteuningsprogramma van het ministerie van BZK en de koepelorganisaties om bewuste omgang met informatie te stimuleren.

Zo is in 2013 de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) opgericht, waarin het Rijk, het Interprovinciaal Overleg (IPO), de Vereniging Nederlandse Gemeenten en de Unie van Waterschappen waren vertegenwoordigd. De Taskforce BID had als doel om het onderwerp informatieveiligheid gedurende twee jaar op de bestuurlijke agenda te zetten, om het bewustzijn van informatieveiligheid te vergroten. Ook was het doel om instrumenten te ontwikkelen om sturing op informatieveiligheid door bestuur en management mogelijk te maken.[11] Op 13 februari 2015 heeft de Taskforce BID haar coördinerende werkzaamheden beëindigd en zijn de betrokken (koepel)organisaties en het Ministerie van BZK zelf verder gegaan met de ontwikkeling van informatieveiligheid.

*De provincies en informatieveiligheid*

Reeds voor de oprichting van de Taskforce BID in 2013 richtten de provincies zich op het bevorderen van informatieveiligheid. Omdat provincies vergelijkbare werkprocessen hebben, streven zij onder het motto 'generiek waar het kan, specifiek waar het moet' zoveel mogelijk naar samenwerking op het terrein van informatieveiligheid.[12] Vanuit dit streven is het Centraal Informatiebeveiligingsoverleg (Cibo) opgericht, dat onderdeel is van het IPO. Het Cibo is een platform waarin provincies kennis en ervaring uitwisselen en de gezamenlijke ontwikkeling van informatieveiligheid vormgeven.[13] Elke provincie is vertegenwoordigd in het Cibo door een medewerker die werkzaam is op het gebied van informatieveiligheid. In 2010 heeft het Cibo, in samenwerking met het IPO, de Interprovinciale Baseline Informatiebeveiliging (IBI) opgesteld.[14] De IBI vormt het formele basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. Het doel is om provincies op een vergelijkbare manier te laten werken aan informatieveiligheid. De IBI geeft een standaard werkwijze waarmee per bedrijfsproces of informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden. Het principe van 'Verplichtende Zelfregulering' staat centraal. Dit betekent dat iedere provincie zelf verantwoordelijk is voor het informatieveiligheidsbeleid, met als stok achter de deur dat wanneer de informatieveiligheid onvoldoende wordt geïntegreerd in de bedrijfsvoering, verplichtingen op basis van (wettelijke) regelgeving zullen volgen.[15]

Om de informatieveiligheid van de provincies verder te optimaliseren en professionaliseren is het Convenant Interprovinciale Regulering Informatieveiligheid opgesteld, dat eind 2014 is ondertekend door alle provincies afzonderlijk en op zowel ambtelijk als bestuurlijk niveau is vastgesteld.[16] Het convenant is een afsprakenkader waarmee provincies verantwoordelijkheid nemen voor het opstellen van informatieveiligheidsbeleid en het uitvoeren en handhaven ervan. Het is de bedoeling dat de provincies op deze manier één standaard ontwikkelen en behouden waardoor informatieveiligheid geen vrijblijvend proces is. Het convenant helpt op deze manier de verplichtende zelfregulering te realiseren. Als het convenant echter tot onvoldoende verbetering leidt, dan blijft het mogelijk dat het Rijk regelgeving opstelt.

*Concrete aanleidingen voor het onderzoek door de Randstedelijke Rekenkamer*

De ondertekening van het convenant (november 2014) en de beëindiging van de werkzaamheden van de Taskforce BID (februari 2015) zijn voor de Rekenkamer aanleiding geweest om de informatieveiligheid van de vier Randstedelijke provincies te onderzoeken. Het is relevant in hoeverre het convenant daadwerkelijk is ingebed in de bestuurlijke, organisatorische en technische processen van de provincies. Indien informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. Een andere aanleiding is gevonden in een onderzoek van de Rekenkamer Den

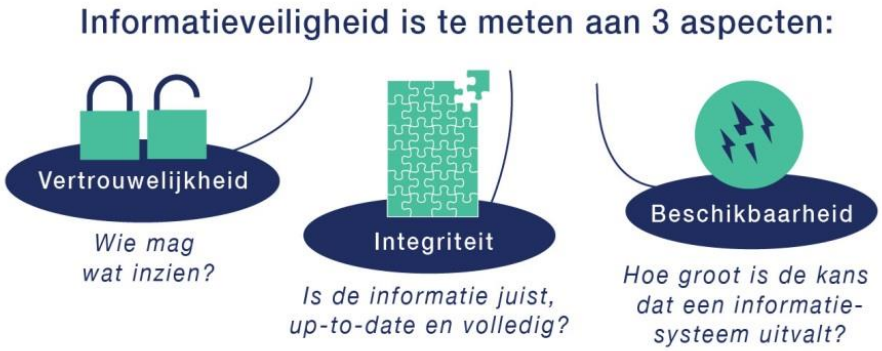
[11] Taskforce BID (2015), www.taskforcebid.nl.
[12] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid.
[13] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014.
[14] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging.
[15] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014.
[16] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid.

Haag naar de digitale veiligheid van de ICT-infrastructuur en van privacygevoelige informatie bij de gemeente Den Haag in 2014.[17] De Rekenkamer Den Haag concludeerde dat het zicht en de grip op informatieveiligheid door de gemeenteraad onvoldoende was. De gemeentelijke website bleek veilig te zijn. Maar op het interne netwerk werden de nodige kwetsbaarheden in de veiligheid gevonden en het bleek mogelijk op verschillende manieren van buiten toegang tot het interne netwerk te verkrijgen. De Rekenkamer Den Haag deed de aanbeveling om meer bestuurlijke aandacht te geven aan digitale veiligheid en periodiek integrale testen uit te voeren.

## 1.2 Achtergrond

De begrippen ‘informatieveiligheid’ en ‘informatiebeveiliging’ worden vaak door elkaar gebruikt. Er is echter een verschil tussen beide begrippen: om informatieveiligheid (het doel) te waarborgen, wordt gebruik gemaakt van informatiebeveiliging (de maatregelen).[18] De Rekenkamer kiest voor de term ‘informatieveiligheid’, omdat deze term meer recht doet aan de breedte van het onderwerp dan de term ‘informatiebeveiliging’, dat vaak wordt geassocieerd met ICT.

Informatieveiligheid richt zich op bescherming van informatie tegen dreigingen om de continuïteit van bedrijfsactiviteiten te waarborgen.[19] Indien de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico’s ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen die genomen worden, moeten echter in verhouding staan tot de grootte van het risico. 100 procent veiligheid bestaat niet. Het doel van informatieveiligheid is daarom risico’s tot een voor de provincie vastgesteld acceptabel niveau terug te brengen.[20] Informatieveiligheid heeft betrekking op het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie (zie Figuur 2).[21]




**Figuur 2 Aspecten van informatieveiligheid**

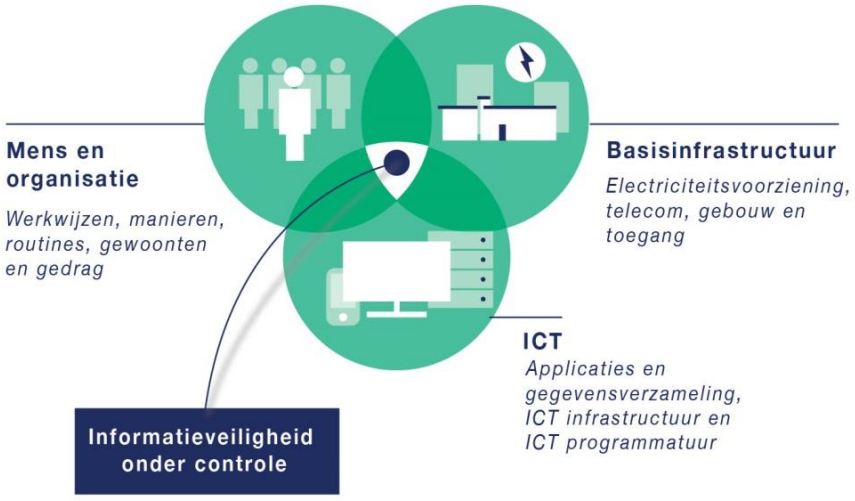
[17] Rekenkamer Den Haag (2014), Digitale Veiligheid.
[18] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid provincie Zuid-Holland, Deel 2 Beleid Informatieveiligheid 2014-2018.
[19] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging en Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid.
[20] Taskforce BID (2015), www.taskforcebid.nl.
[21] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging, p. 4 (oorspronkelijke bron: NEN (2005), NEN-ISO/IEC-27001/27002) en Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid.

Tabel 1 geeft per aspect van informatieveiligheid kenmerken die zorgen voor een hogere mate van informatieveiligheid, welke bedreigingen er zijn indien niet aan de kenmerken wordt voldaan, met enkele voorbeelden daarbij.

**Tabel 1 Informatieveiligheid: kenmerken, bedreigingen en voorbeelden**[22]

| | Aspecten | | |
|---|---|---|---|
| | **Vertrouwelijkheid** | **Integriteit** | **Beschikbaarheid** |
| **Kenmerk** | Exclusiviteit | 1. Correctheid<br>2. Volledigheid<br>3. Geldigheid<br>4. Authenticiteit<br>5. Onweerlegbaarheid | 1. Tijdigheid<br>2. Continuïteit |
| **Bedreiging** | Onthulling<br>Misbruik | 1. Wijziging<br>2. Verwijdering/Toevoeging<br>3. Veroudering<br>4. Vervalsing<br>5. Verloochening | 1. Vertraging<br>2. Uitval |
| **Voorbeeld** | Afluisteren van netwerk<br>Hacking | 1. Onrechtmatig wijzigen<br>2. Onrechtmatige verwijdering/Toevoeging<br>3. Gegevens niet up-to-date<br>4. Frauduleuze transactie<br>5. Ontkennen berichten te hebben verstuurd | 1. Overbelasting infrastructuur<br>2. Defect in infrastructuur |

Om de risico's op schending van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te verkleinen, zijn er drie verschillende aandachtsgebieden waarop kan worden gestuurd en waar maatregelen kunnen worden genomen (zie Figuur 3).[23]




**Figuur 3 Aandachtsgebieden van informatieveiligheid**

[22] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid. Deel 2 Beleid Informatieveiligheid 2014-2018, p.5
[23] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging, p. 5.

Tabel 2 geeft voor elk van de aandachtsgebieden een aantal voorbeelden weer van maatregelen die genomen kunnen worden om de verschillende aspecten van informatieveiligheid te verbeteren en te waarborgen.

**Tabel 2 Informatieveiligheid: aspecten- en aandachtsgebiedenmatrix met voorbeelden van maatregelen**

| | | Aspecten | | |
|---|---|---|---|---|
| | | **Vertrouwelijkheid** | **Integriteit** | **Beschikbaarheid** |
| **Aandachtsgebieden** | **Mens & Organisatie** | Creëren van bewustzijn<br>Procedures<br>(o.a. voorschriften voor wachtwoorden, uitloggen bij inactiviteit, etc.) | Creëren van bewustzijn<br>Procedures<br>(o.a. functiescheiding) | Creëren van bewustzijn<br>Procedures<br>(o.a. beleggen van verantwoordelijkheid voor bijv. back-up en uitwijksystemen) |
| | **Basis-infrastructuur ICT** | Toegangsbeveiliging gebouwen en ruimtes | Toegangsbeveiliging gebouwen en ruimtes | Noodstroomvoorziening |
| | | Autorisatierechten | Autorisatierechten<br>Logfiles bijhouden | Opstellen reserveapparatuur<br>Installeren antivirusprogramma |

## 1.3 Probleemstelling en onderzoeksvragen

De Randstedelijke Rekenkamer heeft voor dit onderzoek de volgende doel- en vraagstelling geformuleerd.

**Doelstelling**
Het doel van dit onderzoek is om inzichtelijk te maken of de informatieveiligheid van de provincie Flevoland voldoende is geborgd. Met de uitkomsten van het onderzoek wil de Rekenkamer handvatten bieden voor het verbeteren van de provinciale informatieveiligheid.

**Centrale vraagstelling**
Heeft de provincie Flevoland de informatieveiligheid voldoende geborgd?

Deze centrale vraagstelling wordt beantwoord aan de hand van een aantal onderzoeksvragen. Er zijn vier onderzoeksvragen, waarbij onderzoeksvraag 2 in drie delen is gesplitst.

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?
   a. Heeft de provincie een informatieveiligheidsbeleid opgesteld dat voldoet aan de daaraan te stellen eisen?
   b. Voert de provincie de benodigde[24] informatieveiligheidsmaatregelen uit?
   c. Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?[25]
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?

[24] 'Benodigd' betekent: 1. alle maatregelen uit de Interprovinciale Baseline Informatiebeveiliging die als generiek zijn gecategoriseerd. Deze maatregelen geven het basisniveau aan waaraan elke provincie moet voldoen; 2. alle aanvullende maatregelen die de individuele provincie zelf heeft geclassificeerd als 'nodig', op basis van risicoanalyses die de provincie zelf uitvoert.
[25] Deze deelvraag richt zich op het aspect vertrouwelijkheid binnen het aandachtsgebied ICT.

*Toelichting op de onderzoeksvragen*
In de Interprovinciale Baseline Informatiebeveiliging (IBI) en het Convenant Interprovinciale Regulering Informatieveiligheid, dat door alle provincies is ondertekend, staat het principe van verplichtende zelfregulering centraal. In een zelfregulerend besturingsmodel zijn vier kernaspecten te onderscheiden[26], waarop de onderzoeksvragen zijn gebaseerd. Deze worden hieronder kort toegelicht.

Het eerste kernaspect is **'sturing en verantwoordelijkheid'**. Naast de ICT infrastructuur horen zaken als toegangsbeveiliging, personeel en beleid tot het werkgebied van informatieveiligheid. Hierdoor kan informatieveiligheid niet de verantwoordelijkheid zijn van één directie of afdeling. Het is daarom van belang dat de provincie de sturing op en verantwoordelijkheid voor informatieveiligheid goed heeft verankerd.

Het tweede kernaspect is **'beleid en normenkader'**. De IBI is het vastgestelde basisnormenkader voor provincies, op basis waarvan de provincies een eigen informatieveiligheidsbeleid formuleren. Het tweede kernaspect is in drie onderzoeksvragen gesplitst en richt zich op de 'opzet' (2a), de 'uitvoering' (2b) en het 'resultaat' (2c) van het informatieveiligheidsbeleid. Vraag 2a gaat na of de provincie een informatieveiligheidsbeleid heeft geformuleerd, dat is gebaseerd op de IBI en daaruit volgende eisen. Vraag 2b richt zich vervolgens op de concretisering en uitvoering van de benodigde maatregelen, waarbij onderscheid wordt gemaakt tussen generieke en aanvullende maatregelen.[27] Dit zegt echter nog niets over de daadwerkelijke veiligheid van informatie: bieden de genomen maatregelen voldoende waarborgen tegen oneigenlijke toegang tot systemen en bestanden? Vraag 2c betreft daarom een toets op het resultaat van het informatieveiligheidsbeleid en de uitvoering van de maatregelen daarvoor. Hieruit zal blijken of aanpassingen in het informatieveiligheidsbeleid en/of maatregelen nodig zijn.

Het derde kernaspect is **'bewustwording, kennis en coördinatie'**. Door aandacht te besteden aan leren, stimuleren en kennisdelen wordt de bewustwording van bestuur, management en medewerkers met betrekking tot informatieveiligheid vergroot. Bij de derde onderzoeksvraag wordt nagegaan of de provincie voldoende aandacht besteedt aan bewustwording op het gebied van informatieveiligheid.

Het laatste kernaspect is **'verantwoording en toezicht'**. Dit kernaspect omvat het verankeren van informatieveiligheid in de reguliere planning en control cyclus, het periodiek uitvoeren van onafhankelijke onderzoeken en zelfevaluaties. De laatste onderzoeksvraag gaat na of de provincie het afleggen van verantwoording en het houden van toezicht op informatieveiligheid goed heeft geregeld.

Aangezien de onderzoeksvragen zijn gebaseerd op deze vier kernaspecten, steunt ook het beoordelingskader hier in belangrijke mate op. Het beoordelingskader komt aan de orde in paragraaf 1.6. In de volgende twee paragrafen gaan we achtereenvolgens in op de afbakening (paragraaf 1.4) en de wijze waarop de onderzoeksvragen zijn beantwoord (paragraaf 1.5).

[26] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid.
[27] Benodigde maatregelen zijn: 1. de generieke maatregelen uit de IBI, 2. aanvullende maatregelen die de provincie zelf heeft geclassificeerd als 'nodig' , op basis van een eigen risicoanalyse van de provincie.

## 1.4 Afbakening

In paragraaf 1.2 kwam naar voren dat informatieveiligheid een breed en complex begrip is. Informatieveiligheid heeft betrekking op het behouden van de aspecten vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarnaast kunnen maatregelen worden genomen op de aandachtsgebieden mens & organisatie, basisinfrastructuur en ICT, om de informatieveiligheid te vergroten.

Om het onderzoek in de juiste context te plaatsen zijn de volgende zaken, in het kader van de afbakening, van belang:

- Dit onderzoek richt zich op alle aspecten en aandachtsgebieden van informatieveiligheid. Uitzondering hierop vormt onderzoeksvraag 2c. Deze onderzoeksvraag, bestaande uit een toets van de daadwerkelijke informatieveiligheid, richt zich met name op het aspect van vertrouwelijkheid binnen het aandachtsgebied ICT.
- Het onderzoeksobject is de provincie. Hiermee wordt bedoeld dat aan de provincie verbonden partijen niet tot de reikwijdte van het onderzoek behoren. Vanzelfsprekend kan de provincie bij verbonden partijen wel een eindverantwoordelijkheid hebben, ook op het gebied van de informatieveiligheid.
- Het verzamelen van de gegevens waarop dit onderzoek is gebaseerd, heeft in de periode oktober 2015 – maart 2016 plaatsgevonden. De bevindingen geven derhalve de situatie van dat moment weer, tenzij anders wordt aangegeven.

## 1.5 Werkwijze

Deze paragraaf beschrijft op welke wijze de onderzoeksvragen zijn beantwoord. Het onderzoek is in de vier Randstedelijke provincies – Flevoland, Noord-Holland, Utrecht en Zuid-Holland – uitgevoerd. Voor het beantwoorden van de onderzoeksvragen zijn interviews gehouden met vertegenwoordigers van de ambtelijke organisatie en relevante documenten bestudeerd.

Voor de beantwoording van vraag 1 is nagegaan hoe GS en het management sturing geven aan informatieveiligheid. Daarnaast is gekeken of en in welke documenten verantwoordelijkheden, taken en bevoegdheden zijn toegekend aan de verschillende functies binnen de organisatie én of de verantwoordelijkheden in de praktijk zijn ingevuld. Voor vraag 2 is allereerst het beleidskader informatieveiligheid geanalyseerd (2a). Voor vraag 2b is onder andere nagegaan of de provincie de generieke maatregelen monitort, risicoanalyses heeft uitgevoerd en aanvullende maatregelen heeft geselecteerd. Voor het beantwoorden van onderzoeksvraag 2c zijn de technische waarborgen voor het beschermen van informatie voor toegang door onbevoegden door een externe partij onderzocht. Voor de beantwoording van vraag 3 is onderzocht welke activiteiten worden ondernomen om bewustwording van informatieveiligheid te bevorderen. Voor de beantwoording van vraag 4 is bekeken of informatieveiligheid is opgenomen in de P&C-documenten en of een onafhankelijke toets en zelfevaluatie zijn uitgevoerd.

