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

EINDRAPPORT

Informatieveiligheid

Provincie Noord-Holland | juli 2016

Voorwoord

'Aantal meldingen cyberaanvallen op overheid verdubbeld'

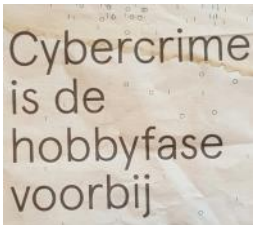
Het aantal gemelde cyberaanvallen op sites en systemen van de overheid is in de afgelopen twee jaar verdubbeld. Het Nationaal Cyber Security Centrum (NCSC) krijgt bijna dagelijks bericht over een aanval. Dat blijkt uit cijfers van het centrum die de Volkskrant heeft opgevraagd.

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



Cybercrime is de hobbyfase voorbij

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 Claudia 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

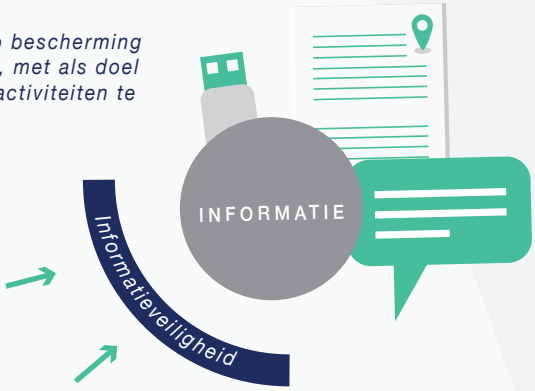
Context

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.

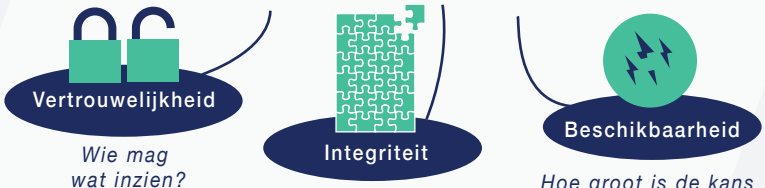
1. Wat is informatieveiligheid?

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?

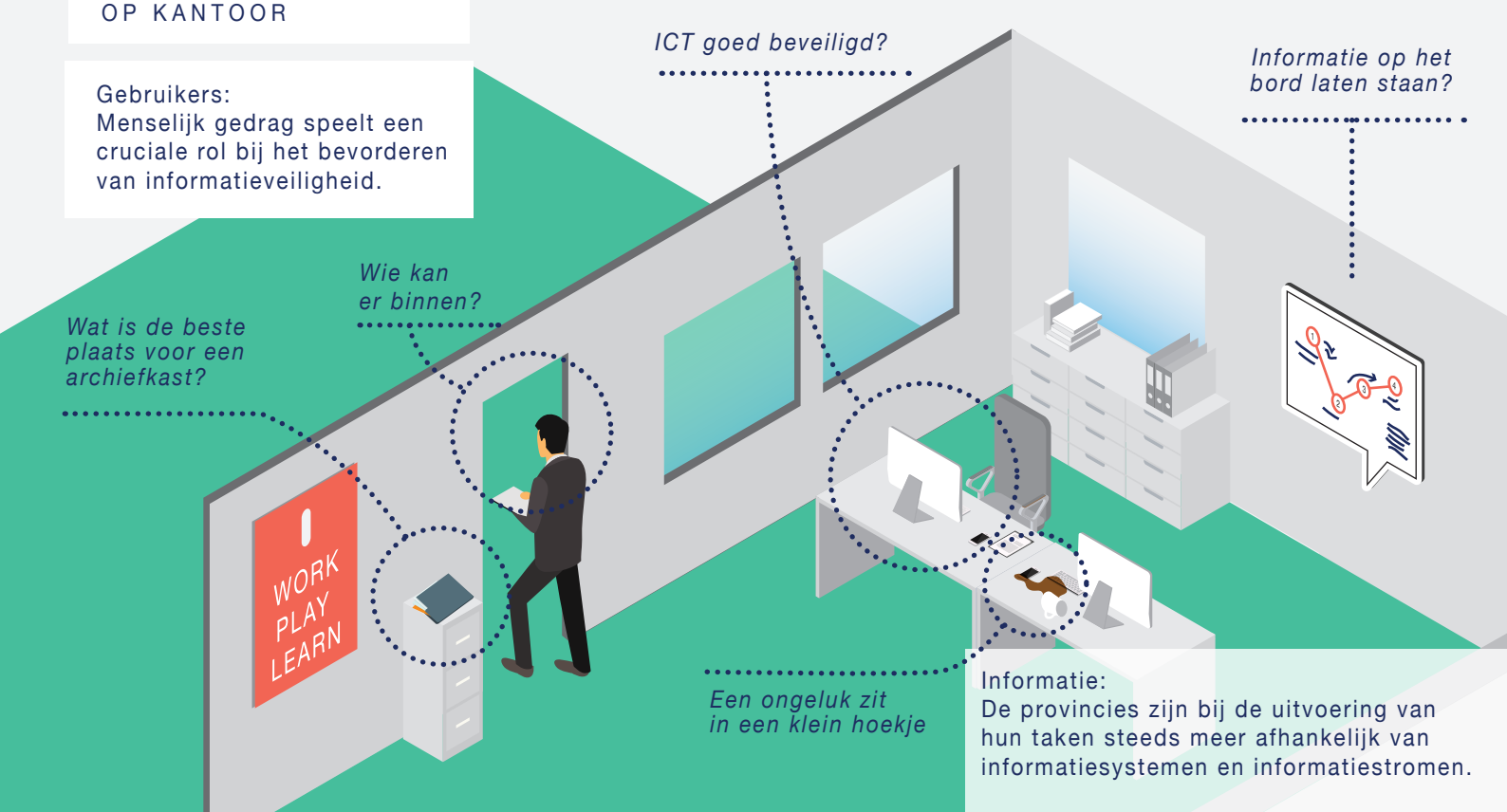
Het doel van informatieveiligheid is om risico's tot een voor de provincie vastgesteld acceptabel niveau terug te brengen.

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

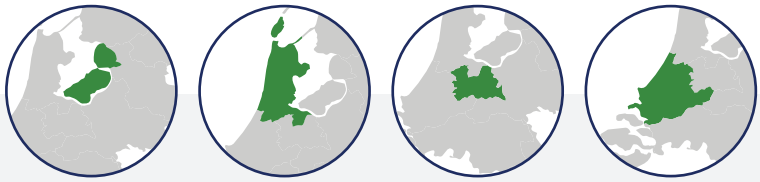
100 procent veiligheid bestaat niet.

INFORMATIEVEILIGHEID OP KANTOOR

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



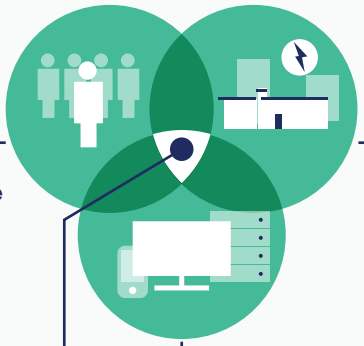
Informatie:
De provincies zijn bij de uitvoering van hun taken steeds meer afhankelijk van informatiesystemen en informatiestromen.



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

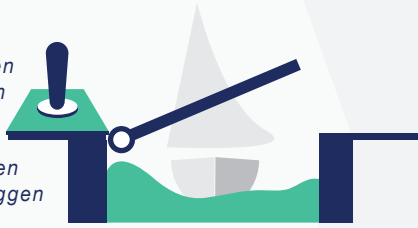
Beschikbaarheid

↓

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 (beschikbaar) is. 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 het stokje 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 Noord-Holland de informatieveiligheid voldoende geborgd?

Conclusie
De provincie besteedt voldoende aandacht aan de bewustwording van het belang van informatieveiligheid binnen de organisatie. Ook heeft de provincie het toezicht op en de verantwoording over informatieveiligheid goed geregeld. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Er is wel verbetering mogelijk in de sturing op het tempo van de implementatie van de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid. Hoewel de provincie veel zaken heeft opgepakt, behoeft de organisatorische verankering en de planmatige aanpak van informatieveiligheid verbetering.

[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.

Sinds 2016 zet de provincie hiertoe wel stappen. Een ander verbeterpunt is de uitvoering van maatregelen om de informatieveiligheid te bevorderen. Het is bijvoorbeeld niet voor alle bedrijfsprocessen duidelijk welke informatieveiligheidsmaatregelen nodig zijn en de provincie heeft geen zicht of de maatregelen daadwerkelijk zijn uitgevoerd.

De 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
Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Zo zijn rollen en verantwoordelijkheden in 2012 vastgesteld. De sturing op het tempo van de besluitvorming en uitvoering ten aanzien van informatieveiligheid kan wel beter. De implementatie van de rollen en verantwoordelijkheden is vertraagd. Hoewel de provincie desondanks veel zaken heeft opgepakt, behoeft de organisatorische verankering en planmatige aanpak van informatieveiligheid verbetering. Sinds begin 2016 zet de provincie stappen met het beleggen van rollen en de invulling van verantwoordelijkheden op het gebied van informatieveiligheid.

Toelichting
De directie neemt beslissingen over onderwerpen op het gebied van informatieveiligheid, bijvoorbeeld over de verbetering van de bewustwording in de organisatie van het belang van informatieveiligheid. Er is wel verbetering mogelijk in de sturing op het tempo van de besluitvorming en de implementatie van de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid. De rollen en verantwoordelijkheden zijn in 2012 vastgesteld, maar de implementatie ervan is vertraagd. De Centrale informatiebeveiligingsfunctionaris, die een centrale rol moet spelen in informatieveiligheid, is bijvoorbeeld nog niet aangesteld. Hoewel de provincie desondanks veel zaken op het gebied van informatieveiligheid heeft opgepakt, behoeft de organisatorische verankering en planmatige aanpak van informatieveiligheid verbetering, zodat alle taken op het gebied van informatieveiligheid volwaardig en structureel kunnen worden uitgevoerd.

De besluitvorming over een nieuw voorstel voor rollen en verantwoordelijkheden op het gebied van informatieveiligheid, waarin ontwikkelingen binnen de organisatie zijn meegenomen, heeft lang geduurd. Het voorstel is in februari 2016 vastgesteld. De belangrijkste verandering is dat de verantwoordelijkheid voor informatieveiligheid wordt belegd over meer functies en dat er een duidelijke scheiding komt tussen kaderstelling, uitvoering en controle. Dit zal moeten leiden tot een goede organisatorische verankering van informatieveiligheid. Op dit moment (mei 2016) wordt het voorstel geïmplementeerd (bevinding 1 en 2).

Aanbeveling 1
Vraag GS om ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld wordt gewerkt.

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

Toelichting
Het informatieveiligheidsbeleid is in 2012 vastgesteld door GS en verwijst naar de Interprovinciale Baseline Informatiebeveiliging (IBI). In 2016 dient een geactualiseerde versie van het informatieveiligheidsbeleid te worden vastgesteld (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.

De provincie coördineert of registreert de uitvoering van de generieke informatieveiligheidsmaatregelen niet. Hierdoor heeft de provincie geen zicht of de generieke maatregelen daadwerkelijk zijn uitgevoerd (bevinding 4). De provincie heeft daarnaast niet voor alle bedrijfsprocessen bepaald of er een risicoanalyse nodig is. In plaats daarvan voert de provincie risicoanalyses uit in het geval van wijziging van een systeem óf voorafgaand aan de implementatie van een nieuw systeem. Hierdoor is niet voor alle bedrijfsprocessen duidelijk welke risico's kunnen optreden en welke informatieveiligheidsmaatregelen daarvoor nodig zijn. De provincie heeft wel het voornemen om in 2016 risicoanalyses uit te voeren op een aantal risicovolle processen (bevinding 5).