## 1.6 Beoordelingskader

De Rekenkamer hanteert voor het maken van haar bevindingen een beoordelingskader (zie Tabel 3). Het beoordelingskader is gebaseerd op de volgende bronnen:

- Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
- Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid

De Rekenkamer heeft het beoordelingskader tijdens het opstellen van de onderzoeksopzet met ambtelijke vertegenwoordigers van de vier provincies besproken. Op basis van deze besprekingen is een aantal aanpassingen gedaan om beter aan te sluiten bij het vakgebied. Vervolgens is het beoordelingskader vastgesteld en naar de ambtelijke vertegenwoordigers gezonden.

**Tabel 3 Beoordelingskader**

| **Onderzoeksvragen en criteria** | | **Bron** |
|---|---|---|
| **VRAAG 1: Heeft de provincie de *sturing* op en de *verantwoordelijkheid* voor informatieveiligheid goed verankerd?** | | **Convenant IRI, sept. 2014** |
| Criterium 1a (H2, par. 2.1) | De provincie heeft informatieveiligheid als onderdeel van de portefeuille van een lid van GS belegd. | Convenant IRI (A.) |
| Criterium 1b (H2, par. 2.1) | Het bestuur (GS) en het management van de provincie zijn zich bewust van de risico's die de provincie loopt op het gebied van informatieveiligheid en hun rol en verantwoordelijkheid daarin. | Convenant IRI (A.) |
| Criterium 2 (H2, par. 2.2) | Er is een duidelijke verantwoordelijkheidsverdeling voor informatieveiligheid binnen de organisatie. | IBI A.6.1 |
| **VRAAG 2A: Heeft de provincie een informatieveiligheidsbeleid opgesteld dat voldoet aan de gestelde eisen?** | | |
| Criterium 3 (H3, par. 3.1) | De provincie heeft (1) een beleidskader informatieveiligheid, dat (2) is vastgesteld op directieniveau (bedrijfsvoering, provinciesecretaris), (3) maximaal 4 jaar oud is, (4) verwijst naar het informatiebeleidsplan en (5) de IBI als uitgangspunt heeft. | (1) IBI A.5.1.1<br>(2) IBI A.6.1.1<br>(3) IBI A.5.1.1<br>(4) IBI A.5.1.1<br>(5) Convenant IRI (B.) |
| **VRAAG 2B: Voert de provincie de benodigde informatieveiligheidsmaatregelen uit?** | | |
| Criterium 4 (H3, par. 3.2) | De provincie heeft de *generieke* maatregelen uit de IBI: (1) geconcretiseerd en (2) monitort de uitvoering ervan. | Convenant IRI (B.)<br>IBI, p. 15 en Bijlage B |
| Criterium 5a (H3, par. 3.2) | De provincie heeft risicoanalyses uitgevoerd en op basis daarvan afgewogen welke *aanvullende* maatregelen zij dient te nemen om de informatieveiligheid te verbeteren. | Convenant IRI (A.)<br>IBI |
| Criterium 5b (H3, par. 3.2) | De provincie controleert de uitvoering van de *aanvullende* maatregelen die zij, op basis van de risicoanalyse en -afweging, nodig vindt om te nemen. | IBI<br>Provinciaal beleid |
| **VRAAG 2C: Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?** | | |
| Criterium 6 (H3, par. 3.3) | De provincie doorstaat de specifieke test. | |
| **VRAAG 3: Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?** | | **Convenant IRI, sept. 2014** |
| Criterium 7a (H4) | Bestuur, management/medewerkers, ingehuurd personeel en externe gebruikers zijn bekendgemaakt met de verantwoordelijkheid die zij hebben in hun dagelijks handelen, op het gebied van informatieveiligheid. | IBI A.8.1.1<br>IBI A.8.1.3 |
| Criterium 7b (H4) | De provincie voert periodiek een bewustwordingsprogramma uit met als doel alle medewerkers te informeren, alsook het op peil houden van kennis en vaardigheden op het gebied van informatieveiligheid. | Convenant IRI, sept. 2014 |

| VRAAG 4: Heeft de provincie het afleggen van *verantwoording* en het houden van *toezicht* op informatieveiligheid goed geregeld? | | Convenant IRI, sept. 2014 |
|---|---|---|
| Criterium 8 (H5, par. 5.1) | De provincie heeft informatieveiligheid verankerd in de reguliere planning & control cyclus en geeft in het jaarverslag inzicht in de status van informatieveiligheid. | Convenant IRI, sept. 2014 |
| Criterium 9 (H5, par. 5.2) | De provincie laat periodiek een onafhankelijke toets uitvoeren op de informatieveiligheid. | Convenant IRI, sept. 2014 |
| Criterium 10 (H5, par. 5.3) | De provincie voert een zelfevaluatie uit. | Convenant IRI, sept. 2014 |

## 1.7 Leeswijzer

In Hoofdstuk 2 gaan we in op de wijze waarop de sturing op en verantwoordelijkheid voor informatieveiligheid binnen de provincie zijn verankerd. Vervolgens worden in Hoofdstuk 3 achtereenvolgens het informatieveiligheidsbeleid in opzet, uitvoering en het resultaat ervan beschouwd. Het centrale onderwerp van Hoofdstuk 4 is de aandacht voor bewustwording van informatieveiligheid. Hoofdstuk 5 gaat vervolgens in op de wijze waarop het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid is geregeld.

In dit hoofdstuk wordt nagegaan of de provincie de sturing op en verantwoordelijkheid voor informatieveiligheid goed heeft verankerd. Achtereenvolgens wordt ingegaan op de bestuurlijke verankering, het risicobewustzijn van bestuur en management en de verantwoordelijkheidsverdeling van informatieveiligheid binnen de provincie.

# | 2 | Sturing & Verantwoordelijkheid

In dit hoofdstuk wordt nagegaan of de provincie de sturing op en verantwoordelijkheid voor informatieveiligheid goed heeft verankerd. Achtereenvolgens wordt ingegaan op de bestuurlijke verankering, het risicobewustzijn van bestuur en management en de verantwoordelijkheidsverdeling van informatieveiligheid binnen de provincie.

## 2.1 Betrokkenheid van GS en management bij informatieveiligheid

**Criterium 1a**
*De provincie heeft informatieveiligheid als onderdeel van de portefeuille van een lid van GS belegd.*

Toelichting op het criterium
Bij informatieveiligheid gaat het niet alleen om ICT, maar ook om de basisinfrastructuur en mens & organisatie. Informatieveiligheid is daarom een breed en complex onderwerp, met een organisatiebreed karakter. Informatieveiligheid kan daarnaast een politiek-bestuurlijke impact hebben, wanneer gevoelige informatie bijvoorbeeld in verkeerde handen valt of informatie onjuist of niet beschikbaar is. Om deze redenen kan informatieveiligheid niet alleen de verantwoordelijkheid van de ambtelijke organisatie zijn, maar is het van belang dat informatieveiligheid bestuurlijk is belegd. Om de veiligheid van informatie te borgen, hebben de provincies in het Convenant Interprovinciale Regulering Informatieveiligheid daarom afgesproken dat zij informatieveiligheid bestuurlijk beleggen binnen de provincie. Aan de hand van dit criterium wordt nagegaan of informatieveiligheid onderdeel uitmaakt van de portefeuille van een lid van GS.

**Criterium 1b**
*Het bestuur (GS) en het management van de provincie zijn zich bewust van de risico's die de provincie loopt op het gebied van informatieveiligheid en hun rol en verantwoordelijkheid daarin.*

Toelichting op het criterium
Het bestuurlijk beleggen van informatieveiligheid alleen is niet voldoende. Het is ook van belang dat GS en het management[28] in de praktijk invulling geven aan deze verantwoordelijkheid. In het convenant hebben de provincies met elkaar afgesproken dat het bestuur en het management van iedere provincie zich bewust moeten zijn van de risico's die de provincie loopt en hun rol en verantwoordelijkheid daarin. GS en het management moeten daarom regelmatig worden geïnformeerd over de stand van zaken op het gebied van informatieveiligheid. Daarnaast is het van belang dat het management actief om informatie vraagt aan de ambtelijke organisatie en op cruciale onderdelen besluiten neemt ten aanzien van informatieveiligheid.

[28] Onder het management verstaat de Rekenkamer de bovenste twee lagen van het organogram: de algemene directie en de leidinggevenden van de organisatie-eenheden daaronder.

**Bevinding 1**

Informatieveiligheid is belegd bij de gedeputeerde met ICT in de portefeuille. De provincie heeft aangegeven dat GS van mening zijn dat informatieveiligheid operationeel een ambtelijke verantwoordelijkheid is. Daarom worden zij alleen op initiatief van de ambtelijke organisatie bij informatieveiligheid betrokken. Er zijn geen schriftelijke rapportages over informatieveiligheid aan GS.

De directie is in het algemeen goed betrokken bij informatieveiligheid. Zij heeft besluiten genomen over de aanpak van verschillende belangrijke zaken, zoals de risico's en speerpunten naar aanleiding van de monitor zelfevaluatie en het bewustwordingstraject voor de organisatie. Het bewustzijn van rollen en verantwoordelijkheden in de managementlagen onder de directie behoeft wel verbetering. Bij veel systemen is het eigenaarschap nog niet belegd en bestaat terughoudendheid om het eigenaarschap (en daarmee de verantwoordelijkheid) te aanvaarden. De naleving van richtlijnen over bijvoorbeeld Clean Desk Policy wordt niet gestimuleerd.

Toelichting op de bevinding

De bevinding wordt toegelicht in de paragrafen 2.1.1 tot en met 2.1.3.

### *2.1.1 Betrokkenheid van GS bij informatieveiligheid*

Het Convenant Interprovinciale Regulering Informatieveiligheid is in de vergadering van GS van 16 december 2014 behandeld en vastgesteld.[29] Het onderwerp informatieveiligheid is belegd bij de gedeputeerde met ICT in de portefeuille. Informatieveiligheid heeft vanuit GS voornamelijk een ICT-perspectief gekregen en wordt minder gezien als een vraagstuk op het gebied van bijvoorbeeld mens en organisatie, omdat dit perspectief in een andere portefeuille is ondergebracht.[30] GS nemen het standpunt in dat bedrijfsvoeringonderwerpen als informatieveiligheid operationeel een ambtelijke verantwoordelijkheid zijn, tenzij deze door de ambtelijke organisatie worden geagendeerd.[31] GS ontvangen geen schriftelijke rapportages over informatieveiligheid.[32]

GS vragen niet proactief om de stand van zaken op het gebied van informatieveiligheid.[33] Het portefeuillehouderoverleg van december 2015 vormt hierop een uitzondering.[34] Toen is op verzoek van de gedeputeerde een presentatie gegeven over informatieveiligheid. Een bijgestelde versie van deze presentatie is daarna in een GS-vergadering gegeven.[35] De bijgestelde versie gaat over de onderdelen waar het convenant uit bestaat en bevat deels een verantwoording over hoe de provincie presteert op de verschillende onderdelen.[36]

[29] Provincie Flevoland (2014), Concept Besluitenlijst vergadering GS, agendapunt 21; Nota Besluitvorming GS instemmen met convenant informatiebeveiliging..
[30] Provincie Flevoland, ambtelijke interviews, 8 december 2015.
[31] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[32] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[33] Provincie Flevoland, ambtelijk interview, 11 januari 2016.
[34] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[35] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[36] Provincie Flevoland (2015), Presentatie Informatieveiligheid voor GS.

### *2.1.2 Betrokkenheid van directie bij informatieveiligheid*

In het informatieveiligheidsbeleidsplan van de provincie is vastgelegd dat de directie verantwoordelijk is voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van het informatieveiligheidsbeleid.[37] Er staat ook in dat de directie een inschatting maakt van het belang en de risico's van de verschillende delen van de informatievoorziening voor de organisatie en welke risico's wel en niet acceptabel zijn.[38]

In de praktijk wordt vanuit de directie invulling gegeven aan deze eindverantwoordelijkheid doordat zij over belangrijke zaken beslissingen neemt. Een belangrijke rol hierbij is weggelegd voor de adviseur informatieveiligheid, die ook de rol van Security Officer heeft. De adviseur informatieveiligheid voert de eindcoördinatie van informatieveiligheid, zowel op het gebied van ICT, mens en organisatie als fysieke toegang en is verantwoordelijk voor het informeren van de directie over informatieveiligheid. Het afdelingshoofd Services en Middelen (SenM) en het afdelingshoofd Managementondersteuning (MO) bepalen samen met de adviseur informatieveiligheid welke zaken worden voorgelegd aan de directie.[39]

In de periode 2014-2015 heeft de directie over vier zaken een besluit genomen.[40]

1. De 15 risico's en speerpunten voor informatieveiligheid, naar aanleiding van de monitor zelfevaluatie 2014
2. Aanbevelingen naar aanleiding van de penetratietest
3. Aanbevelingen naar aanleiding van de monitor zelfevaluatie 2015
4. Start van het bewustwordingstraject

Er is eenmalig een halfjaarlijkse rapportage aan de directie over de voortgang en status van informatieveiligheid gestuurd. Verder rapporteert de adviseur informatieveiligheid tweewekelijks schriftelijk over de voortgang van informatieveiligheid. Deze rapportages worden door de directie gebruikt.[41]

### *2.1.3 Betrokkenheid van management bij informatieveiligheid*

Onder management wordt hier verstaan de managementlagen onder de directie. Het betreft de afdelingshoofden, adjuncthoofden en bureauhoofden.

**Managementberaad**

De directie en de afdelingsmanagers vormen samen het managementberaad. Het managementberaad adviseert de directie en toetst bouwstenen-notities die vanuit de organisatie aan de directie worden voorgelegd. Het managementberaad neemt geen besluiten, dit is aan de directie.[42]

In interviews is aangegeven dat het managementberaad zich bewust is van informatieveiligheid. De adviseur Informatieveiligheid heeft drie keer met het managementberaad de informatieveiligheid binnen de provincie besproken. Het gaat dan onder meer om de vijftien punten die uit de monitor zelfevaluatie zijn gekomen. Ook heeft het managementberaad meegewerkt aan een penetratietest en zijn de aanbevelingen opgepakt.[43]

---

[37] In het beleidsplan wordt de term informatiebeveiligingsbeleid gebruikt. De Rekenkamer hanteert de term informatieveiligheidsbeleid, omdat deze meer recht doet aan de breedte van het onderwerp (zie ook paragraaf 1.2).
[38] Provincie Flevoland (2015), Informatiebeveiligingsbeleid provincie Flevoland, p. 7.
[39] Provincie Flevoland, ambtelijke interviews, 8 december 2015.
[40] Provincie Flevoland, ambtelijk interview, 11 januari 2016; aanvullende informatie, 26 april 2016..
[41] Provincie Flevoland, ambtelijk interview, 11 januari 2016, aanvullende informatie, 26 april 2016..
[42] Provincie Flevoland, ambtelijk interview, 11 januari 2016.
[43] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 11 januari 2016. NB De genoemde penetratietest betreft de test die in 2015 in opdracht van de provincie zelf is uitgevoerd; dus niet de penetratietest die de Randstedelijke Rekenkamer heeft laten uitvoeren in het kader van dit onderzoek informatieveiligheid.

**Rol management in de praktijk**

Vanuit verschillende bronnen wordt gesignaleerd dat de betrokkenheid van het management bij informatieveiligheid wel beter kan. Een extern bureau constateert in oktober 2015 dat de kennis, prioritering, verantwoordelijkheden en risico-inschatting in relatie tot informatieveiligheid divers is bij de stakeholders.[44] Deze uitspraak gaat over zowel GS als het gehele management (dus ook directie) en is daarmee nog vrij algemeen. Een memo van februari 2016 van de afdeling MO (opgesteld door de adviseur Informatieveiligheid) aan het Intaketeam is specifieker. In dit memo wordt gesteld dat de coördinatie van de informatieveiligheid binnen de afdelingen niet werkt. Zo wordt de Clean Desk Policy nauwelijks nageleefd en bewustwording van medewerkers van het belang van informatieveiligheid niet gestimuleerd; in elk geval wordt er niet over gerapporteerd.[45] Ook richtlijnen die zijn voortgekomen uit het project Slim Digitaal Samenwerken, worden niet goed nageleefd.[46]

In een aantal ambtelijk interviews is een vergelijkbaar signaal afgegeven. Het bewustzijn van het belang van informatieveiligheid verschilt per manager. Vanuit het management is niet automatisch aandacht voor informatieveiligheid, al heeft de aanstelling van een adviseur informatieveiligheid het bewustzijn wel versterkt.[47]

De provincie vindt het voor een goede informatieveiligheid van belang dat het eigenaarschap van systemen, gegevens, documenten en processen goed belegd en gedefinieerd is. In verschillende interviews en documenten is aangegeven dat hier nog een uitdaging ligt voor de provincie. De IT-Raad (die namens de directie zorgt voor de dagelijkse aansturing van informatieveiligheid. Zie verder paragraaf 2.2.1) heeft eind 2015 een document vastgesteld waarin per systeem een eigenaar is bepaald. In de praktijk blijkt het eigenaarschap alleen helder en bekend te zijn bij de grote, organisatiebrede systemen (zoals het financiële systeem). Voor vele andere systemen moet nog daadwerkelijk een eigenaar worden benoemd. Het lastige daarbij is dat veel medewerkers terughoudend zijn met het op zich nemen van het systeemeigenaarschap, vanwege het werk en de verantwoordelijkheid die daaruit volgen.[48] Voor gegevens, documenten en processen zijn nog geen eigenaren benoemd[49]

**Meldplicht datalekken**

Op 1 januari 2016 is de Meldplicht datalekken in werking getreden. Deze meldplicht is onderdeel van de Wet Bescherming Persoonsgegevens.[50] Het gaat bij een datalek om toegang tot, of vernietiging, wijziging of vrijkomen van persoonsgegevens, zonder dat dit de bedoeling is van de organisatie. Voorbeelden van een datalek zijn een kwijtgeraakte USB-stick met persoonsgegevens of een inbraak in een databestand door een hacker.[51] De meldplicht houdt in dat organisaties een datalek binnen 72 uur moeten melden bij de Autoriteit Persoonsgegevens.[52] In sommige gevallen moet het datalek ook gemeld worden aan de betrokkenen (degenen van wie de persoonsgegevens zijn gelekt). De meldplicht geldt voor alle organisaties die persoonsgegevens verwerken. Indien het datalek niet op tijd wordt gemeld, riskeert de organisatie een boete die kan oplopen tot 820.000 euro per overtreding.[53]

[44] Provincie Flevoland & BDO (2015), Onderzoek Informatieveiligheid, rapportage onderzoek voortgang project ' Zelfregulering Informatieveiligheid', p. 9.
[45] Provincie Flevoland (2016), Voorstel verbeterde invulling rol adviseur Informatieveiligheid, p. 2.
[46] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[47] Provincie Flevoland, ambtelijke interviews, 8 december 2015.
[48] Provincie Flevoland, ambtelijke interviews, 14 december 2015 en 11 februari 2016.
[49] Provincie Flevoland, aanvullende informatie 26 april 2016.
[50] Eerste Kamer der Staten-Generaal (2016), www.eerstekamer.nl.
[51] Autoriteit Persoonsgegevens (2015), www.autoriteitpersoonsgegevens.nl.
[52] Voorheen het College Bescherming Persoonsgegevens.
[53] Justitia.nl (2015), www. justitia.nl.

Door de directie is aangegeven dat de invoering van de meldplicht datalekken in de provincie projectmatig wordt opgepakt. De teamleider van het cluster informatiemanagement is opdrachtgever van het project. Het projectplan is geschreven door de adviseur Informatieveiligheid. Uit het projectplan blijkt een duidelijke behoefte aan verbetering van de beveiliging van persoonsgegevens. Die was vóór de invoering van de meldplicht al onvoldoende om aan de toenmalig geldende regelgeving (Wet Bescherming Persoonsgegevens) te voldoen. [54] Een eerste stap die volgens de provincie nodig is, is het maken van een inventarisatie van alle systemen. Duidelijk dient te worden in welke van de ruim 100 systemen van de provincie persoonsgegevens zijn opgenomen, inclusief de bijbehorende archiverings- en beveiligingsmaatregelen. Uit capaciteitsoverwegingen is aan de directie voorgesteld eerst de vijf belangrijkste systemen door te lichten en daar zeven maanden (tot medio 2016) voor uit te trekken.[55] Het idee is verder om het proces voor de meldplicht datalekken structureel in te richten in het kader van de Meerjaren Aanpak Bedrijfsvoering (MAB) van de provincie. Voorlopig is afgesproken dat beveiligingsincidenten worden gemeld aan de adviseur informatieveiligheid. Hij beoordeelt of in geval van een incident sprake is van een meldplicht.[56]

## 2.2 Verantwoordelijkheidsverdeling binnen de organisatie

### Criterium 2

*Er is een duidelijke verantwoordelijkheidsverdeling voor informatieveiligheid binnen de organisatie.*

Toelichting op het criterium

Om informatieveiligheid organisatorisch goed te verankeren, is het van belang dat er een duidelijke verantwoordelijkheidsverdeling is binnen de organisatie. Zo beschrijft de IBI dat alle verantwoordelijkheden, taken en bevoegdheden voor informatieveiligheid expliciet moeten zijn toegekend aan bestaande functies binnen de organisatie en dat de eindcoördinatie op één plek en in één functie binnen de organisatie is belegd. Omdat informatieveiligheid betrekking heeft op verschillende aandachtsgebieden (mens & organisatie, basisinfrastructuur, ICT), is het daarnaast van belang dat meerdere disciplines betrokken zijn bij informatieveiligheid. Van belang is ook dat de verantwoordelijkheden goed zijn verdeeld, er geen overlap is of gaten vallen waarover onduidelijkheid kan ontstaan en dat de uitvoerende/operationele en de controlerende rol van elkaar gescheiden zijn.

[54] Provincie Flevoland (2015), Projectplan Beveiliging Persoonsgegevens, p. 3.
[55] Provincie Flevoland (2016), Archivering en beveiliging persoonsgegevens, memo van afdeling MO aan directie; ambtelijk interview, 7 maart 2016.
[56] Provincie Flevoland, aanvullende informatie 26 april 2016.

**Bevinding 2**

In het informatieveiligheidsbeleid worden alle verantwoordelijkheden, taken en bevoegdheden duidelijk toegekend aan bestaande functies of doelgroepen. De directie is eindverantwoordelijk voor informatieveiligheid, de IT-raad heeft de verantwoordelijkheid van de dagelijkse aansturing en de eindcoördinatie is belegd bij de adviseur informatieveiligheid, die functioneel – namens de IT-raad – verantwoordelijk is voor de coördinatie. Daarnaast worden diverse andere doelgroepen benoemd die bepaalde verantwoordelijkheden hebben en is de opzet van het eigenaarschap van processen en systemen aangegeven.

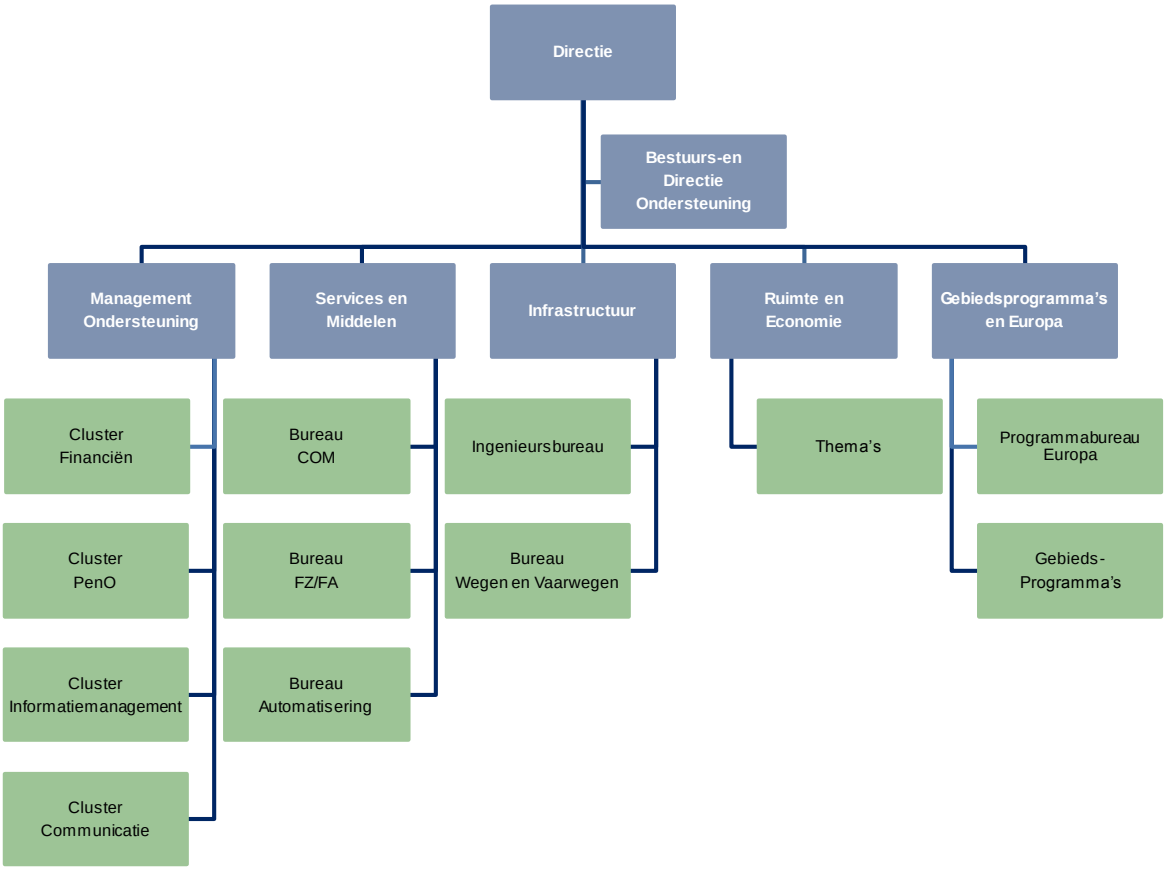
Door de gekozen verdeling van verantwoordelijkheden en de invulling van de verschillende rollen zijn de beleids-/adviesrol en de controlerende rol in de praktijk niet van elkaar gescheiden. Deels geldt dit ook voor de uitvoerende en de controlerende rol.

De provincie heeft een aantal waarborgen ingesteld ten behoeve van de onafhankelijkheid van de controlerende rol, maar in de praktijk leiden deze waarborgen niet tot volledige onafhankelijkheid.

Toelichting op de bevinding

In deze paragraaf worden de verantwoordelijkheden op het gebied van informatieveiligheid binnen de provincie toegelicht. In onderstaande subparagrafen komen achtereenvolgens de eindverantwoordelijkheid en coördinatie, andere verantwoordelijken en eigenaarschap, interdisciplinariteit en als laatste rolscheiding en onafhankelijkheid aan bod.

Voorafgaand daaraan wordt het organogram weergegeven, waaraan in de subparagrafen wordt gerefereerd.




**Figuur 4 Organogram provincie Flevoland**[57]

### *2.2.1 Eindverantwoordelijkheid en coördinatie*

In de eindverantwoordelijkheid en de coördinatie zijn er drie sleutelspelers. De directie is de eerste sleutelspeler, aangezien het informatieveiligheidsbeleid aangeeft dat de directie eindverantwoordelijk is voor informatieveiligheid. Daarbij is gespecificeerd dat de directie van de provincie verantwoordelijk is "*voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van het informatiebeveiligingsbeleid. De directie maakt een inschatting van het belang en de risico's van verschillende delen van de informatievoorziening voor de organisatie. De directie bepaalt welke risico's acceptabel en niet acceptabel zijn. De directie is eindverantwoordelijke.*" Ze draagt daarmee integrale verantwoordelijkheid en de verantwoordelijkheid voor kaderstelling en implementatie.[58] Naast deze beschrijving in het informatieveiligheidsbeleid, blijkt de eindverantwoordelijkheid van de directie ook uit diverse interviews met de ambtelijke organisatie.[59]

De tweede sleutelspeler is de IT-raad. Hierover staat in het informatieveiligheidsbeleid beschreven dat: "*de IT-raad namens de directie op dagelijkse basis invulling geeft aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.*"[60] Daarnaast is de IT-raad volgens het informatieveiligheidsbeleid opdrachtgever van periodieke controles op de kwaliteit van informatieveiligheid door bijvoorbeeld de accountant en onafhankelijke externen (zoals ethical hackers en penetratietesten).[61] Bevindingen

[57] Provincie Flevoland (2016), www.flevoland.nl.
[58] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.7, 10 en 13.
[59] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 14 december 2015.
[60] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.10 en 14.
[61] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.17, 18 en 44.

van deze onderzoeken en controles worden gerapporteerd aan de IT-raad en de directie.[62] De leden van de IT-raad zijn de directeur bedrijfsvoering (voorzitter), de afdelingshoofden Services en Middelen (SenM), Managementondersteuning (MO) en Ruimte en Economie, het bureauhoofd (a.i.) bureau Automatisering en de teamleider van het cluster Informatiemanagement.[63]

Als derde sleutelspeler wordt in het informatieveiligheidsbeleid de adviseur informatieveiligheid genoemd. De adviseur informatieveiligheid is geen lid van de IT-raad, maar is namens de IT-raad (functioneel) verantwoordelijk voor en geeft namens de IT-raad functionele sturing – vanuit de inhoud, niet vanuit de hiërarchie – aan de realisatie van de kaderstelling en zorgt voor toetsing van en advisering over maatregelen.[64] De taken met betrekking tot informatieveiligheid die hieruit voortkomen zijn door de IT-raad belegd bij de adviseur informatieveiligheid. De adviseur informatieveiligheid bevordert en adviseert verder gevraagd en ongevraagd over informatieveiligheid en rapporteert eens per kwartaal aan de IT-raad over de stand van zaken.[65] Daarnaast zorgt de adviseur informatieveiligheid ervoor dat alle bedrijfskritische systemen worden voorzien van een classificatie op risiconiveau en de centrale vastlegging daarvan.[66] Dat de functie van adviseur informatieveiligheid in de praktijk ook zo wordt ingevuld, blijkt uit de gehouden interviews met diverse vertegenwoordigers van de ambtelijke organisatie. Zij stellen dat de coördinatie voor informatieveiligheid bij de adviseur informatieveiligheid ligt, zowel op de aandachtsgebieden mens & organisatie, infrastructuur en ICT alsook op de aspecten vertrouwelijkheid, integriteit en beschikbaarheid.[67] Verder geven de vertegenwoordigers van de ambtelijke organisatie aan dat de adviseur informatieveiligheid: “een spilfunctie heeft in het informeren van de directie over informatieveiligheid, dat hij de lijn vasthoudt, bewaakt en zorgt dat de relevante spelers worden betrokken”[68] en dat hij “de spin in het web is op het gebied van informatieveiligheid door het ontwikkelen van beleid, stellen van kaders, monitoring, de aandacht voor bewustwording en controle.”[69]

### *2.2.2 Overige verantwoordelijken en eigenaarschap*

Naast de eindverantwoordelijkheid en de coördinatie wordt er in het informatieveiligheidsbeleid nog een aantal andere doelgroepen genoemd die een verantwoordelijkheid hebben voor informatieveiligheid (zie Tabel 4).[70]

[62] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.17-18.
[63] Provincie Flevoland, ambtelijke interviews, 8 december 2015, 11 januari 2016 en 11 februari 2016.
[64] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.10 en 13.
[65] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.13.
[66] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.23.
[67] Provincie Flevoland, ambtelijke interviews, 8 december 2015, 14 december 2015 en 11 januari 2016.
[68] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[69] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[70] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.10-11.

**Tabel 4 Doelgroepen en relevantie voor informatieveiligheid**

| | Doelgroep | Relevantie voor informatieveiligheid |
|---|---|---|
| 1 | Hoofd afdeling (proceseigenaren) | Sturing op informatieveiligheid en controle op naleving |
| 2 | Hoofd afdeling (systeemeigenaren) | Classificatie[71] van informatie<br>Verantwoordelijkheid voor de beschermingseisen van informatie |
| 3 | SenM/Automatisering | Technische beveiliging |
| 4 | SenM/Facilitaire zaken | Fysieke toegangsbeveiliging<br>Inkoop & Aanbesteding |
| 5 | MO/P&O | Arbeidsvoorwaardelijke zaken |
| 6 | Medewerkers | Gedrag en naleving |
| 7 | Beleidmakers | Planvorming binnen informatiebeveiligingskaders |
| 8 | Projectleiders | Uitvoering binnen informatiebeveiligingskaders |
| 9 | BDO / Juridische zaken | Juridische zaken |
| 10 | Accountant en ethical hackers | Onafhankelijke toetsing |
| 11 | Leveranciers en ketenpartners | Compliance |

Hieronder worden de eerste zes doelgroepen nader toegelicht.

Ad 1 en 2)
Hierbij gaat het om de rol van afdelingshoofden als proceseigenaar en systeemeigenaar. Voor het goed functioneren van de organisatie die informatieveiligheid voor elkaar moet krijgen is het goed definiëren en beleggen van eigenaarschap van processen, systemen, gegevens en documenten van belang. Een proces-, systeem-, gegevens- en/of documenteigenaar moet namelijk onder andere zorgen voor informatieveiligheidsmaatregelen en het nemen van de verantwoordelijkheid daarvoor.[72]

Begin 2015 is de provincie gestart met het opstellen van de definities van proces-, systeem-, gegevens- en documenteigenaar. Op 6 oktober 2015 zijn deze definities door de IT-raad vastgesteld.[73] Ook is een lijst toegevoegd met alle systemen die in gebruik zijn binnen de provincie. Voor de grotere systemen, die door de hele ambtelijke organisatie worden gebruikt (zoals het financiële systeem of het documentmanagementsysteem) is bekend wie de systeemeigenaren zijn.

Naast het beleggen van het proces- en systeemeigenaarschap is één van de uitgangspunten van het informatieveiligheidsbeleid dat: "*alle informatie en informatiesystemen van kritiek en vitaal belang zijn voor de organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij de hoofden van de afdelingen, behoudens die verantwoordelijkheden welke zijn neergelegd bij SenM en MO.*"[74] Hiermee hebben de afdelingshoofden integrale verantwoordelijkheid voor informatieveiligheid en is een speciale rol toegekend aan de afdelingen SenM en MO (zie hiervoor ad 3, 4 en 5).

[71] Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is.
[72] Provincie Flevoland (2015), Notitie Definities systeem-, gegevens- en documenteigenaar aan IT-raad; ambtelijk interview 11 februari 2016.
[73] Provincie Flevoland (2015), Oplegmemo systeemeigenaarschap aan IT-raad; Notitie Definities systeem-, gegevens- en documenteigenaar aan IT-raad.
[74] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.7.

Ten slotte geeft het informatieveiligheidsbeleid aan dat "*Het hoofd van de afdeling bevordert dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen."* en dat *"De afspraken met interne en externe medewerkers hierover worden vastgelegd in het Individueel Werk Plan (IWP) respectievelijk de opdrachtbrief*."[75] Hiermee is aan de afdelingshoofden ook een specifieke verantwoordelijkheid toebedeeld voor bewustwording van medewerkers op het gebied van informatieveiligheid.

De wijze waarop de afdelingshoofden invulling geven aan hun verantwoordelijkheden is beschreven in paragraaf 2.1.3.

Ad 3, 4 en 5)
De afdelingen/teams SenM/Automatisering, SenM/Facilitaire Zaken en MO/P&O zijn ondersteunende afdelingen en hebben vanuit hun vakgebied een specifieke rol bij informatieveiligheid. Het bureau Automatisering is verantwoordelijk voor het aandachtsgebied ICT, het bureau Facilitaire Zaken voor het aandachtsgebied basisinfrastructuur en het cluster P&O voor het aandachtsgebied mens & organisatie.

Ad 6)
Hierbij gaat het om het gedrag van en de naleving door medewerkers op het gebied van informatieveiligheid. Bewustwording speelt hierbij een belangrijke rol. Dit onderwerp wordt toegelicht in paragraaf 4.1.1.

### *2.2.3 Rolscheiding en onafhankelijkheid*

Zoals eerder genoemd is de coördinatie van informatieveiligheid belegd bij de adviseur informatieveiligheid, binnen het cluster Informatiemanagement van de afdeling MO.[76] De adviseur informatieveiligheid heeft in de praktijk de rollen van beleid maken voor en adviseren over informatieveiligheid en de controle op de uitvoering van informatieveiligheidsmaatregelen. De uitvoering van onder andere de generieke maatregelen[77] ligt voor een deel bij de afdeling SenM ( bureaus Automatisering en Facilitaire Zaken), voor een deel bij de afdeling MO (cluster P&O) en voor een deel bij andere afdelingen (vanuit de rol van proces-/systeemeigenaar). Hierbij heeft de adviseur informatieveiligheid een coördinerende rol.[78] Daarnaast heeft de adviseur informatieveiligheid een rol bij de speerpunten die jaarlijks in het Jaarplan Informatisering en Automatisering (I&A) worden opgenomen. De uitvoering van deze speerpunten wordt vanuit het cluster Informatiemanagement projectmatig opgepakt door de adviseur informatieveiligheid. Hierbij heeft de adviseur informatieveiligheid een aanjaagfunctie totdat een project wordt overgedragen aan de proces-/systeemeigenaren in de lijn.[79]

Door deze verdeling van verantwoordelijkheden en rolneming zijn de beleids-/adviesrol en de controlerende rol in de praktijk niet van elkaar gescheiden.[80] Dit geldt deels ook voor de uitvoerende en de controlerende rol.

Daarnaast vindt de controle op de uitvoering van maatregelen op het gebied van informatieveiligheid plaats door de adviseur informatieveiligheid, vanuit het cluster Informatiemanagement binnen de afdeling MO. Een deel van de uitvoering van informatieveiligheidsmaatregelen en verantwoordelijkheden voor informatieveiligheid is ook binnen deze afdeling belegd, namelijk in de clusters P&O en Financiën. Dit betekent dat de controlerende rol en

[75] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.25.
[76] Provincie Flevoland, ambtelijke interviews 8 december 2015.
[77] In de IBI zijn de eisen ten aanzien van informatieveiligheid geformuleerd. Hierin wordt onderscheid gemaakt tussen generieke en aanvullende maatregelen. Generieke maatregelen zijn maatregelen die het basisniveau van beschikbaarheid, integriteit of vertrouwelijkheid aangeven. Met andere woorden, deze maatregelen dienen áltijd te worden genomen.
[78] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[79] Provincie Flevoland, ambtelijk interview, 14 december 2015.
[80] Provincie Flevoland, ambtelijk interview, 11 februari 2016.

de uitvoerende rol – evenals een deel van de verantwoordelijkheden – zich binnen dezelfde afdeling bevinden. Hierdoor kan de onafhankelijkheid van de controlerende rol in het gedrang komen.