De Rekenkamer heeft de praktijktoets met betrekking tot informatieveiligheid in deze provincie niet uitgevoerd (onderzoeksvraag 2c), omdat de provincie zich in de beginfase van het onderzoek in een overgangsfase van de ene naar de andere leverancier van de kantoorautomatisering bevond. In een dergelijke kritieke periode, waarin het systeem substantiële veranderingen ondergaat, wordt het uitvoeren van een praktijktoets afgeraden (bevinding 6).

Aanbeveling 2
Vraag GS om ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld.

Aanbeveling 3
Vraag GS te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

Bewustwording van informatieveiligheid

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

Deelconclusie 3
De provincie heeft voldoende aandacht voor bewustwording van het belang van informatieveiligheid. De provincie heeft onafhankelijke onderzoeken laten verrichten die inzicht geven in de mate van bewustzijn van medewerkers van het belang van informatieveiligheid. De bevindingen van deze onderzoeken zijn gebruikt om het bewustzijn van medewerkers op het gebied van informatieveiligheid te vergroten. In 2015 was het bewustzijn van medewerkers verbeterd ten opzichte van 2013.

Toelichting
Technische maatregelen alleen zijn ontoereikend om informatieveiligheid te waarborgen. Ook het gedrag van mensen is daarbij van belang. Bijlagen van niet-bekende mailafzenders openen, onbekenden zonder toegangspas laten meelopen en het voeren van vertrouwelijke gesprekken in openbare ruimtes zijn voorbeelden van gedrag dat risico's oplevert voor de informatieveiligheid. Daarom is het van belang dat alle medewerkers zich bewust zijn van hun rol bij het bevorderen van de informatieveiligheid.

De provincie heeft hier voldoende aandacht aan besteed. In 2013 en 2015 heeft de provincie onafhankelijke *mystery guest*-onderzoeken laten verrichten. Het doel van de onderzoeken was het testen van de weerbaarheid van de organisatie tegen onbevoegden, die toegang probeerden te krijgen tot informatie van de provincie. De bevindingen zijn gebruikt om de bewustwording van medewerkers te vergroten, door inzicht te geven in hun eigen handelen ten aanzien van informatieveiligheid en hen bewust te maken van mogelijke risico's. Ook heeft de provincie documenten in de organisatie verspreid waarmee zij medewerkers bekendmaken met de verantwoordelijkheid die zij hebben in het dagelijks handelen op het gebied van informatieveiligheid (bevinding 7).

Het mystery guest-onderzoek van 2015 toonde aan dat het bewustzijn van medewerkers op het gebied van informatieveiligheid was verbeterd ten opzichte van 2013. Wel toont het onderzoek van 2015 een aantal verbeterpunten aan, die gelijkenissen vertonen met de bevindingen van 2013. Dit toont het belang van continue aandacht voor bewustwording op het gebied van informatieveiligheid aan. Ook in 2016 voert de provincie bewustwordingsactiviteiten uit (bevinding 7 en 9).

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 zijn onder de aandacht gebracht van de directie en hebben tot vervolgacties geleid.

Ook heeft de provincie het afleggen van verantwoording over informatieveiligheid goed geregeld. Informatieveiligheid maakt onderdeel uit van de ambtelijke P&C-cyclus en sinds 2016 ook van de bestuurlijke P&C-cyclus. De provincie heeft tevens de zelfevaluatie over informatieveiligheid uitgevoerd.

Toelichting
De externe accountant heeft een toets uitgevoerd op informatieveiligheid in het kader van de jaarrekeningcontrole. De resultaten hiervan en de mystery guest-onderzoeken onderzoeken uit 2013 en 2015 zijn besproken door de directie en hebben tot vervolgacties geleid. Sinds begin 2014 heeft de provincie het voornemen om een ICT penetratietest te laten uitvoeren. Omdat de provincie zich in een overgangsfase van de ene naar de andere leverancier van de kantoorautomatisering bevond, was de uitvoering van de test uitgesteld. De test is in 2016 alsnog uitgevoerd (bevinding 9).

De provincie heeft het afleggen van verantwoording over informatieveiligheid goed geregeld. Informatieveiligheid is onderdeel van de ambtelijke P&C cyclus (aan het management). In 2016 is informatieveiligheid voor het eerst opgenomen in de Programmabegroting (de bestuurlijke P&C cyclus) (bevinding 8).

De provincie heeft in 2014 en 2015 de zelfevaluatie over informatieveiligheid uitgevoerd. De zelfevaluatie over 2015 is uitgebreider ingevuld dan de zelfevaluatie over 2014, waardoor het beter navolgbaar is waarop de scores op de verschillende informatieveiligheidsmaatregelen gebaseerd zijn. De bevindingen van de zelfevaluatie worden niet besproken met de directie. De maatregelen met de laagste scores van de zelfevaluatie zijn omgezet als speerpunt in het concernjaarplan. Voor de overige maatregelen is het niet goed navolgbaar óf en zo ja, welke acties de provincie op basis van de resultaten onderneemt (bevinding 10).

Reactie Gedeputeerde Staten

Provincie Noord-Holland

POSTBUS 3007 2001 DA HAARLEM

Randstedelijke Rekenkamer
Mevrouw A.W.C. Hoenderdos-Metselaar
Teleportboulevard 110
1043 EJ Amsterdam

Gedeputeerde Staten
Uw contactpersoon
W. Kegel
AD/STAF

Doorkiesnummer +31235143679
kegelw@noord-holland.nl

Betreft: **Bestuurlijk wederhoor conceptnota van bevindingen Informatieveiligheid**

Verzenddatum

- 6 JULI 2016

Kenmerk
826783/826838

Uw kenmerk
2016/AH/067

Geachte mevrouw Hoenderdos-Metselaar,

Met uw brief van 17 juni stelt u ons college in de gelegenheid te reageren op de conclusies en aanbevelingen uit de concept bestuurlijke nota *´Informatieveiligheid´* waarin de resultaten beschreven staan van het onderzoek naar de vraag of de provincie Noord-Holland de informatieveiligheid voldoende heeft geborgd. Met deze brief reageren op uw conclusies en aanbevelingen.