De provincie heeft een aantal waarborgen ten behoeve van de onafhankelijkheid van de controlerende rol:

- Eén van de uitgangspunten van het informatieveiligheidsbeleid is als volgt geformuleerd: "*De adviseur informatieveiligheid ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover. Deze onafhankelijke positie waarborgt een objectieve toetsing van genomen besluiten en onderzoeksresultaten. Dit betekent bijvoorbeeld dat de betreffende documenten door zijn leidinggevenden "voor gezien" in plaats van "voor akkoord" getekend worden.*"[81]

De adviseur informatieveiligheid heeft geen mandaat en werkt op basis van het draagvlak dat hij creëert. De directie besluit uiteindelijk.[82] Dit betekent bijvoorbeeld dat de adviseur informatieveiligheid wel het controleplan informatieveiligheid opstelt, maar dat daar goedkeuring van de directie op wordt gegeven.[83]
De rol van adviseur informatieveiligheid is vormgegeven naar analogie van de verbijzonderde interne controle. Dit betekent dat de adviseur informatieveiligheid in de controlerende rol de bevoegdheid heeft om direct aan de directie te rapporteren.[84]

Overigens is door een aantal vertegenwoordigers van de ambtelijke organisatie desgevraagd aangegeven dat de functie van adviseur informatieveiligheid op de andere taken dan de controlerende taak niet onafhankelijk is en dat de onafhankelijkheid – ook op de controlerende taak – mede wordt bepaald door de wijze waarop invulling wordt gegeven aan de functie.[85] Daarnaast is een van de aanbevelingen uit een onafhankelijk onderzoek van een derde partij om de interne controle op de werking van de beheersmaatregelen door een onafhankelijke functionaris te laten uitvoeren.[86]

Als onderdeel van de afdeling Bestuurs- en Directieondersteuning (BDO) heeft de concerncontroller wel een onafhankelijke positie voor een aantal activiteiten, maar door vertegenwoordigers van de ambtelijke organisatie is aangegeven dat de concerncontroller geen expliciete rol ten aanzien van informatieveiligheid heeft.[87]

[81] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.8.
[82] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[83] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[84] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[85] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 14 december 2015.
[86] Provincie Flevoland en BDO IT Audit & Security (2015), Onderzoek informatieveiligheid, Rapportage onderzoek voortgang project 'Zelfregulering Informatieveiligheid.
[87] Provincie Flevoland (2015), Afdelingsplan BDO 2015; ambtelijke interviews 8 december 2015.

# | 3 | Informatieveiligheidsbeleid

Provincies hebben in 2010 de Interprovinciale Baseline Informatiebeveiliging (IBI) opgesteld. Dit is het basisnormenkader voor provincies, dat aangeeft wat het basisniveau is van informatieveiligheid waaraan de provincies minimaal willen voldoen. In dit hoofdstuk wordt nagegaan of het informatieveiligheidsbeleid van de provincie in opzet, uitvoering én in resultaat adequaat is.

Paragraaf 3.1 gaat na of de provincie een in opzet adequaat informatieveiligheidsbeleid heeft geformuleerd, dat de IBI als uitgangspunt heeft. Paragraaf 3.2 richt zich op de uitvoering van het beleid en de benodigde informatieveiligheidsmaatregelen. Hierbij wordt onderscheid gemaakt tussen generieke maatregelen die voor elke provincie gelden en aanvullende maatregelen, die de provincie heeft geselecteerd op basis van de eigen risicoanalyse en –afweging. Paragraaf 3.3 tot slot, gaat in op de vraag of de genomen maatregelen voldoende waarborgen bieden tegen oneigenlijke toegang tot systemen en bestanden. Deze paragraaf betreft een technische test die toetst of een specifiek deel van de informatieveiligheid in de praktijk ook daadwerkelijk op orde is.

## 3.1 Informatieveiligheidsbeleid in opzet

**Criterium 3**

*De provincie heeft (1) een beleidskader informatieveiligheid, dat (2) is vastgesteld op directieniveau, (3) maximaal 4 jaar oud is, (4) verwijst naar het informatiebeleidsplan en (5) de IBI als uitgangspunt heeft.*

Toelichting op het criterium

Dit criterium is heel feitelijk en komt direct voort uit het convenant (zie paragraaf 1.1) en de IBI. Het is van belang dat het informatieveiligheidsbeleid op directieniveau is vastgesteld, zodat het management zich bewust is van zijn verantwoordelijkheid en sturing kan geven aan informatieveiligheid. Informatieveiligheid kan niet los worden gezien van het totale informatiebeleid; vandaar dat het beleidskader informatieveiligheid dient te verwijzen naar het informatiebeleidsplan van de provincie. In de IBI en de daaraan ten grondslag liggende ISO 27001 (2005) norm zijn de eisen ten aanzien van de informatieveiligheid geformuleerd. Het is daarom van belang dat het informatieveiligheidsbeleid van de provincie de IBI als uitgangspunt heeft.

**Bevinding 3**

Het Informatieveiligheidsbeleid van de provincie is in mei 2015 vastgesteld door de directie. De IBI wordt expliciet als basis en uitgangspunt voor het informatieveiligheidsbeleid genomen. Aan alle elf categorieën van de IBI is een hoofdstuk gewijd met beheersmaatregelen, doelstellingen en risico's.

Toelichting op de bevinding

*Informatiebeleidsplan*

Op 12 december 2012 heeft de directie de Nota Informatie in Beweging vastgesteld.[88] Deze nota bevat een compacte beschrijving van de positie waarin de provinciale organisatie zich op het gebied van informatievoorziening bevindt en schetst de belangrijkste opgaven op dit terrein. Op basis van deze nota heeft de afdeling MO het project Kaderstelling Informatieveiligheid 2014 opgestart. Het doel van dit project is een bijdrage te leveren aan de bedrijfsdoelstelling "*het op orde hebben van de basis van de ondersteunende afdelingen*"[89], onder andere door kaders te stellen voor het informatieveiligheidsbeleid en door aansluitend het informatiebeleidsplan op te stellen. De start van het opstellen van het informatiebeleidsplan was voorzien in 2015.[90] Echter, door andere prioriteiten is het informatiebeleidsplan nog niet gereed.[91] Het informatieveiligheidsbeleid heeft dus geen verwijzing naar het informatiebeleidsplan.

*Informatieveiligheidsbeleid*

Op 19 november 2014 – nagenoeg gelijktijdig met de ondertekening van het convenant door het IPO – heeft de directie het projectplan 'Implementeren proces verplichtende zelfregulering informatieveiligheid' vastgesteld.[92] De uitdaging voor dit project is als volgt geformuleerd: "*Voor 1 april 2015 het proces van de verplichte zelfregulering Informatieveiligheid implementeren zodat de provincie Flevoland voldoet aan de afspraken in de Interprovinciale Regulering Informatieveiligheid.*"[93] In het projectplan wordt aangegeven dat het vaststellen van een vierjaarlijks beleidskader Informatieveiligheid wordt doorgeschoven naar 2015. De reden hiervan is dat de verkiezingen dan zijn geweest en dat informatieveiligheid expliciet kan worden opgenomen in een nieuw collegeuitvoeringsprogramma 2015-2019.[94]

Het Informatieveiligheidsbeleid is op 20 mei 2015 vastgesteld door de directie.[95] In het informatieveiligheidsbeleid wordt de beheerstructuur voor informatiebeveiliging beschreven, worden de verantwoordelijkheden voor informatiebeveiliging belegd[96] en wordt de wijze waarop informatieveiligheid is ingebed in de reguliere planning- en control cyclus[97] uiteengezet. Daarnaast wordt een aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en –maatregelen opgenomen die voor alle processen en systemen van de organisatie kunnen gelden.[98]

Het Informatieveiligheidsbeleid kent de volgende uitgangspunten:[99]

1. *Het informatieveiligheidsbeleid van de provincie is in lijn met het algemene beleid van de provincie en de relevante wet- en regelgeving.*[100]
2. *Het beleid is gebaseerd op de IBI die is afgeleid van de Code voor Informatiebeveiliging (NEN/ISO 27002).*

[88] Provincie Flevoland (2012), Informatie in Beweging: Ontwikkeling van de informatievoorziening in de provincie Flevoland 2012-2015, p.4.
[89] Provincie Flevoland (2015), Werkplan I&A 2015-2016, p.20.
[90] Provincie Flevoland (2015), Werkplan I&A 2015-2016, p.20.
[91] Provincie Flevoland, e-mail 4 maart 2016.
[92] Provincie Flevoland (2014), Verslag directievergadering 19 november 2014.
[93] Provincie Flevoland (2014), Projectplan Implementeren proces verplichtende zelfregulering Informatieveiligheid, p.4.
[94] Provincie Flevoland (2014), Projectplan Implementeren proces verplichtende zelfregulering Informatieveiligheid, p.6.
[95] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0 , p.8.
[96] Deze verantwoordelijkheden zijn aan de orde gekomen in Hoofdstuk 2, paragraaf 2.2 van dit rapport.
[97] De wijze waarop informatieveiligheid is ingebed in de planning- en controlcyclus komt aan de orde in Hoofdstuk 5, paragraaf 5.1 van dit rapport.
[98] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.5.
[99] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.10.
[100] Daarbij geldt het 'comply or explain' principe (pas toe of leg uit).

3. *Voor iedere maatregel uit de IBI geldt: Pas toe of leg uit. De uitleg bevat altijd een risicoafweging.*
4. *Het informatieveiligheidsbeleid wordt vastgesteld door de directie. Het beleid wordt minimaal één keer per vier jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.*

In het Informatieveiligheidsbeleid staat expliciet vermeld dat het is gebaseerd op de IBI en dat de IBI als normenkader wordt gehanteerd.[101] De elf categorieën uit de IBI komen in het Informatieveiligheidsbeleid van de provincie aan bod in de hoofdstukken 5 t/m 17. Voor elk van de categorieën worden beheersmaatregelen genoemd die de provincie van belang vindt om te nemen, met daarbij de doelstellingen en de risico's die respectievelijk worden nagestreefd en beheerst.

*Beleidsuitgangspunten en het Werkplan I&A*
Het Informatieveiligheidsbeleid wordt vervolgens op een aantal onderwerpen verder uitgewerkt in beleidsuitgangspunten en de speerpunten op het gebied van informatieveiligheid worden opgenomen in het Werkplan I&A. We gaan nader in op deze beleidsuitgangspunten en het Werkplan I&A in paragraaf 3.2.1 en in paragraaf 5.1.

## 3.2 De uitvoering van informatieveiligheidsmaatregelen

### *3.2.1 Uitvoering van generieke maatregelen*

**Criterium 4**
*De provincie heeft alle generieke maatregelen uit de IBI: (1) geconcretiseerd en (2) monitort de uitvoering ervan.*

Zoals eerder is aangegeven, zijn in de IBI de eisen ten aanzien van informatieveiligheid geformuleerd. Hierin wordt onderscheid gemaakt tussen generieke en aanvullende maatregelen. Generieke maatregelen zijn maatregelen die het basisniveau van beschikbaarheid, integriteit of vertrouwelijkheid aangeven. Met andere woorden, deze maatregelen dienen áltijd genomen te worden.[102] In de IBI zijn de generieke en aanvullende maatregelen ingedeeld in elf verschillende categorieën, die betrekking hebben op de aandachtsgebieden ICT, basisinfrastructuur en personeel & organisatie. Deze categorieën zijn toegelicht in Tabel 5.

De provincies hebben in het convenant afgesproken dat zij alle generieke maatregelen uit de IBI uitvoeren. De maatregelen uit de IBI zijn echter dusdanig breed geformuleerd, waardoor niet is na te gaan of de maatregelen daadwerkelijk zijn uitgevoerd. De maatregelen kunnen worden gezien als richtlijnen, waaraan een nadere invulling moet worden gegeven voordat ze kunnen worden uitgevoerd. De Rekenkamer is daarom nagegaan of de provincie de generieke maatregelen zelf heeft geconcretiseerd. Daarnaast is de Rekenkamer nagegaan of de provincie de uitvoering ervan monitort.

[101] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.5 en 7.
[102] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging.

**Tabel 5 De elf categorieën waarin de generieke en aanvullende maatregelen zijn ingedeeld**

| | Categorie | Voorbeeld |
|---|---|---|
| 1 | Beveiligingsbeleid | Het beleid moet onder meer gebaseerd zijn op ISO-normen voor informatiebeveiliging |
| 2 | Organisatie van informatiebeveiliging | De eigenaar van elk proces (bijvoorbeeld subsidieverlening) moet verantwoordelijk zijn voor het niveau van informatieveiligheid van zijn proces |
| 3 | Beheer van bedrijfsmiddelen | Er zijn regels voor het verantwoord gebruik van internet, e-mail, social media opgesteld. |
| 4 | Beveiliging van personeel | Alle nieuwe en bestaande medewerkers (ook tijdelijke en ingehuurde krachten) moeten bekend zijn gemaakt met bijvoorbeeld de regels voor verantwoord gebruik van internet. |
| 5 | Fysieke beveiliging en beveiliging van de omgeving | Alleen bevoegd personeel heeft toegang tot bepaalde ruimten. Dat kan het provinciegebouw zijn, maar bijvoorbeeld ook serverruimten. |
| 6 | Beheer van communicatie- en bedieningsprocessen | Voorbeelden zijn het installeren van antivirusprogramma's, het maken van back-ups en afspraken over het gebruik van USB-sticks. |
| 7 | Toegangsbeveiliging | Dit gaat over digitale toegangsbeveiliging, zoals wachtwoordbeleid en procedures die erop toezien dat alleen de juiste personen op bepaalde applicaties (zoals een financieel administratiesysteem) kunnen inloggen. |
| 8 | Verwerving, ontwikkeling en onderhoud van informatiesystemen | In eisen aan nieuwe informatiesystemen moeten ook beveiligingseisen worden opgenomen. |
| 9 | Beheer van informatiebeveiligingsincidenten | Zorgen dat goed en snel actie op informatiebeveiligingsincidenten wordt ondernomen. Ook moet over beveiligingsincidenten worden gerapporteerd aan management. |
| 10 | Bedrijfscontinuïteitsbeheer | Plannen opstellen met maatregelen om te zorgen dat belangrijke informatiesystemen bij grote storingen tijdig weer werken. |
| 11 | Naleving | Dit betreft onder meer naleving van de privacywetgeving. |

**Bevinding 4**

Uit eigen controles van de provincie is gebleken dat ook bij kritieke systemen de generieke maatregelen doorgaans niet volledig geïmplementeerd zijn. De provincie zet daarom eerst in op de uitvoering van generieke maatregelen, met name bij de kritieke systemen.

De provincie gebruikt de interprovinciale monitor informatieveiligheid om de uitvoering van de generieke maatregelen jaarlijks te monitoren. Hiervoor vult de provincie het standaard format van de monitoringtool voor elke generieke maatregel aan met concreet te ondernemen acties en de verantwoordelijken daarvoor. Voor de maatregelen uit de IBI en/of het informatieveiligheidsbeleid die wat meer op hoofdlijnen zijn geformuleerd en daardoor minder goed controleerbaar zijn, heeft de provincie beleidsuitgangspunten geformuleerd die kunnen functioneren als een 'vinklijst'. Voor deze beleidsuitgangspunten heeft de provincie specifieke controleplannen opgesteld.

Gezien de verwachte nieuwe IBI, met meer en concretere maatregelen, heeft de provincie begin 2016 een projectplan opgesteld voor de ingebruikname van een nieuw monitoringinstrument.

Toelichting op de bevinding

De provincie heeft in het feitelijk wederhoor aangegeven dat uit controles is gebleken dat zelfs bij de kritieke systemen de generieke maatregelen nog niet volledig zijn geïmplementeerd. Op advies van de adviseur informatieveiligheid worden eerst de kritieke systemen op orde gebracht.[103]

In de concretisering en de monitoring op de uitvoering van de generieke maatregelen uit de IBI zijn in de provincie drie zaken relevant: de wijze waarop de monitoringtool wordt ingezet, de beleidsuitgangspunten en monitoring/controles en de ontwikkelingen op het gebied van monitoring. Hieronder wordt ingegaan op deze punten.

***De wijze waarop de monitoringtool wordt ingezet***

De provincie gebruikt de interprovinciale monitor informatieveiligheid (monitoringtool) als basis voor de concretisering van de informatieveiligheidsmaatregelen uit de IBI en de monitoring van de uitvoering ervan.[104] De monitoringtool is ontwikkeld door het Cibo, wordt ingevuld door de provincie zelf en brengt in beeld hoe de informatieveiligheid van de provincie zich verhoudt tot het basisniveau uit de IBI. De monitoringtool omvat alle generieke maatregelen uit de IBI (zie Tabel 5). In paragraaf 5.3 “Uitvoering van een zelfevaluatie“ wordt de monitoringtool verder toegelicht.

Ten opzichte van het normale gebruik van de monitoringtool – het invullen van het standaard format – wordt er door de adviseur informatieveiligheid extra informatie aan de monitoringtool toegevoegd. Zo worden er per generieke maatregel concretere acties geformuleerd die aangeven wat er op een bepaalde maatregel volgens de IBI zou moeten worden geregeld. Daarnaast worden er in de monitoringtool ten opzichte van het reguliere format ook verantwoordelijken per maatregel toegevoegd door de adviseur informatieveiligheid.[105] De adviseur informatieveiligheid voert hiervoor gesprekken met de verantwoordelijken over wat de status is van de maatregel en wat er (nog) dient te gebeuren op de betreffende maatregel.[106] De monitoringtool wordt ook aangevuld met resultaten en aanbevelingen uit andere (onderzoeks)rapporten op het gebied van informatieveiligheid bij de provincie.[107]

***Beleidsuitgangspunten en monitoring / controles***

Door de ambtelijke organisatie is aangegeven dat sommige hoofdstukken uit het informatieveiligheidsbeleid wat meer op hoofdlijnen zijn geformuleerd en dat de uitvoering van het beleid daardoor niet altijd goed controleerbaar is. Daarom zijn onderdelen van het informatieveiligheidsbeleid door de adviseur informatieveiligheid uitgewerkt in beleidsuitgangspunten. Deze beleidsuitgangspunten worden gebaseerd op de kaders en stukken van de Informatiebeveiligingsdienst[108] en vertaald naar de provincie. De beleidsuitgangspunten zijn een concretisering van de generieke maatregelen uit de IBI die kunnen worden ‘afgevinkt’.[109] Tegelijkertijd met het vaststellen van

[103] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.
[104] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[105] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab ‘Baseline implementatie’; provincie Flevoland (2016), Monitoringtool Informatiebeveiliging provincie Flevoland 2015, tab ‘Baseline implementatie’.
[106] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[107] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab ‘Baseline implementatie’; provincie Flevoland (2016), Monitoringtool Informatiebeveiliging provincie Flevoland 2015, tab ‘Baseline implementatie’; ambtelijk interview, 11 februari 2016.
[108] De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete (incident)ondersteuning aangaande informatiebeveiliging. (bron: www.ibdgemeenten.nl).
[109] Provincie Flevoland, ambtelijk interview, 11 februari 2016.

het informatieveiligheidsbeleid is op 20 mei 2015 ook een aantal van deze beleidsuitgangspunten door de directie vastgesteld.[110] Het gaat dan om beleidsuitgangspunten met betrekking tot onder andere:

- Wachtwoordenbeleid[111]
- Clean desk[112]
- Logische toegangsbeleid[113]
- Beveiliging webapplicaties[114]

Naast de reeds genoemde monitoringtool zijn deze beleidsuitgangspunten de basis voor de controles die de adviseur informatieveiligheid uitvoert. De provincie geeft hierover aan dat in principe alle maatregelen toegepast moeten worden, maar dat omwille van beschikbare tijd niet elke maatregel kan worden gecontroleerd. De controles richten zich op de meest kritische systemen.[115] Het controleplan geeft weer welke controles er worden gedaan en waarom en wanneer ze worden uitgevoerd.[116]

De resultaten van een controle worden opgenomen in een controlerapport.[117] Dit controlerapport wordt besproken met de verantwoordelijke afdelingsmanager.[118] Hieruit kan – indien nodig – een actieplan volgen.[119]

***Ontwikkelingen op het gebied van monitoring***

De controles op de uitvoering van de generieke maatregelen vinden nu vooral plaats op basis van de monitoringtool, met daarnaast de genoemde controleplannen. Echter, de monitoringtool wordt niet meer als adequaat beschouwd. De reden hiervoor is dat de provincies binnen het Cibo werken aan een nieuwe IBI, die in 2016 van kracht moet worden. De monitoringtool, die is gebaseerd op de huidige IBI, komt met de nieuwe IBI te vervallen.