Wij verwerken als provincie Noord-Holland veel informatie. In veel gevallen is informatie een eindproduct binnen onze dienstverlening. Wij hechten dan ook groot belang aan de betrouwbaarheid van onze informatie. Onze informatiebeveiliging richt zich daarom op de bescherming van informatie tegen dreigingen om een ongestoorde voortgang van bedrijfsactiviteiten te waarborgen en om risico's te minimaliseren.

Hoofdconclusie
De conclusie van de Rekenkamer luidt als volgt:
De provincie besteedt voldoende aandacht aan de bewustwording van het belang van informatieveiligheid binnen de organisatie. Ook heeft de provincie het toezicht op en de verantwoording over informatieveiligheid goed geregeld. Er is een aantal beslissingen genomen, waarmee invulling wordt gegeven aan de verantwoordelijkheid voor informatieveiligheid. Er is wel verbetering mogelijk in de sturing op het tempo van de implementatie van de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid. Hoewel de provincie veel zaken heeft opgepakt, behoeft de organisatorische verankeringen de planmatige aanpak van informatieveiligheid verbetering. Sinds 2016 zet de provincie hiertoe wel stappen. Een ander verbeterpunt is de uitvoering van maatregelen om de

Postbus 3007
2001 DA Haarlem
Telefoon (023) 514 3143
Fax (023) 514 3030

Houtplein 33
Haarlem [2012 DE]
www.noord-holland.nl

informatieveiligheid te bevorderen. Het is bijvoorbeeld niet voor alle bedrijfsprocessen duidelijk welke informatieveiligheidsmaatregelen nodig zijn en de provincie heeft geen zicht of de maatregelen daadwerkelijk zijn uitgevoerd.

Wij zijn tevreden met de conclusie van de Rekenkamer dat toezicht op en verantwoording over informatieveiligheid op orde is. Over uw constatering dat het tempo van de implementatie van rollen en verantwoordelijkheden verbeterd kan worden, kunnen wij u melden dat wij een afweging hebben gemaakt tussen snelheid en zorgvuldigheid als het gaat om de inspanningen om informatieveiligheid organisatorisch te verankeren. Die inspanningen hangen nauw samen met de ontwikkelingen die wij in gang hebben gezet op het gebied van informatiebeleid in brede zin. Met de recente aanstelling van een Chief Information Officer (CIO) en het vaststellen van het concernbrede informatiebeleid zijn de juiste voorwaarden gecreëerd om de rollen en verantwoordelijkheden op het gebied van informatieveiligheid stevig en duurzaam te verankeren.
U geeft tevens aan dat de uitvoering van maatregelen ter bevordering van de informatieveiligheid verbeterd kan worden. De belangrijkste argumenten voor deze conclusie, namelijk dat niet voor alle bedrijfsprocessen duidelijk is welke maatregelen nodig zijn en of deze daadwerkelijk zijn uitgevoerd, verdienen enige nuance. Om een zeker minimaal niveau van beveiliging te organiseren is een basisnormenkader vastgesteld: de Interprovinciale Baseline Informatiebeveiliging (IBI). Dit normenkader is op alle bedrijfsprocessen van toepassing. De vraag of vanwege de gevoeligheid van een proces *aanvullende* maatregelen nodig zijn wordt weliswaar wel gesteld, maar is inderdaad nog voor verbetering vatbaar. Dit punt wordt nadrukkelijk meegenomen in het te vernieuwen informatieveiligheidsbeleid. Daarin zal ook aandacht worden geschonken aan de wijze waarop de uitvoering van maatregelen wordt gecontroleerd. Wij willen echter benadrukken dat het uitvoeren van maatregelen niet alleen binnen de grenzen van onze eigen organisatie gebeurt, maar voor een groot deel ook bij leveranciers en ketenpartners. Controle op uitvoering zal dus maatwerk vereisen.

Aanbeveling 1
Vraag GS ervoor te zorgen dat er zo spoedig mogelijk volgens de rollen en verantwoordelijkheden op het gebied van informatieveiligheid die in februari 2016 zijn vastgesteld wordt gewerkt.

Deze aanbeveling nemen wij over. Wij achten een duidelijke rolverdeling en heldere bevoegdheden een noodzakelijke voorwaarde voor een efficiënte en effectieve organisatie, ook op het gebied van informatieveiligheid. Het besluit waarin de rollen en

verantwoordelijkheden zijn gedefinieerd is het resultaat van een zorgvuldige afweging van belangen en ontwikkelingen. Momenteel wordt dit voorstel geïmplementeerd. Evaluatie van het gekozen model staat gepland voor begin 2018.

Aanbeveling 2
Vraag GS ervoor te zorgen dat een geactualiseerde versie van het informatieveiligheidsbeleid in 2016 wordt vastgesteld.

Deze aanbeveling nemen wij over. Het huidige informatiebeveiligingsbeleid stamt uit 2012 en zal dit jaar geactualiseerd worden. Wij hechten belang aan heldere en werkbare kaders. Informatieveiligheid is als fundament onder het Concerninformatieplan (CIP) dit jaar opnieuw stevig verankerd in een strategisch bedrijfsvoeringkader. Op ambtelijk niveau zal dit uitgewerkt worden in tactisch en operationeel informatieveiligheidsbeleid.

Aanbeveling 3
Vraag GS te bewaken dat voor alle bedrijfsprocessen wordt bepaald of een risicoanalyse nodig is en dat deze risicoanalyses worden uitgevoerd, evenals de aanvullende maatregelen die daaruit voortkomen.

Deze aanbeveling nemen wij over. Wij achten het van belang dat voor alle processen een adequaat beveiligingsniveau is vastgesteld, en dat de benodigde aanvullende beheersmaatregelen uitgevoerd worden. Momenteel geven wij hier invulling aan uw aanbeveling door via de Verbijzonderde Interne Controle (VIC) de processen die door de ambtelijke organisatie als risicovol worden beschouwd aan bovengenoemde eisen te toetsen. Inspanningen om ook de overige bedrijfsprocessen aan deze werkwijze te onderwerpen worden meegenomen in nieuwe beleidsplan.