De nieuwe IBI kent meer en verder geconcretiseerde (generieke) maatregelen. In een aantal andere provincies (Utrecht en Noord-Brabant) wordt daarom een ander instrument – GRC-*tooling*[120] – ingezet ten behoeve van de monitoring op de uitvoering van de generieke maatregelen. Dit instrument is veel uitgebreider dan de monitoringtool die nu wordt gebruikt binnen de provincie. Het gebruik ervan zal daarom meer inspanning vergen. Mede daarom heeft de directie op 17 december 2015 besloten om eerst de keuze voor een bepaalde monitoringtool van het Strategisch Informatie Overleg (SIO; dit is een overleg in IPO-verband) af te wachten en voorlopig geen eigen initiatieven te nemen.[121]
Begin 2016 is er een activiteitenplan gemaakt om de genoemde GRC-*tooling* in het eerste half jaar van 2016 in gebruik te nemen.[122] Ook is er een activiteitenplan opgesteld voor de implementatie van een Information Security

[110] Provincie Flevoland (2015), Verslag directievergadering 20 mei 2015, agendapunt 4: operationele beleidsuitgangspunten informatieveiligheid.
[111] Provincie Flevoland (2015), Beleidsuitgangspunten wachtwoordbeleid van provincie Flevoland.
[112] Provincie Flevoland (2015), Beleidsuitgangspunten Clean Deskbeleid van provincie Flevoland.
[113] Provincie Flevoland (2015), Beleidsuitgangspunten logische toegangsbeleid van provincie Flevoland.
[114] Provincie Flevoland (2015), Beleidsuitgangspunten beveiliging webapplicaties van provincie Flevoland.
[115] Provincie Flevoland, ambtelijk interview 8 december 2015.
[116] Provincie Flevoland (2016), Intern Controleplan Informatieveiligheid Provincie Flevoland.
[117] Provincie Flevoland (2015), Controle Beleidsuitgangspunten clean desk bij Afdeling Management Ondersteuning; Controle fysieke toegang provincie Flevoland.
[118] Provincie Flevoland (2015), Managementreactie controle fysieke toegang, juni 2015 V2; ambtelijk interview 14 december 2015.
[119] Provincie Flevoland (2015), Actieplan opvolging controle fysieke toegang.
[120] GRC tooling staat voor het monitoring instrument op het gebied van Governance, Risk & Compliance-tooling..
[121] Provincie Flevoland (2015), Nota Besluitvorming BDO Onderzoek Informatieveiligheid, aan het directieteam, 30 november 2015
[122] Provincie Flevoland (2016), Activiteitenplan GRC-tooling.

Management System (ISMS).[123] Het doel van een ISMS is om te zorgen dat er een Plan-Do-Check-Act cyclus voor informatieveiligheid komt. Een ISMS betekent dat er een structurele beheercyclus voor informatieveiligheid is, zodat de provincie 'in control' kan zijn met betrekking tot:

- de maatregelen die de provincie gepland had te doen ('Plan');
- het gestructureerd uitvoeren ervan ('Do');
- het controleren of de maatregelen daadwerkelijk zijn uitgevoerd ('Check');
- indien nodig, het ondernemen van actie ('Act').

### *3.2.2. Uitvoering van risicoanalyses en aanvullende maatregelen*

**Criterium 5a**

*De provincie heeft risicoanalyses uitgevoerd en op basis daarvan afgewogen welke aanvullende maatregelen zij dient te nemen om de informatieveiligheid te verbeteren.*

Toelichting op het criterium

De IBI schrijft voor dat iedere provincie begint met de implementatie van de generieke maatregelen. Daarnaast dient elke provincie te inventariseren welke bedrijfsprocessen en informatiesystemen verhoogd risico lopen vanuit het oogpunt van informatieveiligheid. Op basis van deze inventarisatie kan de provincie bepalen voor welke processen en systemen zij een risicoanalyse gaat uitvoeren. Op basis van de risicoanalyse kan de provincie vaststellen wat de impact op een bedrijfsproces of informatiesysteem is indien de informatieveiligheid niet gewaarborgd of zelfs geschaad is. De standaardmethode voor het uitvoeren van de risicoanalyse is de Business Impact Analyse (BIA). De bedrijfsprocessen of informatiesystemen waarvoor een BIA wordt uitgevoerd krijgen door middel van de BIA een classificatie mee op het niveau van beschikbaarheid, integriteit en vertrouwelijkheid (laag, midden of hoog). Op basis van deze classificatie maakt de provincie een afweging van aanvullende maatregelen die genomen kunnen worden.

De Rekenkamer heeft onderzocht of de provincie een inventarisatie heeft gemaakt van potentieel risicovolle bedrijfsprocessen en systemen en aan de hand daarvan heeft bepaald voor welke bedrijfsprocessen en systemen een BIA (of een vergelijkbare risicoanalyse) uitgevoerd moet worden. Vervolgens is onderzocht of aanvullende maatregelen ter verbetering van de informatieveiligheid uit deze risicoanalyses zijn voortgekomen.

**Criterium 5b**

*De provincie controleert de uitvoering van de aanvullende maatregelen die zij, op basis van de risicoanalyse en –afweging, nodig vindt om te nemen.*

Toelichting op het criterium

Het is van belang dat de aanvullend te nemen maatregelen die uit de eigen risicoanalyse en –afweging zijn voortgekomen, worden uitgevoerd. Ook is het van belang dat de provincie zicht heeft op de uitvoering van de maatregelen. De Rekenkamer heeft daarom onderzocht of de provincie de uitvoering van de aanvullende maatregelen monitort.

[123] Provincie Flevoland (2016), Activiteitenplan ISMS Processen – Kwaliteitssysteem.

**Bevinding 5**

De provincie heeft vooralsnog geen inventarisatie gemaakt van potentieel risicovolle bedrijfsprocessen en systemen, noch bepaald voor welke processen en systemen een BIA (of vergelijkbare risicoanalyse) moet worden uitgevoerd. Er worden nauwelijks risicoanalyses gedaan met bijbehorende bepaling van de mate van risicoacceptatie. Er zijn in de afgelopen zes jaar geen BIA's uitgevoerd, behalve de BIA op het financieel systeem. Hieruit kwamen geen aanvullende maatregelen voort.

Sinds eind 2015 loopt een traject om de in gebruik zijnde systemen in kaart te brengen en wordt bij een beperkt aantal systemen waarvan de provincie al weet dat ze cruciaal zijn, getoetst of zij voldoen aan het gewenste veiligheidsniveau.

Toelichting op de bevinding

De directie heeft er in november 2014 voor gekozen om eerst alle aandacht aan de generieke maatregelen uit de IBI te besteden en het onderzoeken en implementeren van aanvullende maatregelen voorlopig niet ter hand te nemen.[124] In het feitelijk wederhoor heeft de provincie een extra reden gegeven. Uit controles is gebleken dat ook bij de kritieke systemen de generieke maatregelen nog niet volledig waren geïmplementeerd. Daarom is prioriteit gegeven aan de uitvoering van de generieke maatregelen voor deze systemen.[125]

Door de ambtelijke organisatie is aangegeven dat tot voor kort nauwelijks bewust is gekeken naar de risico's die er zijn; er zijn nauwelijks risicoanalyses gedaan met bijbehorende bepaling van de mate van risicoacceptatie.[126] Dit blijkt ook uit het volgende. De provincie heeft in 2009 voor het laatst een overzicht gemaakt van mogelijk risicovolle processen. Daarna zijn er tot eind 2015 nagenoeg geen risicoanalyses uitgevoerd in het kader van informatieveiligheid.[127] Een uitzondering daarop vormt de BIA die in mei 2014 is uitgevoerd op het financiële systeem.[128] Er werden geen aanvullende maatregelen nodig geacht en deze zijn daarom niet gedefinieerd. In het feitelijk wederhoor heeft de provincie aangegeven dat in 2016 een afhankelijkheids- en kwetsbaarheidsanalyse is uitgevoerd voor de digitale handtekening.[129]

Eind 2015 is de provincie begonnen met het maken van een totaaloverzicht van in gebruik zijnde systemen. Dit zijn er meer dan honderd. Het overzicht is nodig om te kunnen zien op welk systeem wel of geen BIA zou moeten worden uitgevoerd. Dit proces vindt plaats via drie stappen:[130]

1. Eerst wordt voor alle in gebruik zijnde applicaties bekeken welke gegevens een applicatie opslaat, waar de applicatie die gegevens opslaat, wie er toegang heeft tot de applicatie, et cetera.
2. Vervolgens wordt per applicatie bekeken hoe de applicatie scoort op de risico's met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid (BIV-score). Deze stap kan worden beschouwd als eerste stap van een risicoanalyse.
3. Daarna wordt op basis van de BIV-score beslist om wel of geen BIA uit te voeren op het betreffende systeem. De beslissing hiertoe wordt genomen door de directie, op advies van de Adviseur informatieveiligheid.

[124] Provincie Flevoland (2014), Projectplan Implementeren proces verplichtende zelfregulering Informatieveiligheid.
[125] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.
[126] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 14 december 2015.
[127] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[128] Provincie Flevoland (2014), BIA Financiële Systeem, mei 2014.
[129] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.
[130] Provincie Flevoland, ambtelijk interview, 11 februari 2016.

De inventarisatie is bedoeld om de meest kritische systemen te kunnen identificeren en deze vervolgens te laten voldoen aan de IBI. In februari 2016 is de eerste stap voor zeven systemen doorlopen en gestart met de tweede stap.[131]

Bij de inventarisatie van de in gebruik zijnde applicaties hebben vertegenwoordigers van de ambtelijke organisatie twee aandachtspunten genoemd.:

- De afdelingen mogen zelfstandig hun eigen processen definiëren en systemen aanschaffen. Daardoor is er geen (centrale) controle op de aanschaf van systemen en is er ook niet vanzelf één centraal overzicht van applicaties. Daardoor is het mogelijk dat de inventarisatie van kritische systemen niet meer actueel is op het moment dat deze voltooid is.[132]
- Eigenlijk zijn systeemeigenaren verantwoordelijk voor de informatieveiligheid van de systemen die ze beheren. In beginsel zijn zij meer gericht op de functionaliteit van het systeem, met de kans dat zij niet de verantwoordelijkheid nemen om bijvoorbeeld de toegang tot het systeem te regelen en zich niet af te vragen of het systeem dat ze beheren ook veilig is.[133] (zie ook paragraaf 2.1)

Het is de bedoeling dat op basis van het totaaloverzicht van applicaties de adviseur informatieveiligheid aan de directie een voorstel doet voor de processen waarop een BIA zou moeten worden toegepast. De directie zal dan vervolgens besluiten op welke systemen er een BIA moet worden uitgevoerd. Aan de hand van een op een systeem uitgevoerde BIA zal de adviseur informatieveiligheid de risico's met betrekking tot dat systeem doorgeven aan de systeemeigenaar. De systeemeigenaar zal als verantwoordelijke eigenaar van het systeem vervolgens bepalen welke risico's worden geaccepteerd en welke niet. Hieruit zal een voorstel volgen voor te nemen maatregelen om de niet-acceptabele risico's te mitigeren. Dit voorstel zal door de adviseur informatieveiligheid vervolgens worden voorgelegd aan de directie, die als eindverantwoordelijke zal beslissen. Hierna is het de verantwoordelijkheid van de eigenaar van het systeem dat er – indien nodig geacht op basis van de BIA – maatregelen worden getroffen.[134]

Van een aantal applicaties is reeds bekend dat deze cruciaal zijn voor de organisatie, zoals het financiële systeem en het personeelssysteem. De adviseur Informatieveiligheid is in februari 2016 gestart met het toetsen van deze cruciale systemen aan de beleidsuitgangspunten (maatregelen), zodat de verschillen tussen de actuele situatie en de gewenste situatie zichtbaar worden.[135]

Aangezien er – behalve op de BIA op het financieel systeem, waar geen maatregelen uit zijn gekomen – geen BIA's zijn uitgevoerd, zijn er geen aanvullende maatregelen waarvan de uitvoering wordt gemonitord.

[131] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[132] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[133] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[134] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[135] Provincie Flevoland, ambtelijk interview, 11 februari 2016.

## 3.3 Informatieveiligheidsbeleid: het resultaat

**Criterium 6**
*De provincie doorstaat de specifieke test.*

Toelichting op het criterium
Naast de aanwezigheid van een adequaat informatieveiligheidsbeleid en de uitvoering daarvan, is het ook van belang dat het resultaat ervan voldoende is. Bieden de genomen maatregelen voldoende waarborgen tegen oneigenlijke toegang tot systemen en bestanden? De Rekenkamer heeft daarom onderzocht of de informatie in de praktijk daadwerkelijk voldoende is beschermd tegen toegang door onbevoegden.

Om dit te kunnen toetsen heeft een externe specialist in opdracht van de Rekenkamer een penetratietest uitgevoerd via applicaties die op de iPad en iPhone staan die aan de medewerkers van de provincie worden uitgereikt. Hierbij is gebruikgemaakt van de Open Web Application Security Project (OWASP) Mobile Risks standaard. OWASP heeft de tien meest voorkomende kwetsbaarheden in mobiele applicaties vastgesteld.

**Bevinding 6**
De penetratietest had betrekking op de mobiele apparaten iPhone, iPad en HTC en de daarop geïnstalleerde applicaties. Er zijn drie belangrijke kwetsbaarheden met een groot risico gevonden. Deze kwetsbaarheden hebben betrekking op de mobiele apparaten iPhone en iPad. De kwetsbaarheden die technisch oplosbaar zijn, zijn grotendeels verholpen. Een deel van de kwetsbaarheden is echter gerelateerd aan het gedrag van medewerkers ten aanzien van informatieveiligheid.

Toelichting op de bevinding[136]
In de periode van 30 november tot 11 december 2015 is een penetratietest uitgevoerd. Het doel van de penetratietest was om:
1. na te gaan of informatie in de praktijk voldoende is beschermd tegen toegang door onbevoegden;
2. inzicht te krijgen in de risico's en kwetsbaarheden van de te onderzoeken systemen;
3. handvatten te bieden aan de provincie voor verbetering van de informatieveiligheid van mobiele apparaten.

Alvorens in te gaan op de resultaten van de penetratietest is het van belang om de scope van het onderzoek te kennen. Immers, bevindingen en conclusies over de onderzochte applicaties en systemen gelden niet noodzakelijkerwijs voor andere applicaties en systemen. Daarnaast zijn er nog twee voorbehouden:
1. De mogelijkheid bestaat dat de externe specialist niet iedere kwetsbaarheid heeft gevonden, omdat diens onderzoek gebonden was aan een budget- en tijdslimiet;
2. De bevindingen zijn tijdsgebonden: na de uitvoering van de penetratietest kunnen nieuwe ontwikkelingen nieuwe kwetsbaarheden met zich meebrengen die ten tijde van de uitvoering van de penetratietest nog niet bekend waren.

*Scope van de penetratietest*
De scope van het onderzoek is in overleg met de provincie bepaald aan de hand van de meest toegevoegde waarde op eerdere praktijktoetsen. Het interne en externe netwerk en de systemen zijn reeds in 2015 getest. Onderdeel van deze tests waren onder andere het documentmanagementsysteem, het financiële systeem, het

[136] De toelichting is gebaseerd op: Hoffmann B.V. (2016), Onderzoek i.o.v. Randstedelijke Rekenkamer naar Informatieveiligheid bij de provincie Flevoland, Managementrapport nr. 21509118.

personeelssysteem, de verkeersregelinstallaties, de bediening van bruggen en sluizen, internet en intranet (websites) en het wifi-netwerk. Daarnaast verkeert één systeem in de opstartfase, waarvan de provincie weet dat de beveiliging niet sterk is, maar waar reeds aan wordt gewerkt om de beveiliging te verbeteren. Tegen deze achtergrond en aangezien het nieuwe werken met steeds intensiever gebruik van mobiele apparaten en applicaties toeneemt, is ervoor gekozen om de penetratietest uit te voeren op de mobiele apparaten (iPad, iPhone en HTC) met de daarop geïnstalleerde applicaties.

*Algemene beveiliging van de onderzochte mobiele apparaten*

De onderzochte mobiele apparaten bevatten meerdere beveiligingslagen. Om bij bepaalde systeemgegevens op de apparaten te kunnen komen, moeten deze beveiligingslagen worden doorbroken. Hieronder worden de verschillende beveiligingslagen beschreven die zijn aangetroffen.

1. Als eerste moet er een lockcode worden ingevoerd. Dit is over het algemeen een code bestaande uit vier cijfers. Via geavanceerde technieken kan deze lockcode worden gekraakt. Dit proces neemt echter zeer veel tijd in beslag. Het doorbreken van deze eerste laag kan dan ook als zeer moeilijk worden omschreven. Voor deze penetratietest is de lockcode daarom aan de externe specialisten bekendgemaakt.
2. De onderzochte apparaten bevatten een besturingssysteem (iOS, Windows) dat door de fabrikant regelmatig wordt bijgewerkt om aan de laatste beveiligingseisen te voldoen. Kwetsbaarheden die in systemen voorkomen die niet regelmatig worden bijgewerkt, kunnen door kwaadwillenden worden benut om het systeem aan te passen. Het gevolg hiervan is dat men in feite beheerrechten over het apparaat krijgt en meer rechten heeft dan een standaard gebruiker. Voor verschillende versies van het besturingssysteem bestaan er zogenaamde *jailbreaks*. Dit zijn programma's die worden ontwikkeld om gebruik te maken van kwetsbaarheden die zich in een bepaalde versie van het besturingssysteem bevinden. Het ontwikkelen van een jailbreak neemt zeer veel tijd in beslag en is uiterst complex. De installatieprocedure is echter zeer eenvoudig en wordt over het algemeen goed beschreven in openbare bronnen. Het doorbreken van deze beveiligingslaag kan dan ook als eenvoudig worden omschreven, maar is wel afhankelijk van de beschikbaarheid van een jailbreak voor een specifieke versie van het besturingssysteem. Des te ouder een versie van het besturingssysteem, des te groter is de kans dat er een jailbreak voor beschikbaar is. Voor de onderzochte apparaten iPhone en iPad is volgens de externe specialist een jailbreak openbaar beschikbaar, waarvan gebruik is gemaakt. Voor het mobiele apparaat HTC was het volgens de externe specialist niet nodig om een jailbreak uit te voeren, vanwege de aard van de penetratietest op dit apparaat.
3. Om in te kunnen loggen op de applicaties die op het mobiele apparaat zijn geïnstalleerd, is een Active Directory (AD) account nodig dat bestaat uit een gebruikersnaam en een wachtwoord. Net als bij de eerste laag zijn ook hier technieken bekend waarmee men het wachtwoord zou kunnen kraken. Ook hier neemt dit zeer veel tijd in beslag en doorbreken van deze laag kan dan ook als moeilijk worden omschreven.

*Geconstateerde kwetsbaarheden*

Tijdens het onderzoek is een drietal belangrijke kwetsbaarheden met een groot risico gevonden. Deze kwetsbaarheden worden hieronder toegelicht.

1. Eén van de apps op de iPad accepteert een vals certificaat. Hierdoor kunnen onbevoegden zich toegang verschaffen tot de app, wanneer zij in staat zijn om een vals certificaat aan te bieden. Echter, door de verschillende genoemde algemene beveiligingslagen is deze kwetsbaarheid door kwaadwillenden van buiten de provincie moeilijk te benutten.
2. Via één van de apps op de iPad zijn documenten met vertrouwelijke informatie in te zien. De externe specialist vond hier, na een eenvoudig en kort zoekproces, een aantal documenten met persoonlijke gegevens (naam, adres, woonplaats en BSN-nummer van een medewerker van de provincie of familielid of kennis daarvan) en bijvoorbeeld een screeningsrapport onder de BIBOB-wetgeving. Ook hier geldt dat deze kwetsbaarheid door kwaadwillenden van buiten de provincie moeilijk is te benutten, door de verschillende

genoemde algemene beveiligingslagen. Echter, de kans dat iemand van binnen de provincie onbedoeld toegang tot dit soort stukken heeft is zeker wel aanwezig. Dergelijke documenten behoren, op basis van rollen die medewerkers kunnen hebben, te worden afgeschermd. Dit wordt in de organisatie wel toegepast, maar is blijkbaar (nog) niet correct geïmplementeerd binnen het documentbeheersysteem.

3. Voor één van de apps op de iPad geldt wel een verhoogd risico, omdat het dataverkeer – de gegevensoverdracht tussen mobiel apparaat en de server – kan worden achterhaald, zonder dat bovengenoemde algemene beveiligingslagen hoeven te worden gepasseerd. Via het achterhaalde dataverkeer waren gebruikersnaam en wachtwoord van het ingelogde account te bemachtigen. Hiervoor moet een kwaadwillende zich wel op hetzelfde netwerk als het apparaat bevinden en kennis hebben van de ARP-poisoning[137] techniek, wat voor mensen met enige technische kennis niet moeilijk is.

Naast bovenstaande drie als technisch 'kritiek' te kenmerken kwetsbaarheden heeft de externe specialist nog enkele kwetsbaarheden in de categorieën 'medium' en 'laag' gevonden.

Er zijn geen kwetsbaarheden aangetroffen op de onderzochte applicaties op het mobiele apparaat HTC.

*Getroffen maatregelen*

Op 18 mei 2016 hebben de provincie, de externe specialist en de Rekenkamer de geconstateerde kwetsbaarheden en de maatregelen om de kwetsbaarheden tegen te gaan, doorgesproken. De provincie heeft aangegeven dat aan de maatregelen wordt gewerkt. De kwetsbaarheden die technisch oplosbaar zijn, zijn grotendeels verholpen. Een belangrijke factor is echter bewustwording: een deel van de kwetsbaarheden is gerelateerd aan het gedrag van medewerkers.

[137] ARP-poisoning is een techniek waarbij een hacker ervoor zorgt dat al het verkeer van het doelwit (bijvoorbeeld een computer, tablet of mobiele telefoon) wordt omgeleid via de machine van de aanvaller, waardoor deze al het dataverkeer kan monitoren.

# | 4 | Bewustwording van informatie-veiligheid

Eén van de aandachtsgebieden van informatieveiligheid is mens & organisatie. Het gedrag van mensen is van cruciaal belang voor het borgen van informatieveiligheid. Met ICT-maatregelen (bijvoorbeeld firewalls, wachtwoordbeleid) en fysieke maatregelen (bijvoorbeeld toegangspasjes en -poorten) kan de informatieveiligheid binnen een organisatie worden bevorderd. Maar ICT en fysieke maatregelen alleen zijn niet voldoende. Zo is een strikt wachtwoordbeleid zinloos als wachtwoorden regelmatig gedeeld worden of op een zichtbare plek zijn opgeschreven.

Het gedrag van mensen in een organisatie is dus eveneens zeer belangrijk. Iedereen dient zich ervan bewust te zijn dat men met zijn of haar gedrag de mate van informatieveiligheid kan beïnvloeden. De Rekenkamer heeft onderzocht wat de provincie heeft gedaan om het bewustzijn van informatieveiligheid bij de provincie te vergroten. Het gaat daarbij om bestuur, management, medewerkers, ingehuurd personeel en externe gebruikers.

## 4.1 Verantwoordelijkheid van medewerkers in hun dagelijks handelen

**Criterium 7a**
*Bestuur, medewerkers, ingehuurd personeel en externe gebruikers zijn bekendgemaakt met de verantwoordelijkheid die zij hebben in hun dagelijks handelen op het gebied van informatieveiligheid.*

Toelichting op het criterium
Voor dit criterium heeft de Rekenkamer onderzocht hoe alle medewerkers[138] zijn geïnformeerd over wat zij kunnen of moeten doen in hun dagelijks handelen om de informatieveiligheid te borgen. Het gaat dan zowel om de verstrekking van informatie bij aantreding of inhuur, als om informatie die tussentijds aan alle medewerkers wordt verspreid. Het kan bijvoorbeeld gaan om gedragsregels voor sociale media en het gebruik van laptops, tablets of USB-sticks.

**Criterium 7b**
*De provincie voert periodiek een bewustwordingsprogramma uit met als doel alle medewerkers te informeren, alsook het op peil houden van kennis en vaardigheden op het gebied van informatieveiligheid.*

Toelichting op het criterium
Voor dit criterium is de Rekenkamer nagegaan of de provincie een programma heeft om medewerkers bewust te maken van risico's bij informatieveiligheid en hun mogelijkheden om deze risico's te verkleinen. En als de provincie een dergelijk bewustwordingsprogramma heeft, hoeveel medewerkers daarmee worden bereikt.

[138] Met 'alle medewerkers' bedoel de Rekenkamer het bestuur, het management, medewerkers, ingehuurd personeel en externe gebruikers.

**Bevinding 7**

In december 2012 heeft de provincie in de nota Informatie in Beweging 2012-2015 het voornemen voor een bewustwordingsprogramma opgenomen. De uitvoering van dit voornemen heeft lang op zich laten wachten. Pas in 2014 is een projectplan bewustwording informatieveiligheid opgesteld. Na een langzame start is de provincie eind 2015 actief aan de slag gegaan met de uitvoering van het bewustwordingsprogramma. Er is een activiteitenplan gemaakt voor 2016 en de eerste activiteiten zijn inmiddels gestart.

Toelichting op de bevinding

Bovenstaande bevinding wordt in onderstaande subparagrafen toegelicht. Achtereenvolgens wordt ingegaan op de bewustwording onder de medewerkers, de uitvoering van bewustwordingsprogramma's en de manier waarop en de mate waarin de provincie medewerkers bekend worden gemaakt met hun verantwoordelijkheden ten aanzien van informatieveiligheid.

### *4.1.1 Bewustwording onder de medewerkers*

Door diverse vertegenwoordigers van de ambtelijke organisatie is aangegeven dat de bewustwording onder de medewerkers op dit moment wisselt per afdeling, niet op orde is en vatbaar voor verbetering.[139] Als voorbeelden hiervan worden gegeven:

- Medewerkers houden zich niet aan de richtlijnen voor het delen – zowel extern als intern – van informatie. Zo wordt er informatie gedeeld via Google Drive, Drop-Box en WeTransfer;[140]
- Het niet volgens de richtlijnen gebruiken van eDocs (het documentmanagementsysteem van de provincie), waarbij eDocs door de een als archief wordt gebruikt en door de ander als opslagplaats voor kladversies;[141]
- Het niet volgens de normen opzetten en het actief beheren van publiek toegankelijke sites / URL's vanuit de provincie, waardoor er mogelijk onbedoeld en onbewust gegevens buiten de provincie staan;[142]
- Het in gang zetten van wijzigingen op IT-gebied, zonder daarbij vooraf het Cluster Informatiemanagement vanuit het perspectief van informatieveiligheid te betrekken. Hierdoor is informatieveiligheid niet altijd goed geborgd en/of is er achteraf bijsturen of herstelwerk nodig;[143]
- Het binnenhalen van een virus door op een onbekende link in een e-mail te klikken.[144]

### *4.1.2 Uitvoering van bewustwordingsprogramma*

In de nota 'Informatie in Beweging 2012-2015' wordt een bewustwordingsprogramma genoemd als beheersmaatregel voor het gebruik van eigen apparaten door medewerkers en de risico's die hieruit kunnen voortkomen op het gebied van informatiebeveiliging.[145] Tot medio 2014 is weinig tot geen aandacht geschonken aan het onderwerp bewustwording door minimale bezetting en bijbehorende prioriteitsstelling.[146] Op 8 oktober 2014 heeft de directie het project Verplichtende Zelfregulering Informatieveiligheid provincie Flevoland vastgesteld. Daarin is opgenomen dat het creëren van draagvlak noodzakelijk is voor het succesvol

[139] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 11 januari 2016.
[140] Provincie Flevoland, ambtelijke interviews, 8 december 2015, 14 december 2015 en 11 januari 2016.
[141] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[142] Provincie Flevoland, ambtelijke interviews, 14 december 2015 en 11 januari 2016.
[143] Provincie Flevoland, ambtelijk interview, 14 december 2015.
[144] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[145] Provincie Flevoland (2012), Informatie in Beweging: Ontwikkeling van de informatievoorziening in de provincie Flevoland 2012-2015, p.21.
[146] Provincie Flevoland (2014), Projectplan Bewustwordingscampagne Informatieveiligheid Provincie Flevoland, p.4.

implementeren van de Verplichtende Zelfregulering.[147] Hierbij aansluitend heeft de directie gelijktijdig het Projectplan Bewustwordingscampagne Informatieveiligheid Provincie Flevoland vastgesteld.[148]

De bewustwordingscampagne richt zich op het vierde kwartaal van 2014 en het eerste kwartaal van 2015 en kent twee doelstellingen:[149]

- *De provincie Flevoland wil informatieveiligheid voldoende onder de aandacht hebben van het management en medewerkers, zodat er draagvlak is voor het kunnen implementeren van de Verplichtende Zelfregulering Informatieveiligheid.*
- *De provincie Flevoland neemt haar verantwoordelijkheid voor de bewustwording informatieveiligheid serieus door het grondig bestuderen van de suggesties en producten van het CIBO en de Taskforce.*

De volgende projectresultaten worden met de bewustwordingscampagne beoogd:[150]

- *Posters Informatieveiligheid zijn opgesteld en opgehangen in het gebouw.*
- *Een brochure Informatieveiligheid is opgesteld en verspreid.*
- *Een presentatie Informatieveiligheid is opgesteld en gegeven in bijeenkomsten met nieuwe medewerkers en in werkoverleggen.*
- *Enkele artikelen zijn opgesteld, verzameld en / of geplaatst op het Intranet.*
- *Een penetratietest is uitgevoerd.*
- *Een organisatie-brede enquête en een tiental interviews zijn uitgevoerd.*

In een Halfjaarsrapportage Informatieveiligheid van februari 2015 wordt over het onderwerp bewustwording gerapporteerd.[151] Hieruit blijkt dat er eind 2014 een start is gemaakt met de bewustwordingscampagne:

- De posters en brochures zijn beschikbaar, maar niet opgehangen/verspreid;
- Er is een presentatie over informatieveiligheid opgesteld, maar de uitnodiging voor een dialoogsessie is door zowel GS als de directie niet opgepakt;
- Er is in januari 2015 een artikel in de Flevoflits geplaatst en een artikel over een interview door de Taskforce is gepland voor publicatie medio maart 2015;
- Een voorstel voor een brede enquête en een aantal interviews is opgesteld, maar de enquête is nog niet uitgezet en de interviews zijn nog niet gehouden.

Niet lang daarna is de bewustwordingscampagne on-hold gezet.[152] Op 20 mei 2015 wordt eerst het Informatiebeveiligingsbeleid Provincie Flevoland vastgesteld door de directie.[153] Hierin is opgenomen dat "*alle medewerkers van de provincie worden getraind in het gebruik van beveiligingsprocedures*".[154] Daarna zijn er door de adviseur informatieveiligheid nog werkplekonderzoeken uitgevoerd bij een aantal afdelingen. Hierbij is gekeken naar het achterblijven van documenten op bureaus, het vergrendelen/afsluiten van computers, het sluiten van de kasten en dergelijke.[155]

[147] Provincie Flevoland (2014), Projectplan Implementeren proces verplichtende zelfregulering Informatieveiligheid.
[148] Provincie Flevoland (2014), Verslag directievergadering 19 november 2014.
[149] Provincie Flevoland (2014), Projectplan Bewustwordingscampagne Informatieveiligheid Provincie Flevoland, p.4.
[150] Provincie Flevoland (2014), Projectplan Bewustwordingscampagne Informatieveiligheid Provincie Flevoland, p.4.
[151] Provincie Flevoland (2015), Eerste halfjaarsrapportage Informatieveiligheid Provincie Flevoland: augustus 2014 – februari 2015.
[152] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 11 februari 2016.
[153] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.8.
[154] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.8.
[155] Provincie Flevoland, ambtelijke interviews, 8 december 2015.

Sinds het vierde kwartaal 2015 is het onderwerp bewustwording weer opgepakt.[156] De volgende acties zijn uitgevoerd in het kader van bewustwording:

- De adviseur informatieveiligheid is begonnen met het opstellen van een bewustwordingsplan, mede op basis van gesprekken met de managementteams van de afdelingen, waarin wordt besproken waar de afdelingen behoefte aan hebben in het kader van bewustwording op het gebied van informatieveiligheid;[157]
- Er zijn presentaties gehouden in het managementberaad en in de managementteams;[158]
- De zogenaamde "Tien gouden regels" met belangrijke aandachtspunten uit het informatieveiligheidsbeleid van de provincie zijn beschikbaar gesteld voor alle medewerkers.[159]
- Het Cluster Informatiemanagement heeft de Pleio-Box gepresenteerd in de entreehal van het provinciehuis. De Pleio-Box is een veilig alternatief systeem voor onder andere bestandsuitwisseling binnen de overheid en wordt gehost door de Belastingdienst.[160]

Hierbij aansluitend is voor 2016 een activiteitenplan bewustwording informatieveiligheid opgesteld met de teamleider cluster Informatiemanagement als opdrachtgever en de adviseur informatieveiligheid als opdrachtnemer. Hierin staan acties beschreven die vanaf de tweede helft van december 2015 en verder in 2016 worden opgepakt, zoals presentaties aan GS, de managementteams, in de afdelingsoverleggen en aan de nieuwe en huidige medewerkers, het plaatsen van artikelen, beleidsdocumenten, filmpjes etc. op Intranet, het hangen van posters op de prikborden en leggen van brochures op de bureaus, het instellen van een inloopspreekuur en het verspreiden van de brochure met de Tien Gouden Regels.[161] In aanvulling daarop is in het Intern Controleplan Informatieveiligheid opgenomen dat de eerder genoemde werkplekonderzoeken (‘clean desk’ controles) zullen worden voortgezet met een frequentie van een half jaar.[162]

### *4.1.3 Documenten en richtlijnen m.b.t. verantwoordelijkheden informatieveiligheid*

De provincie heeft enkele documenten waarmee zij medewerkers (inclusief nieuwe medewerkers en ingehuurd personeel) bekendmaken met de verantwoordelijkheid die zij hebben in hun dagelijks handelen op het gebied van informatieveiligheid. Tabel 6 geeft een overzicht van deze documenten, met een korte toelichting op het document, de doelgroep en de manier van overdracht.

[156] Provincie Flevoland, ambtelijke interviews, 14 december 2015 en 11 februari 2016.
[157] Provincie Flevoland, ambtelijke interviews, 8 december 2015, 14 december 2015 en, 11 februari 2016
[158] Provincie Flevoland (2015), Presentatie informatieveiligheid Managementberaad;, Presentatie Verbetertraject informatieveiligheid; Presentatie Bewustwording informatieveiligheid voor de managementteams.
[159] Provincie Flevoland (2015), Nota Besluitvorming directieteam, BDO Onderzoek Informatieveiligheid, 16 december 2015 .
[160] Provincie Flevoland, ambtelijk interview, 14 december 2015.
[161] Provincie Flevoland (2015), Activiteitenplan Bewustwording Informatieveiligheid.
[162] Provincie Flevoland (2016), Intern Controleplan Informatieveiligheid Provincie Flevoland, februari 2016.

**Tabel 6 Overzicht van documenten met betrekking tot verantwoordelijkheden van medewerkers op het gebied van informatieveiligheid**

| Document | Toelichting | Doelgroep |
|---|---|---|
| 10 Gouden Regels[163] | Bevat belangrijke aandachtspunten uit het informatieveiligheidsbeleid van de provincie. Ter informatie in het introductiepakket en beschikbaar op Intranet. | Nieuwe en bestaande medewerkers |
| Verklaring geheimhouding | Verklaring voor ontvangst van de toegangspas en een verklaring van geheimhouding en handelen naar de gedragscode. Deze wordt afgelegd ten overstaan van een medewerker van de provincie als getuige, ondertekend en medeondertekend door de getuige. | Tijdelijke medewerkers |
| Verklaring omtrent geheimhouding en integriteit | Verklaring over hoe om te gaan met (vertrouwelijke) informatie. | Externe inhuur |
| Bruikleenovereenkomst iPad[164] | Deze bruikleenovereenkomst geeft de rechten en plichten en regels van goed gebruik weer van een iPad. | Leidinggevenden / programmamanagers |
| Gedragscode ambtelijke integriteit 2016[165] | Artikel 3 gaat over de wijze van omgang met informatie | Alle medewerkers, ook externe inhuur |

Er loopt nog een project Instroom-Doorstroom-Uitstroom (IDU) bij P&O. Het IDU-proces is inmiddels beschreven, maar het project is nog niet afgerond. De introductie over informatieveiligheid, de bruikleenovereenkomst, et cetera, maken hier onderdeel van uit.[166] Vaste medewerkers dienen de ambtseed af te leggen.[167]

[163] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[164] Provincie Flevoland, Bruikleenovereenkomst iPad.
[165] Provincie Flevoland (2016), Gedragscode ambtelijke integriteit Flevoland.
[166] Provincie Flevoland, e-mail 7 maart 2016.
[167] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.

# | 5 | Verantwoording & Toezicht

Dit hoofdstuk gaat na of de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed heeft geregeld. Achtereenvolgens wordt ingegaan op de borging van informatieveiligheid in de planning en control cyclus, de uitvoering van een onafhankelijke toets en het doen van zelfevaluaties.

## 5.1 Informatieveiligheid in de planning & controle cyclus

**Criterium 8**
*De provincie heeft informatieveiligheid verankerd in de reguliere planning en control cyclus en geeft in het jaarverslag inzicht in de status van informatieveiligheid.*

Toelichting op het criterium
Bij het borgen van informatieveiligheid van provincies staat het principe van verplichtende zelfregulering centraal. Dit principe houdt in dat iedere provincie zelf verantwoordelijk is voor het informatieveiligheidsbeleid, met als stok achter de deur dat wanneer de informatieveiligheid onvoldoende wordt geïntegreerd in de bedrijfsvoering, verplichtingen op basis van (wettelijke) regelgeving zullen volgen.[168]

De verplichtende zelfregulering betekent dus dat er geen sprake is van een vrijblijvend proces. Dat maakt het van belang dat bestuur en management van de provincie goed zicht hebben op de stand van zaken bij informatieveiligheid. Daarom is in het convenant afgesproken dat over informatieveiligheid wordt gerapporteerd in de planning & control cyclus (P&C-cyclus). Onder P&C-cyclus wordt de rapportagesystematiek aan management, GS en PS verstaan. Er wordt dus ook gekeken naar de verantwoording over informatieveiligheid in de jaarstukken.