We rekenen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Gedeputeerde Staten van Noord-Holland,

waarnemend provinciesecretaris
H.M. Schartman

voorzitter
J.W. Remkes

NH0001

Nawoord Rekenkamer

De Rekenkamer dankt GS voor hun reactie. Wij zijn verheugd dat het college op een enkele nuancering na de conclusies deelt en alle aanbevelingen overneemt. De reactie van GS geeft geen aanleiding tot het maken van nadere opmerkingen.

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 informatiesamenleving. Dit betekent dat onze activiteiten meer en meer zijn georganiseerd in informatienetwerken, worden geconcentreerd rondom informatieverwerking en zijn gebaseerd op informatietechnologie.[3] 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.[4] 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.[5] Daarnaast kunnen inbreuken op digitale veiligheid leiden tot financiële en imagoschade.[6] Uit onderzoek blijkt echter dat de helft van alle digitale inbraakpogingen vaak pas na maanden wordt ontdekt.[7] 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.[8] 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[9] (Bron: iBewustzijn Overheid, 2015)

[3] Castells (1996), The Information Age: Economy, Society, and Culture
[4] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
[5] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[6] Rekenkamer Den Haag (2014), Digitale Veiligheid
[7] FOX-IT (2015), www.fox-it.nl
[8] Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
[9] 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.[10] 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.[11] 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.[12] 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.[13] 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.[14]

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.[15] 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

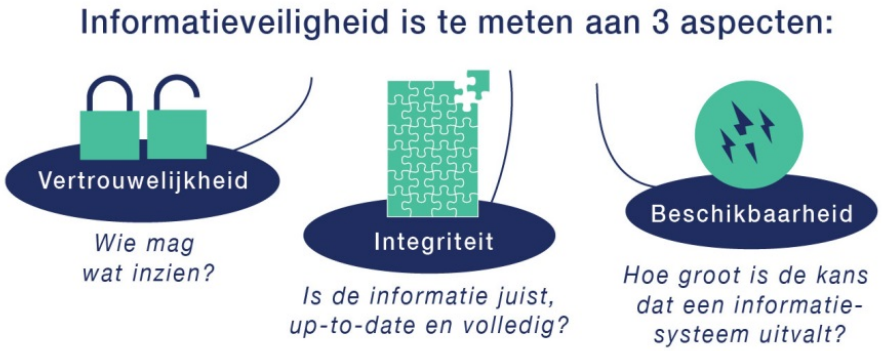
[10] Taskforce BID (2015), www.taskforcebid.nl
[11] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid
[12] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[13] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[14] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[15] 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.[16] 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).[17] De Rekenkamer kiest voor de term ‘informatieveiligheid’, omdat deze term meer recht doet aan de breedte van het onderwerp dan de term ‘informatiebeveiliging’, die vaak wordt geassocieerd met ICT.

Informatieveiligheid richt zich op bescherming van informatie tegen dreigingen, met als doel om de continuïteit van bedrijfsactiviteiten te waarborgen.[18] 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.[19] Informatieveiligheid heeft betrekking op het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie (zie Figuur 2).[20]



Figuur 2 Aspecten van informatieveiligheid

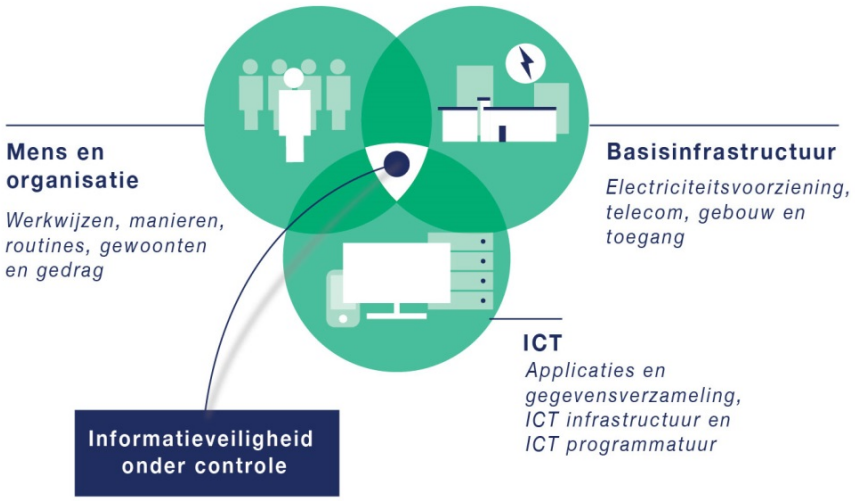
[16] Rekenkamer Den Haag (2014), Digitale Veiligheid
[17] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid provincie Zuid-Holland, Deel 2 Beleid Informatieveiligheid 2014-2018
[18] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging en Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
[19] Taskforce BID (2015), www.taskforcebid.nl
[20] 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[21]

	Aspecten		
	Vertrouwelijkheid	**Integriteit**	**Beschikbaarheid**
Kenmerk	Exclusiviteit	1. Correctheid 2. Volledigheid 3. Geldigheid 4. Authenticiteit 5. Onweerlegbaarheid	1. Tijdigheid 2. Continuïteit
Bedreiging	Onthulling Misbruik	1. Wijziging 2. Verwijdering/Toevoeging 3. Veroudering 4. Vervalsing 5. Verloochening	1. Vertraging 2. Uitval
Voorbeeld	Afluisteren van netwerk Hacking	1. Onrechtmatig wijzigen 2. Onrechtmatige verwijdering/Toevoeging 3. Gegevens niet up-to-date 4. Frauduleuze transactie 5. Ontkennen berichten te hebben verstuurd	1. Overbelasting infrastructuur 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).[22]



Figuur 3 Aandachtsgebieden van informatieveiligheid

[21] Provincie Zuid-Holland (2014), Integraal veiligheidsbeleid. Deel 2 Beleid Informatieveiligheid 2014-2018, p.5
[22] 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 Procedures (o.a. voorschriften voor wachtwoorden, uitloggen bij inactiviteit, etc.)	Creëren van bewustzijn Procedures (o.a. functiescheiding)	Creëren van bewustzijn Procedures (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 Logfiles bijhouden	Opstellen reserveapparatuur 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 Noord-Holland 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 Noord-Holland 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[23] informatieveiligheidsmaatregelen uit?
   c. Is informatie in de praktijk voldoende beschermd tegen toegang door onbevoegden?[24]
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?

[23] '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.
[24] 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[25], 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.[26] 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).

[25] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid

[26] 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 o.a. 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 o.a. 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. Deze onderzoeksvraag wordt voor de provincie Noord-Holland overigens niet beantwoord. De reden daarvoor wordt in paragraaf 3.3 toegelicht. 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 (2) IBI A.6.1.1 (3) IBI A.5.1.1 (4) IBI A.5.1.1 (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.) 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.) 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 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 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.

| 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[27] 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.

[27] Onder het management verstaat de Rekenkamer de bovenste twee lagen van het organogram: de algemene directie en de leidinggevenden van de organisatie-eenheden daaronder. De provincie duidt de twee bovenste lagen van het organogram echter doorgaans aan als 'de directie'. De Rekenkamer hanteert daarom in het vervolg de term directie in plaats van management.

Bevinding 1

Informatieveiligheid is belegd bij de gedeputeerde met onder andere ICT en personeel en organisatie in de portefeuille. De gedeputeerde wordt periodiek geïnformeerd over informatieveiligheid. De directie geeft in de praktijk invulling aan haar verantwoordelijkheid voor informatieveiligheid door beslissingen te nemen over onderwerpen op het gebied van informatieveiligheid. De directie heeft de rollen en verantwoordelijkheden in 2012 vastgesteld, maar de implementatie ervan is vertraagd. De besluitvorming over een nieuw voorstel voor rollen en verantwoordelijkheden op het gebied van informatieveiligheid, waarin ontwikkelingen binnen de organisatie zijn meegenomen, heeft lang geduurd. In februari 2016 heeft de directie dit voorstel vastgesteld. Op dit moment (mei 2016) wordt het voorstel geïmplementeerd.

Toelichting op de bevinding

In onderstaande paragrafen wordt achtereenvolgens ingegaan op de betrokkenheid van GS en de directie bij informatieveiligheid.

2.1.1 Betrokkenheid van GS bij informatieveiligheid

Portefeuilleverdeling

GS hebben het informatieveiligheidsbeleid van de provincie in de vergadering van 17 juli 2012 vastgesteld.[28] Eind 2014 hebben GS de Commissaris van de Koning gemachtigd om het Convenant Interprovinciale Regulering Informatieveiligheid te ondertekenen.[29] GS hebben het convenant voor akkoord verklaard bij behandeling van de agenda van het IPO tijdens de vergadering van 11 november 2014.[30] Informatieveiligheid is sinds mei 2015 ondergebracht bij de gedeputeerde met onder andere ICT en Personeel en organisatie in de portefeuille.[31]

Informatievoorziening aan GS

De gedeputeerde wordt in een periodiek stafoverleg geïnformeerd over zaken met betrekking tot informatieveiligheid.[32] Het gaat hierbij vooral om het informeren en het afleggen van verantwoording en niet zozeer om het geven van sturing.[33] Er zijn geen periodieke schriftelijke rapportages aan GS specifiek over informatieveiligheid. Er wordt ad hoc gerapporteerd over informatieveiligheid. Daarnaast maakt informatieveiligheid onderdeel uit van een aantal reguliere rapportages, zoals de Concernmanagementrapportage en de IT managementletter.[34] Deze rapportages worden besproken met de gedeputeerde.[35]

2.1.2 Betrokkenheid van de directie bij informatieveiligheid

Verantwoordelijkheden van de directie

In het informatieveiligheidsbeleid is vastgelegd dat de algemeen directeur eindverantwoordelijk is voor de informatieveiligheid van de provincie. In het document staat beschreven dat de algemeen directeur onder andere verantwoordelijk is voor het bepalen van de risicobereidheid van de provincie, het beschikbaar stellen van

[28] Provincie Noord-Holland (2012), Openbare besluitenlijst van de vergadering van gedeputeerde staten van Noord-Holland, 17 juli 2012
[29] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[30] Provincie Noord-Holland, e-mail, 26 oktober 2015
[31] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[32] Provincie Noord-Holland, bestuurlijk interview, 28 april 2016
[33] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[34] Provincie Noord-Holland (2014), Doorwerking IT Management Letter 2013, 1 november; Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage, periode 1, 2 en 3; Provincie Noord-Holland (2015), Concernmanagementrapportages, viermaandsrapportage, periode 1 en 2
[35] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016

middelen en het maken van afspraken met directeuren over de uitvoering van het informatieveiligheidsbeleid en het toezicht daarop. In het informatieveiligheidsbeleid is tevens vastgelegd dat directeuren binnen hun directie verantwoordelijk zijn voor informatieveiligheid. Zij zijn bijvoorbeeld verantwoordelijk voor het bepalen van de beveiligingsbehoefte binnen de eigen directie, het uitvoeren van risicoanalyses en het nemen van besluiten over de risicobereidheid voor de bedrijfsvoering. De directie Concernzaken[36] heeft daarnaast een aanvullende verantwoordelijkheid met betrekking tot de levering van generieke beveiligingsdiensten aan de andere bedrijfsonderdelen.[37]