**Bevinding 8**
Informatieveiligheid is sinds de ondertekening van het convenant onderdeel van de bestuurlijke P&C-cyclus (aan GS en PS). Er is een korte toelichting op het onderwerp opgenomen in de Jaarstukken 2014 en de Programmabegroting 2016.

Informatieveiligheid is ook onderdeel van de ambtelijke P&C-cyclus (aan het management). Het Werkplan I&A, met daarin opgenomen het Jaarplan Informatieveiligheid, wordt gemonitord door de IT-raad.

[168] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014.

Toelichting op de bevinding

Achtereenvolgens gaan we hier in op de bestuurlijke P&C-cyclus en de ambtelijke P&C-cyclus.

*Bestuurlijke P&C-cyclus*

Sinds de ondertekening van het convenant eind 2014 zijn de volgende documenten verschenen in de bestuurlijke P&C-cyclus. Dit zijn:

- P&C-cyclus jaar 2014: Jaarstukken 2014
- P&C-cyclus jaar 2015: Perspectiefnota 2015-2019, Zomernota 2015
- P&C-cyclus jaar 2016: Programmabegroting 2016

In de Jaarstukken 2014 valt in de paragraaf Bedrijfsvoering te lezen dat PS bij de behandeling van de jaarstukken 2010 de noodzaak van een 'aanvalsplan interne beheersing' vast hebben gesteld en dat dit vervolgens, voorzien van een budget van € 1,2 miljoen, is opgenomen in het Coalitieakkoord 2011-2015. In 2011 is een Programmaplan verbetering interne beheersing aangeboden aan de statenwerkgroep Planning en Control, met daarin zeven speerpunten, waaronder 'Beheersing van de IT-omgeving'. *Als onderdeel van het speerpunt Beheersing van de IT-omgeving is ook aandacht besteed aan informatiebeveiliging. De provincie is immers verantwoordelijk voor een passende beveiliging van de informatie waarover zij beschikt. In 2014 zijn de kaders geformuleerd die nodig zijn om deze beveiliging op een structurele wijze vorm te geven en te borgen in de bestaande planning en control cyclus. Er is actief gewerkt aan de informatieveiligheid van Flevoland. Het informatiebeveiligingsbeleid wordt op dit moment aangepast op de Interprovinciale Baseline Informatiebeveiliging. In 2015 worden diverse maatregelen uitgevoerd op basis van een afweging van het risicoprofiel.*[169] Over dit programma is een afzonderlijke eindrapportage voor PS opgesteld, waarin inhoudelijk wordt ingegaan op de resultaten.[170] Deze eindrapportage stond ter kennisname op de agenda van de PS vergadering van 17 december 2014.[171]

In zowel de Perspectiefnota 2015-2019 als de Zomernota 2015 is niets opgenomen over informatieveiligheid.[172]

In de Programmabegroting 2016 wordt informatieveiligheid expliciet genoemd onder de noemer van de Meerjaren aanpak Bedrijfsvoering vanwege de *strengere eisen die worden gesteld aan informatieveiligheid en privacyregelgeving.*[173] Het onderwerp wordt nader toegelicht in de paragraaf 'Overig': *Als onderdeel van het speerpunt Beheersing van de IT-omgeving wordt ook weer aandacht besteed aan informatiebeveiliging. Medio 2015 heeft de directie een nieuw informatiebeveiligingsbeleid vastgesteld.*
*De actuele stand van zaken wordt bijgehouden in een zogenaamd monitoringtool. Diverse aanvullende maatregelen zijn inmiddels getroffen, waaronder een penetratietest van het IT-netwerk en het actualiseren van autorisaties tot systemen. In 2016 staan onder meer de uitwijk van informatiesystemen en het verbeteren van incidentdetectie en –preventie op het programma.*[174]

*Ambtelijke P&C-cyclus*

De basis voor de ambtelijke planning en control cyclus van informatieveiligheid is het jaarplan informatieveiligheid. Dit jaarplan is een onderdeel van het Werkplan I&A: het gezamenlijke werkplan van het cluster Informatiemanagement en bureau Automatisering. Het Werkplan I&A, inclusief het jaarplan

[169] Provincie Flevoland (2015), Jaarstukken 2014, p.129-130.
[170] Provincie Flevoland (2014), Mededeling Bestuurlijke eindrapportage Interne Beheersing, 25 november 2014.
[171] Provincie Flevoland (2014), www.flevoland.nl.
[172] Provincie Flevoland (2015), Perspectiefnota 2015-2019; Zomernota 2015.
[173] Provincie Flevoland (2015), Programmabegroting 2016, p.101.
[174] Provincie Flevoland (2015), Programmabegroting 2016, p.101.

informatieveiligheid, wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, incidenten en de uitkomst van de monitoringtool.[175] Na de bijstelling wordt het Werkplan I&A ambtelijk vastgesteld, waarna het wordt besproken in en indien nodig geamendeerd door de IT-raad en vervolgens aan de directie gezonden. De IT-raad bewaakt de voortgang van het Werkplan I&A.[176] Andere organisatie-eenheden dan het cluster Informatiemanagement en bureau Automatisering, hebben informatieveiligheid niet in hun afdelings-/werkplannen opgenomen en verantwoorden niet over informatieveiligheid.[177]

De adviseur informatieveiligheid bespreekt in het tweewekelijks bilateraal overleg met de accounthouder / teamleider cluster Informatiemanagement en in het maandelijkse bilateraal overleg met het afdelingshoofd MO de voortgang op het gebied van informatieveiligheid.[178] Het jaarplan informatieveiligheid met daarin de speerpunten op het gebied van informatieveiligheid dient als basis voor de bilaterale overleggen. Daarnaast hebben zowel het afdelingshoofd MO als de adviseur informatieveiligheid regelmatig bilateraal overleg met het directielid met bedrijfsvoering in de portefeuille.[179]

Er is ook een controleplan dat is gericht op informatieveiligheid: het Intern Controle Plan Informatieveiligheid (ICP).[180] Het doel van het ICP is om te kunnen vaststellen of juist, volledig en/of tijdig wordt voldaan aan de beleidsuitgangspunten. Het ICP wordt elk jaar door de directie vastgesteld.[181] In het ICP staan de specifieke interne controles (SIC's) die periodiek worden uitgevoerd. Het ICP 2016 bevat een dynamische meerjarenplanning 2016-2019. Hiervan kan zowel de inhoud als de prioriteit worden bijgesteld aan de hand van de actualiteit. De te controleren maatregelen komen voort uit de resultaten van de monitoringtool (zie paragraaf 0 voor een toelichting daarop), en door de directie, afdelingshoofden en medewerkers aangedragen onderwerpen. Voor elke te controleren maatregel zijn op basis van de IBI de doelstelling, aandachtspunten en de frequentie van de controle benoemd. Ambtelijk is aangegeven dat de uitvoering van het ICP 2016 vanwege capaciteitsgebrek in het eerste kwartaal van 2016 nog niet is gestart.[182]

Voor 2016 is een detailplanning opgesteld. De SIC-werkzaamheden worden gedocumenteerd vastgelegd zodat ze navolgbaar en bruikbaar zijn voor de accountant en het management. De controles worden door de adviseur informatieveiligheid uitgevoerd. De uitkomsten van deze werkzaamheden worden samengevat in een controleverslag dat eerst met betrokkenen wordt besproken en vervolgens bij de directie ter besluitvorming wordt aangeboden.

Het plan is om vanaf 2016 één controleplan te maken voor de afdeling MO, bestaande uit de verbijzonderde interne controle, de fiscale controles en de controles op informatieveiligheid.[183]

[175] Provincie Flevoland (2015), Informatiebeveiligingsbeleid Provincie Flevoland, Versie 1.0, p.7; ambtelijk interview, 11 februari 2016.
[176] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[177] Provincie Flevoland, ambtelijk interview, 14 december 2015.
[178] Provincie Flevoland, e-mail 10 maart 2016.
[179] Provincie Flevoland, ambtelijk interview, 11 januari 2016.
[180] Provincie Flevoland (2016), Intern Controleplan Informatieveiligheid 2016.
[181] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[182] Provincie Flevoland, aanvullende informatie, 26 april 2016.
[183] Provincie Flevoland, ambtelijk interview, 8 december 2015.

## 5.2 Onafhankelijke toets op informatieveiligheid

**Criterium 9**

*De provincie laat periodiek een onafhankelijke toets uitvoeren op de informatieveiligheid.*

Toelichting op het criterium

Het principe van verplichtende zelfregulering houdt ook in dat de provincie via onafhankelijke onderzoeken laat toetsen of de informatieveiligheid op orde is. In het convenant staat daarover dat onafhankelijk onderzoek bijdraagt aan het creëren van grotere transparantie over informatieveiligheid. Hierdoor is zonder extra regeldruk elke provincie aanspreekbaar op haar beveiligingsniveau.[184]

De Rekenkamer heeft onderzocht of de provincie onafhankelijke onderzoeken heeft uitgevoerd naar het beveiligingsniveau en de implementatiestatus van het informatieveiligheidsbeleid. Er is nagegaan hoe onafhankelijk deze onderzoeken waren. Ook is onderzocht of de bevindingen van deze onderzoeken met bestuur en management zijn besproken, welke acties hieruit zijn voortgekomen en hoe de voortgang van deze acties wordt bijgehouden.

**Bevinding 9**

De provincie heeft in 2014/2015 verschillende onafhankelijke onderzoeken naar de informatieveiligheid laten uitvoeren: een penetratietest op de IT-infrastructuur, een penetratietest op het netwerk van bruggen en sluizen en een onderzoek naar de status en voortgang van het project informatieveiligheid in relatie tot het kader van de Verplichtende Zelfregulering. De onderzoeken zijn in opdracht van de directie uitgevoerd door externe partijen en begeleid door de adviseur informatieveiligheid. De bevindingen van de onderzoeken hebben geleid tot acties ter verbetering van de informatieveiligheid. De voortgang op deze acties wordt gemonitord door de adviseur informatieveiligheid en besproken met het management.

Toelichting op de bevinding

De provincie heeft in 2014/2015 de volgende onafhankelijke onderzoeken laten uitvoeren naar informatieveiligheid:

- Een penetratietest op de IT-infrastructuur
- Een penetratietest op het netwerk van bruggen en sluizen
- Een penetratietest op de website www.flevoland.nl en intranet.[185]
- Onderzoek naar de huidige status en voortgang van het project informatieveiligheid binnen de provincie in relatie tot het kader van de Verplichtende Zelfregulering

*Penetratietesten*[186]

De eerste twee penetratietesten zijn in april 2015 in opdracht van de directie uitgevoerd door een extern specialist. De eerste penetratietest heeft plaatsgevonden op de externe web-omgeving, de kantoorautomatisering en het wifi-netwerk. De tweede penetratietest is uitgevoerd op de software van de afstandsbediening van bruggen en sluizen. In totaal zijn tijdens deze twee onderzoeken 45 kwetsbaarheden geïdentificeerd, waarvan 6 met een

[184] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid.
[185] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.
[186] Provincie Flevoland (2015), Werkplan I&A 2015-2016, p.15.

zeer hoog risico, 17 met een hoog risico, 19 met een gemiddeld risico en 3 met een laag risico.[187] De derde penetratietest is in november 2015 uitgevoerd.[188]
Op basis van de resultaten van de penetratietesten is een plan van aanpak vastgesteld door de directie. Per bevinding is een actie gedefinieerd en een einddatum vastgesteld, waarbij voor één bevinding met een laag risico een bewuste keuze is gemaakt deze niet verder op te pakken.[189] Bijna alle acties zijn inmiddels uitgevoerd, onder coördinatie van de adviseur informatieveiligheid.[190]

*Onderzoek naar status en voortgang project informatieveiligheid in relatie tot de Verplichtende Zelfregulering*[191]
Dit onderzoek naar de voortgang en stand van zaken op de vier kernaspecten uit het convenant is in opdracht van de directie uitgevoerd door een extern bureau in de periode augustus – september 2015. De coördinatie en begeleiding van het onderzoek heeft plaatsgevonden door de adviseur informatieveiligheid. De onderzoeksvraag is als volgt geformuleerd: *"Evalueer de huidige status en voortgang van het project Informatieveiligheid binnen de provincie Flevoland in relatie tot het kader van de Verplichtende Zelfregulering. Rapporteer hierbij over de status, geconstateerde aandachtpunten en aanbevelingen op niveau van het project".*
In het onderzoeksrapport wordt geconstateerd dat er goede progressie wordt gemaakt met het project. Tegelijkertijd is er ook voldoende ruimte voor verbetering.

De resultaten van het onderzoek zijn besproken door de directie op 17 december 2015.[192] De directie heeft besloten om de vijf belangrijkste maatregelen te gaan uitvoeren. Deze maatregelen worden conform het directiebesluit opgenomen in het Werkplan I&A 2016-2017. Daarnaast neemt de adviseur informatieveiligheid ze ook op in de monitor zelfevaluatie (deze wordt nader toegelicht in paragraaf 0). Op deze manier zijn ze onderdeel van het centrale overzicht van maatregelen, waardoor ze niet worden vergeten en de uitvoering ervan kan worden gemonitord.[193] De adviseur informatieveiligheid bespreekt zijn bevindingen over de voortgang met de betreffende inhoudelijk verantwoordelijke medewerker en legt de bevindingen van zijn monitor-activiteiten ook voor aan zijn direct leidinggevende en het afdelingshoofd MO.[194]

## 5.3 Uitvoering van een zelfevaluatie

**Criterium 10**
*De provincie voert een zelfevaluatie uit.*

Toelichting op het criterium
In het convenant is afgesproken dat elke provincie de interprovinciale monitor informatieveiligheid (monitoringtool) gebruikt als instrument voor zelfevaluatie. Deze monitor is ontwikkeld voor het Cibo en brengt in beeld hoe de informatieveiligheid van een provincie zich verhoudt tot het basisniveau uit de IBI. De monitor wordt ingevuld door

[187] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[188] Provincie Flevoland, reactie op feitelijk wederhoor, 17 mei 2016.
[189] Provincie Flevoland (2015), Nota Besluitvorming directieteam: Resultaten en aanpak penetratietest bruggen & sluizen en kantoorautomatisering, 12 augustus 2015.
[190] Provincie Flevoland, ambtelijk interview, 8 december 2015.
[191] Provincie Flevoland en BDO IT Audit & Security (2015), Onderzoek informatieveiligheid, rapportage onderzoek voortgang project 'Zelfregulering Informatieveiligheid'.
[192] Provincie Flevoland (2015), Nota Besluitvorming directieteam: BDO Onderzoek Informatieveiligheid, 30 november 2015.
[193] Provincie Flevoland, ambtelijk interview, 11 februari 2016.
[194] Provincie Flevoland, e-mail 10 maart 2016.

de provincie zelf en is voor de provincie van belang om een inschatting te maken van sterke en zwakke punten van de informatieveiligheid.
In paragraaf 3.2.1 is aangegeven dat de generieke en aanvullende maatregelen uit de IBI zijn ingedeeld in elf categorieën, die betrekking hebben op de aandachtsgebieden mens & organisatie, basisinfrastructuur en ICT. In de monitoringtool van het Cibo wordt binnen deze categorieën per maatregel een oordeel gegeven over de stand van zaken met betrekking tot de opzet, het bestaan en de werking van de maatregel:

- Opzet: er is vastgesteld beleid ten aanzien van de maatregel;
- Bestaan: de maatregel is geïmplementeerd;
- Werking: de maatregel werkt structureel en is aantoonbaar.[195]

Het oordeel wordt gegeven door middel van een cijfer 1 tot en met 4. De betekenis van deze cijfers is weergegeven in Tabel 7.

**Tabel 7 Toelichting monitoringtool Cibo**

| Oordeel | Opzet: vastgesteld beleid | Bestaan: maatregel is geïmplementeerd | Werking: maatregel werkt structureel en is aantoonbaar |
|---|---|---|---|
| 1 | Niets voorhanden | Beleid is geaccordeerd door MT | Beleid/proces wordt incidenteel gevolgd |
| 2 | Beleid is 33% gereed | Beleid is voor 33% geïmplementeerd | Beleid/proces wordt circa 33% gevolgd |
| 3 | Beleid is 66% gereed | Beleid is voor 66% geïmplementeerd | Beleid/proces wordt circa 66% gevolgd |
| 4 | Beleid is 100% gereed | Beleid is voor 100% geïmplementeerd | Proces wordt structureel 100% gevolgd |

De Rekenkamer is nagegaan of de provincie deze zelfevaluatie monitor daadwerkelijk heeft uitgevoerd. En als dit het geval is, of de resultaten van deze monitor zijn besproken met het management, welke acties daaruit zijn voortgekomen en of deze ook zijn uitgevoerd.

**Bevinding 10**

De provincie heeft de interprovinciale monitor zelfevaluatie voor zowel 2014 als voor 2015 uitgevoerd. Voor nagenoeg alle maatregelen heeft de provincie ook acties gedefinieerd. De monitor is in 2015 geactualiseerd ten opzichte van de monitorresultaten in 2014, waardoor de voortgang zichtbaar is.

Aan de hand van de resultaten van de monitor zelfevaluatie 2014 en 2015 zijn op basis van een risico-inschatting de belangrijkste risico's benoemd en gecategoriseerd als 'hoog' of 'midden'. De bevindingen van zowel de monitor 2014 als 2015 zijn door de IT-raad en de directie besproken. Voor beide jaren geldt dat de uit de monitor voortkomende maatregelen die zijn geformuleerd bij de risico's van de categorie 'hoog' en 'midden', zijn opgenomen in het Werkplan van I&A en dat de uitvoering van de maatregelen wordt gemonitord.

Toelichting op de bevinding

*De wijze waarop de resultaten van de interprovinciale monitor zelfevaluatie tot stand komen*
Sinds zijn aanstelling vult de adviseur informatieveiligheid jaarlijks de interprovinciale monitor zelfevaluatie in.[196] Het doel van de meting is het "*krijgen van een globaal inzicht in het basisbeveiligingsniveau (beschikbaarheid,*

[195] Provincie Zuid-Holland (2014), Monitoringtool Cibo.
[196] Provincie Flevoland, ambtelijke interviews, 8 december 2015 en 11 februari 2016.

*integriteit en vertrouwelijkheid) van de provincie*".[197] Voor elk van de 133 maatregelen die zijn opgenomen in de monitor, heeft de adviseur informatieveiligheid voor zowel de 'opzet', het 'bestaan' en de 'werking' van elke maatregel een oordeel gegeven over de stand van zaken op de schaal van 1 tot en met 4. De monitor biedt voor elke maatregel ruimte voor opmerkingen bij of een toelichting op het gegeven oordeel. Hiervan is gebruik gemaakt. Bij elk van de 133 maatregelen heeft de adviseur informatieveiligheid opmerkingen geplaatst die relevant zijn voor de beoordeling van de stand van zaken.[198]

Het oordeel en de toelichting daarop worden gegeven op basis van een inschatting van de adviseur informatieveiligheid. Deze inschatting maakt hij door op basis van de IBI en het Informatiebeleid van de Taskforce, gerichte vragen te stellen aan elk van de verantwoordelijken voor de uitvoering van de betreffende maatregel[199] en door een enkele rapportage die hij ontvangt, zoals de incidentrapportage.[200]

Naast de ruimte voor opmerkingen of een toelichting, geeft de monitor bij elk van de maatregelen ook ruimte voor het formuleren van acties. Ook hiervan heeft de provincie gebruik gemaakt. Nagenoeg voor elk van de 133 maatregelen die minder dan 100% scoren op de 'opzet', het 'bestaan' of de 'werking' ervan, is een actie geformuleerd.[201]

*Monitor zelfevaluatie 2014*

In de monitor 2014 is voor elke categorie de totale score van de opzet, het bestaan en de werking van de maatregelen opgeteld, waardoor een totaalbeeld ontstaat van de score op de verschillende categorieën. Uit dit totaalbeeld blijkt dat de provincie van de elf categorieën het beste scoort op de categorieën 'beheer van bedrijfsmiddelen', 'fysieke beveiliging en beveiliging van de omgeving' en 'beveiliging van personeel'. Van de elf categorieën scoort de provincie het laagst op 'bedrijfscontinuïteitsbeheer', 'informatieveiligheidsbeleid', 'naleving' en 'organisatie'.[202]

Echter, deze scores geven geen indicatie voor het risico dat optreedt wanneer een maatregel niet of deels is uitgevoerd. Om maatregelen te kunnen prioriteren is de monitor 2014 daarom door de adviseur informatieveiligheid aangevuld met een risico-inschatting en -afweging.[203] De aanbevelingen uit de Interim Controle 2014 van PWC met betrekking tot het aandachtspunt 'logische toegangsbeveiliging' en autorisatiematrices, zijn daarbij ook meegenomen.[204] Op basis van de risico-inschatting en –afweging zijn vijftien risico's gelabeld als 'hoog'. De uitkomsten van de risico-inschatting en –afweging zijn door de adviseur informatieveiligheid afgestemd met relevante contactpersonen binnen zowel de afdeling MO als de afdeling SenM.[205]

---

[197] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab 'Toelichting'; provincie Flevoland (2016), Monitor Baseline Implementatie 2016, tab 'Toelichting'.