Informatievoorziening aan de directie
Er is geen periodiek overleg waarin de directie wordt geïnformeerd over zaken rondom informatieveiligheid. Indien nodig agenderen de Kwartiermaker informatieveiligheid en/of zijn leidinggevende het onderwerp bij de algemeen directeur. Dit gebeurt doorgaans op initiatief van de Kwartiermaker en/of zijn leidinggevende. Er zijn geen periodieke schriftelijke rapportages aan de directie specifiek over informatieveiligheid. Er wordt ad hoc gerapporteerd over informatieveiligheid. Zoals beschreven in voorgaande paragraaf, maakt informatieveiligheid daarnaast onderdeel uit van een aantal reguliere rapportages, zoals de Concernmanagementrapportage en de IT managementletter. Deze rapportages worden besproken met de directie.[38]

Sturing in de praktijk
In de praktijk geeft de directie invulling aan haar (eind)verantwoordelijkheid voor informatieveiligheid door beslissingen te nemen over onderwerpen die spelen op het gebied van informatieveiligheid. Voorbeelden hiervan zijn beslissingen met betrekking tot het uitvoeren van een ICT penetratietest, een phishingmail-actie om de bewustwording van medewerkers te vergroten (zie hoofdstuk 4) en beslissingen met betrekking tot het proces rondom de Meldplicht datalekken die op 1 januari 2016 in werking is getreden.[39] De ambtelijke organisatie heeft aangegeven dat sturing op informatieveiligheid door de directie voornamelijk indirect plaatsvindt.[40]

In 2012 heeft de directie een besluit genomen over de inrichting van de organisatie op het gebied van informatieveiligheid. De implementatie van dit besluit heeft echter vertraging opgelopen; in de periode 2012-2015 is weinig voortgang geboekt. Begin 2016 heeft de directie een nieuw voorstel voor rollen en verantwoordelijkheden vastgesteld, waarin ontwikkelingen binnen de organisatie zijn meegenomen. Ook is gestart met de implementatie ervan. Dit wordt in onderstaande alinea's nader toegelicht. Achtereenvolgens wordt ingegaan op 1) de rollen en verantwoordelijkheden zoals vastgesteld in 2012 en 2) de implementatie ervan in de periode 2012-2016.

<u>Rollen en verantwoordelijkheden volgens het informatieveiligheidsbeleid (2012)</u>
In 2012 heeft de directie het informatieveiligheidsbeleid vastgesteld.[41] Het beleid biedt onder andere de kaders voor de inrichting van de organisatie op het gebied van informatieveiligheid. De rollen en verantwoordelijkheden zijn nader uitgewerkt in het document Inrichten beveiligingsorganisatie[42] (hierna: inrichtingsplan), dat de directie tegelijkertijd met het informatieveiligheidsbeleid heeft vastgesteld.[43] Het inrichtingsplan beschrijft de verantwoordelijkheden van alle functionarissen op het gebied van informatieveiligheid, waaronder die van de

[36] Tot 1 januari 2016 was dit de directie Middelen
[37] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
[38] Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[39] Provincie Noord-Holland, zes e-mails, 3 juni 2016
[40] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[41] Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
[42] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
[43] Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni

algemeen directeur, directeuren van de organisatie-eenheden, Concern control en medewerkers in het algemeen. Volgens het plan hebben proceseigenaren (lijnmanagers) een primaire rol in informatieveiligheid: "*de manager is de enige die verantwoord kan beslissen over de mogelijk tegenstrijdige belangen tussen informatiebeveiliging, efficiency in de procesvoering, kosten en baten en gebruiksvriendelijkheid van informatiesystemen*".[44] Het inrichtingsplan beschrijft daarnaast twee functionarissen die er tot dat moment niet waren:

- *Kwartiermaker informatieveiligheid:* deze functionaris is de centrale spil in de opstartfase van informatieveiligheid. De Kwartiermaker moet de weg banen voor de Centrale informatiebeveiligings-functionaris, waarbij de positionering van deze functionaris in de organisatie moet worden bepaald. Ook is de Kwartiermaker verantwoordelijk voor het tot stand brengen van de beveiligingsorganisatie.
- *Centrale informatiebeveiligingsfunctionaris*: deze functionaris is de centrale spil in de operationele fase van informatieveiligheid, met een onafhankelijke – nog te bepalen – positie binnen de organisatie. Deze functionaris is gedelegeerd verantwoordelijk voor de coördinatie van taken op het gebied van informatieveiligheid.[45]

Implementatie van de rollen en verantwoordelijkheden 2012-2016

De implementatie van de rollen en verantwoordelijkheden met betrekking tot informatieveiligheid is echter vertraagd. De Centrale informatiebeveiligingsfunctionaris, die een centrale rol moet gaan spelen in informatieveiligheid, is bijvoorbeeld nog niet aangesteld. Tot die tijd ligt die rol bij de Kwartiermaker informatieveiligheid, die in 2013 is aangesteld bij Concern control (dit wordt nader toegelicht in paragraaf 2.2).

De Kwartiermaker heeft in 2014 op basis van het inrichtingsplan een voorstel voor het inrichten van de beveiligingsorganisatie geschreven. De ambtelijke organisatie heeft aangegeven dat de directie dit voorstel destijds heeft afgewezen, onder andere omdat het voorstel volgens de directie niet goed aansloot op ontwikkelingen binnen de organisatie. Volgens de ambtelijke organisatie is er om die reden een nieuw voorstel gemaakt, waarin de volgende ontwikkelingen zijn meegenomen:[46]

- *Het traject van de Houtskoolschetsen*: in de houtskoolschetsen van de provincie is kaderstelling op het gebied van bedrijfsvoering – waar informatieveiligheid onderdeel van uitmaakt – een primaire verantwoordelijkheid geworden van de directie Concernzaken. In het informatieveiligheidsbeleid en inrichtingsplan uit 2012 werd uitgegaan van directe sturing door de algemeen directeur. In het kader van de houtskoolschetsen wordt een aantal bevoegdheden op het gebied van informatieveiligheid gedelegeerd aan de directeur Concernzaken.
- *De ontwikkeling van informatiemanagement en het informatiebeleid*: informatieveiligheid is één van de pijlers van het informatiebeleid. Het informatiebeleid was in 2012 echter nog niet opgesteld. Gezien de overlap moet informatieveiligheid langs dezelfde lijnen georganiseerd worden als informatiemanagement. Dit betekent dat de informatiemanager en de Chief Information Officer (CIO) in het nieuwe voorstel een coördinerende rol hebben op het gebied van informatieveiligheid. In het inrichtingsplan uit 2012 hadden zij geen rol.[47]