[198] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab 'Baseline implementatie'; provincie Flevoland (2016), Monitor Baseline Implementatie 2016, tab 'Baseline implementatie'

[199] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab 'Toelichting'; ambtelijke interviews, 8 december 2015 en 11 februari 2016.

[200] Provincie Flevoland (2016), Aantal Beveiligingsincidenten 2015: per jaar, per maand, grafiek; ambtelijk interview, 11 februari 2016.

[201] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014 [#1657065], tab 'Baseline implementatie'; provincie Flevoland (2016), Monitoringtool Informatiebeveiliging provincie Flevoland 2015, tab 'Baseline implementatie'.

[202] Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014, tab 'Ambitieniveau vs. realisatie'

[203] Provincie Flevoland, ambtelijk interview, 11 februari 2016.

[204] Provincie Flevoland (2014), Rapportage interim bevindingen controle 2014, PWC.

[205] Provincie Flevoland (2014), Memo Monitoringtool Informatiebeveiliging provincie Flevoland 2014, van Afdeling Management Ondersteuning aan IT-raad, 12 november 2014, p.1.

*Monitor zelfevaluatie 2015*

De provincies hadden afgesproken de interprovinciale monitor zelfevaluatie jaarlijks in te vullen. Dit hebben zij tot en met 2014 gedaan. Omdat de provincies binnen het Cibo werken aan een nieuwe IBI, die binnenkort wordt aangeboden, heeft het Cibo besloten om in 2015 de monitor op basis van de oude IBI niet meer te gebruiken. De provincies konden er wel zelf voor kiezen om deze monitor in te vullen. Op het moment dat de nieuwe IBI geldt, zal het Cibo mogelijk aansturen op het opstellen van een nulmeting op basis van deze nieuwe IBI.[206]

Een aantal provincies heeft naar aanleiding van deze bespreking besloten om de monitoringtool voor 2015 niet meer in te vullen. Echter, de provincie gebruikt de monitoringtool ook als intern overzichts- en monitorinstrument en heeft daarom de monitoringtool ook voor 2015 ingevuld.

*Opvolging van de uitkomsten van de monitor*

De aangegeven prioritering die heeft plaatsgevonden bij de monitorresultaten uit 2014 heeft geleid tot een lijst van vijftien onderwerpen met een hoge risico-inschatting, waarop een toelichting wordt gegeven en per onderwerp acties worden voorgesteld. De IT-Raad heeft hiervoor vijftien aanbevelingen geformuleerd, waarop de directie op 10 december 2014 heeft besloten dat deze in 2015 moeten worden opgepakt. De aanbevelingen zijn opgenomen in het Werkplan I&A.[207]

Net zoals bij de monitor 2014 heeft ook bij de monitor 2015 een prioritering plaatsgevonden. Het resultaat van deze prioritering is dat er elf speerpunten zijn benoemd: vier onderwerpen met een hoog risico en zeven onderwerpen met een midden risico. Deze uitkomsten van de monitor 2015 zijn achtereenvolgens in het Intaketeam, de IT-raad en op 16 december 2015 door de directie besproken.[208] De directie heeft besloten om alle vier de maatregelen met een hoog risico en de zeven maatregelen met een gemiddeld risico op te pakken in 2016.[209] Deze maatregelen zijn opgenomen in het Werkplan I&A 2016-2017.[210]

Voor de maatregelen die voortkomen uit de monitor 2014 en 2015 en zijn opgenomen in de Werkplannen van I&A, geldt dat de adviseur informatieveiligheid de uitvoering ervan monitort. Hij bespreekt zijn bevindingen met de betreffende inhoudelijk verantwoordelijke medewerker en legt de bevindingen van zijn monitor-activiteiten ook voor aan zijn direct leidinggevende en de afdelingsmanager MO. Op deze manier wordt gewerkt met een ‘ acht ogen principe’.[211]

[206] Provincie Zuid-Holland (2016), e-mail 8 februari 2016 van een Cibo-lid vanuit Zuid-Holland.
[207] Provincie Flevoland (2014), Memo directieteam, Uitkomsten monitoringtool informatiebeveiliging provincie Flevoland 2014; Werkplan I&A 2015-2016, p. 14.
[208] Provincie Flevoland, e-mail 10 maart 2016.
[209] Provincie Flevoland (2015), Nota Besluitvorming directieteam: Uitkomsten monitoringtool informatiebeveiliging provincie Flevoland 2015.
[210] Provincie Flevoland, Concept Werkplan I&A 2016-2017.
[211] Provincie Flevoland, e-mail 10 maart 2016.

# Bijlage A Geraadpleegde bronnen

***Algemeen***


- Castells, M. (1996), The information Age: Economy, Society, and Culture
- Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
- Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
- Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid
- Hoffmann B.V. (2016), Onderzoek i.o.v. Randstedelijke Rekenkamer naar Informatieveiligheid bij de provincie Flevoland, Managementrapport nr. 21509118.
- Norea (2015), Handreiking ICT-beveiligingsassessments DigiD door RE's
- Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
- Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
- Provincie Zuid-Holland (2014), Monitoringtool Cibo
- Rekenkamer Den Haag (2014), Digitale Veiligheid


***Websites***


- Autoriteit Persoonsgegevens (2016), www.autoriteitpersoonsgegevens.nl
- Eerste Kamer der Staten-Generaal (2016), www.eerstekamer.nl
- FOX-IT (2015), www.fox-it.nl
- Informatiebeveiligingsdienst (IBD) gemeenten, www.ibdgemeenten.nl
- iBewustzijn Overheid (2015), www.ibewustzijnoverheid.nl
- Justitia.nl (2016), www.justitia.nl
- Logius (2016), www.logius.nl
- Taskforce BID (2015), www.taskforcebid.nl


***Provincie Flevoland***


- Provincie Flevoland, Bruikleenovereenkomst iPad
- Provincie Flevoland, Concept Werkplan I&A 2016-2017
- Provincie Flevoland, Monitor Baseline Implementatie 2016
- Provincie Flevoland (2012), Informatie in Beweging: Ontwikkeling van de informatievoorziening in de provincie Flevoland 2012-2015
- Provincie Flevoland (2014), BIA Financiële Systeem
- Provincie Flevoland (2014), Concept Besluitenlijst vergadering GS
- Provincie Flevoland (2014), Nota Besluitvorming GS instemmen met convenant informatiebeveiliging
- Provincie Flevoland (2014), Verslag directievergadering 19 november 2014
- Provincie Flevoland (2014), Projectplan Implementeren proces verplichtende zelfregulering Informatieveiligheid
- Provincie Flevoland (2014), Projectplan Bewustwordingscampagne Informatieveiligheid provincie Flevoland
- Provincie Flevoland (2014), Mededeling Bestuurlijke eindrapportage Interne Beheersing
- Provincie Flevoland (2014), Monitoringtool Informatiebeveiliging provincie Flevoland 2014
- Provincie Flevoland (2014), Memo directieteam: Uitkomsten monitoringtool informatiebeveiliging provincie Flevoland 2014
- Provincie Flevoland (2014), Rapportage interim bevindingen controle 2014 (PWC)
- Provincie Flevoland (2015), Activiteitenplan Bewustwording Informatieveiligheid

- Provincie Flevoland (2015), Afdelingsplan BDO 2015
- Provincie Flevoland (2015), Beleidsuitgangspunten wachtwoordbeleid van provincie Flevoland
- Provincie Flevoland (2015), Beleidsuitgangspunten Clean Deskbeleid van provincie Flevoland
- Provincie Flevoland (2015), Beleidsuitgangspunten logische toegangsbeleid van provincie Flevoland
- Provincie Flevoland (2015), Beleidsuitgangspunten beveiliging webapplicaties van provincie Flevoland
- Provincie Flevoland (2015), Controle Beleidsuitgangspunten clean desk bij Afdeling Managementondersteuning
- Provincie Flevoland (2015), Controle fysieke toegang provincie Flevoland
- Provincie Flevoland (2015), Managementreactie controle fysieke toegang
- Provincie Flevoland (2015), Actieplan opvolging controle fysieke toegang
- Provincie Flevoland (2015), Eerste halfjaarsrapportage Informatieveiligheid provincie Flevoland
- Provincie Flevoland (2015), Jaarstukken 2014
- Provincie Flevoland (2015), Perspectiefnota 2015-2019
- Provincie Flevoland (2015), Zomernota 2015
- Provincie Flevoland (2015), Programmabegroting 2016
- Provincie Flevoland (2015), Nota Besluitvorming directieteam: resultaten en aanpak penetratietest bruggen en sluizen en kantoorautomatisering
- Provincie Flevoland (2015), Verslag directievergadering 20 mei 2015
- Provincie Flevoland (2015), Werkplan I&A 2015-2016
- Provincie Flevoland (2015), Informatiebeveiligingsbeleid provincie Flevoland, versie 1.0
- Provincie Flevoland (2015), Presentatie Informatieveiligheid voor GS
- Provincie Flevoland (2015), Presentatie Informatieveiligheid Managementberaad
- Provincie Flevoland (2015), Presentatie Verbetertraject Informatieveiligheid
- Provincie Flevoland (2015), Presentatie Bewustwording Informatieveiligheid voor de managementteams
- Provincie Flevoland en BDO IT Audit & Security (2015), Onderzoek Informatieveiligheid, rapportage onderzoek voortgang project ‘ Zelfregulering Informatieveiligheid’
- Provincie Flevoland (2015), Nota Besluitvorming Directieteam: BDO Onderzoek Informatieveiligheid
- Provincie Flevoland (2015): Nota Besluitvorming Directieteam: Uitkomsten monitoringtool informatiebeveiliging provincie Flevoland 2015
- Provincie Flevoland (2015), Projectplan Beveiliging Persoonsgegevens
- Provincie Flevoland (2015), Notitie Definities systeem-, gegevens- en documenteigenaar aan IT-Raad
- Provincie Flevoland (2015), Oplegmemo systeemeigenaarschap aan IT-Raad
- Provincie Flevoland (2015), Nota Besluitvorming directieteam: Uitkomsten monitoringtool informatiebeveiliging provincie Flevoland 2015
- Provincie Flevoland (2016), Aantal Beveiligingsincidenten 2015
- Provincie Flevoland (2016), Activiteitenplan GRC-tooling
- Provincie Flevoland (2016), Activiteitenplan ISMS-Processen - Kwaliteitssysteem
- Provincie Flevoland (2016), Intern Controleplan Informatieveiligheid provincie Flevoland
- Provincie Flevoland (2016), Monitoringtool Informatiebeveiliging provincie Flevoland 2015
- Provincie Flevoland (2016), Voorstel verbeterde invulling rol adviseur Informatieveiligheid
- Provincie Flevoland (2016), Archivering en beveiliging persoonsgegevens, memo van afdeling MO aan directie
- Provincie Flevoland (2016), Gedragscode ambtelijke integriteit provincie Flevoland
- Provincie Flevoland (2016), Conceptverslag directievergadering 29 juni 2016

***Websites provincie Flevoland***

- www.flevoland.nl

# Bijlage B Geraadpleegde personen

***Algemeen***

| | |
|---|---|
| Dhr. T. Bosma | Senior Onderzoeker Rekenkamer Den Haag |
| Dhr. H. Wesseling | Voormalig Hoofd Taskforce Bestuur en Informatieveiligheid Dienstverlening |
| Dhr. D. Leguit | Voormalig Manager Taskforce Bestuur en Informatieveiligheid Dienstverlening |

***Provincie Flevoland***

| | |
|---|---|
| Dhr. R. Kalk | Senior Statenadviseur |
| Dhr. J. Karens | Senior Statenadviseur (tijdelijk) |
| Dhr. O. de Meij | Afdelingshoofd Services en Middelen |
| Mevr. M. Overmars | Directielid |
| Dhr. M. Rijsberman | Gedeputeerde Communicatie en ICT |
| Mevr. A. Spijker | Accounthouder / Teamleider Cluster Informatiemanagement |
| Dhr. R. Terbijhe | Adviseur informatieveiligheid |
| Dhr. W. Timmers | Afdelingshoofd Managementondersteuning |
| Dhr. W. Van de Veen | Bureauhoofd Automatisering |

# Bijlage C Afkortingen en begrippen

***Afkortingen***

| | |
|---|---|
| **BIA** | Business Impact Analyse |
| **BIV** | Beschikbaarheid, integriteit, vertrouwelijkheid |
| **Cibo** | Centraal Informatiebeveiligingsoverleg |
| **CISO** | Chief Information Security Officer |
| **GRC** | Governance, Risk & Compliance |
| **GS** | Gedeputeerde Staten |
| **I&A** | Informatisering & Automatisering |
| **IBI** | Interprovinciale Baseline Informatiebeveiliging |
| **ICP** | Intern Controle Plan Informatieveiligheid |
| **ICT** | Informatie- en Communicatietechnologie |
| **IPO** | Interprovinciaal Overleg |
| **ISMS** | Information Security Management System |
| **MAB** | Meerjaren Aanpak Bedrijfsvoering |
| **MO** | Afdeling Managementondersteuning |
| **NCSC** | Nationaal Cyber Security Centrum |
| **OWASP** | Open Web Application Security Project |
| **P&C** | Planning & Control |
| **P&O** | Cluster Personeel & Organisatie |
| **PS** | Provinciale Staten |
| **SenM** | Afdeling Services en Middelen |
| **SIC** | Specifieke interne controles |
| **SIO** | Strategisch Informatie Overleg |

***Begrippen***

| | |
|---|---|
| **Aanvullende maatregelen** | Het bedrijfsproces of informatiesysteem waarvoor een risicoanalyse wordt uitgevoerd (zie: Risicoanalyse) krijgt een classificatie op het niveau van beschikbaarheid, integriteit en vertrouwelijkheid. Op basis hiervan selecteert de provincie aanvullende maatregelen uit de IBI die genomen moeten worden ter verbetering van de informatieveiligheid. |
| ***Basisinfrastructuur*** | Basisinfrastructuur is één van de aandachtsgebieden van informatieveiligheid. Basisinfrastructuur betreft o.a. de elektriciteits-voorziening, telecommunicatievoorzieningen en gebouwen en toegang. |
| ***Beschikbaarheid*** | In het kader van informatieveiligheid betreft beschikbaarheid de eigenschap dat informatie toegankelijk en bruikbaar is op verzoek van een bevoegde functionaris. |

| | |
|---|---|
| ***BIA*** | De BIA is de standaardmethode voor het uitvoeren van een risicoanalyse (zie: Risicoanalyse). |
| ***Cibo*** | Het Cibo is onderdeel van het IPO. Het is een platform waarin provincies kennis en ervaring uitwisselen en de gezamenlijke ontwikkeling van informatieveiligheid vormgeven. |
| ***Convenant Interprovinciale Regulering Informatieveiligheid*** | Het convenant Interprovinciale Regulering Informatieveiligheid is een afsprakenkader waarmee provincies verantwoordelijkheid nemen voor het opstellen van het informatieveiligheidsbeleid en het uitvoeren en handhaven ervan. Het is de bedoeling dat de provincies op deze manier één standaard ontwikkelen en behouden. |
| ***Generieke maatregelen*** | Alle maatregelen uit de IBI die als generiek zijn gecategoriseerd. Deze maatregelen geven het basisniveau van beschikbaarheid, integriteit of vertrouwelijkheid aan, waaraan elke provincie moet voldoen. |
| ***IBI*** | De IBI vormt het formele basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. De IBI geeft een standaard werkwijze waarmee per bedrijfsproces of informatiesysteem wordt bepaald welke beveiligingsmaatregelen getroffen moeten worden. |
| ***ICT*** | In het kader van informatieveiligheid betreft ICT het aandachtsgebied applicaties en gegevensverzameling, ICT infrastructuur (computers, netwerkapparatuur en randapparatuur) en ICT programmatuur (besturingsprogramma's). |
| ***Integriteit*** | In het kader van informatieveiligheid betreft integriteit de eigenschap dat de nauwkeurigheid en volledigheid van bedrijfsmiddelen wordt beveiligd. De informatie is juist, up-to-date, volledig en niet gecorrumpeerd. |
| ***ISO 27001/27002*** | De IBI is gebaseerd op de landelijke standaard ISO 27001/27002 (voluit: NEN-ISO/IEC-27001/27002). Dit wordt ook wel de code van informatiebeveiliging genoemd, waarin de eisen ten aanzien van informatieveiligheid zijn geformuleerd. |
| ***Mens en organisatie*** | In het kader van informatieveiligheid betreft Mens en Organisatie het aandachtsgebied dat gaat om werkwijzen, zoals manieren, routines, gewoonten en gedrag. |
| ***Penetratietest*** | Een penetratietest is een geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken, waarbij een beveiligingsspecialist probeert om zónder de vereiste toegangsgegevens informatie te verkrijgen uit het systeem. Het doel is om inzicht te krijgen in de risico's en kwetsbaarheden van het onderzochte systeem. |

| | |
|---|---|
| ***Risicoanalyse*** | Volgens de IBI dient elke provincie een risicoanalyse uit te voeren op bedrijfsprocessen en informatiesystemen die verhoogd risico lopen. De provincie maakt deze selectie zelf. Op basis van de risicoanalyse krijgt het bedrijfsproces of informatiesysteem een classificatie op het niveau van beschikbaarheid, integriteit en vertrouwelijkheid. |
| ***Verplichtende Zelfregulering*** | In de IBI staat het principe van Verplichtende Zelfregulering centraal, wat betekent dat iedere provincie zelf verantwoordelijk is voor het informatieveiligheidsbeleid, met als stok achter de deur dat wanneer de informatieveiligheid onvoldoende wordt geïntegreerd in de bedrijfsvoering, verplichtingen op basis van (wettelijke) regelgeving zullen volgen. |
| ***Vertrouwelijkheid*** | In het kader van informatieveiligheid betreft vertrouwelijkheid de eigenschap dat informatie niet beschikbaar wordt gesteld of wordt ontsloten aan onbevoegde personen, organisaties of processen. |

# Colofon

**Randstedelijke Rekenkamer**
Teleportboulevard 110
1043 EJ Amsterdam
020 – 58 18 585
info@randstedelijke-rekenkamer.nl
www.randstedelijke-rekenkamer.nl
Volg ons op twitter via: @rekenrandstad
Juli 2016