De directie heeft het aangepaste voorstel uiteindelijk in februari 2016 vastgesteld.[48] Op dit moment (mei 2016) wordt het voorstel geïmplementeerd.[49] Volgens de ambtelijke organisatie lag het voorstel er al enige tijd, maar heeft de besluitvorming erover vertraging opgelopen vanwege de samenhang met besluitvorming over het

[44] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie, p. 5
[45] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie en Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
[46] Provincie Noord-Holland, e-mail, 5 februari 2016 en Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari
[47] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari en Provincie Noord-Holland, e-mail, 5 februari 2016
[48] Provincie Noord-Holland (2012), Nota directie, betreft: governance informatiebeveiliging, 4 februari 2016
[49] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016

informatiebeleid.[50] De ambtelijke organisatie heeft aangegeven dat het opstellen van en de besluitvorming over het informatiebeleid dusdanig vertraging heeft opgelopen, dat de directie het voorstel voor de rollen en verantwoordelijkheden op het gebied van informatieveiligheid uiteindelijk afzonderlijk heeft vastgesteld. In het feitelijk wederhoor heeft de provincie aangegeven dat het informatiebeleid in mei 2016 alsnog is vastgesteld door de directie.[51] Het voorstel voor de rollen en verantwoordelijkheden op het gebied van informatieveiligheid wordt nader toegelicht in paragraaf 2.2.

Meldplicht datalekken

In het kader van de Meldplicht datalekken, die op 1 januari 2016 in werking is getreden, waren de verantwoordelijkheden in maart 2016 nog niet vastgesteld.[52] Deze meldplicht is onderdeel van de Wet bescherming persoonsgegevens.[53] 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.[54] De meldplicht houdt in dat organisaties een datalek binnen 72 uur moeten melden bij de Autoriteit Persoonsgegevens.[55] In sommige gevallen moet het datalek ook gemeld worden aan 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.[56]

De provincie is in 2015 een project gestart om te inventariseren welke stappen zij moet ondernemen om aan de Meldplicht datalekken te voldoen.[57] De directeur Concernzaken is opdrachtgever van het project.[58] Acties die de provincie moet ondernemen zijn bijvoorbeeld het opstellen van een meldingsprotocol voor datalekken, het in kaart brengen welke persoonsgegevens de provincie verwerkt en welke externe partijen in opdracht van de provincie persoonsgegevens verwerken en het aanpassen van het sjabloon voor de bewerkersovereenkomst met externe partijen. In deze overeenkomst moet worden vastgelegd wat de taken, verantwoordelijkheden en verplichtingen zijn van de externe partij met betrekking tot de meldplicht.[59] Ook moet de provincie een functionaris gegevensbescherming aanstellen. Deze functionaris beheert het meldpunt datalekken, voert het contact over (mogelijke) datalekken met de Autoriteit Persoonsgegevens en is binnen de organisatie het aanspreekpunt voor het melden en registreren van datalekken. Uit een voortgangsrapportage (januari 2016) blijkt dat het meldingsprotocol is opgesteld en dat voor een groot deel is geïnventariseerd welke persoonsgegevens de provincie en partijen in opdracht van de provincie verwerken. Uit de rapportage blijkt dat het sjabloon voor de bewerkersovereenkomst nog niet is aangepast.[60] In het feitelijk wederhoor (mei 2016) heeft de provincie aangegeven dat een aantal, maar nog niet alle overeenkomsten inmiddels zijn aangepast.[61] Daarnaast blijkt uit

[50] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[51] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[52] Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016
[53] Eerste Kamer der Staten-Generaal (2016), www.eerstekamer.nl
[54] Autoriteit Persoonsgegevens (2015), www.autoriteitpersoonsgegevens.nl
[55] Voorheen het College Bescherming Persoonsgegevens (CBP)
[56] Justitia.nl (2015), www.justitia.nl
[57] Provincie Noord-Holland (2015), Memo aan Stuurgroep I&I, betreft: wijziging Wet bescherming persoonsgegevens en Provincie Noord-Holland (2015), Plan van aanpak meldplicht datalekken, 2 november
[58] Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016
[59] Provincie Noord-Holland (2015), Plan van aanpak meldplicht datalekken, 2 november
[60] Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016
[61] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016

de rapportage dat de functionaris gegevensbescherming nog niet aangesteld.[62] De directeur Concernzaken moet op dit moment (maart 2016) nog een besluit nemen over de positionering van deze functionaris.[63]

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.

Bevinding 2

De directie heeft de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid in 2012 vastgesteld, maar de implementatie ervan is vertraagd. In de periode 2012-2015 is weinig voortgang geboekt. Zo is de Centrale informatiebeveiligingsfunctionaris – de centrale spil in de operationele fase van informatieveiligheid – nog niet aangesteld. Tot die tijd vervult de Kwartiermaker informatieveiligheid deze rol. De provincie heeft aangegeven dat de mate waarin proceseigenaren invulling geven aan hun verantwoordelijkheid in informatieveiligheid, varieert.

In februari 2016 heeft de directie een aangepast voorstel voor rollen en verantwoordelijkheden vastgesteld. De belangrijkste verandering is dat de verantwoordelijkheid voor informatieveiligheid wordt belegd over meer functies en er een duidelijke scheiding komt tussen kaderstelling, uitvoering en controle. Op dit moment (mei 2016) wordt het voorstel geïmplementeerd.

Toelichting op de bevinding

In deze paragraaf wordt allereerst de huidige verdeling van rollen en verantwoordelijkheden op het gebied van informatieveiligheid toegelicht. Vervolgens wordt ingegaan op het nieuwe voorstel voor de verantwoordelijkheidsverdeling, dat op 4 februari 2016 door de directie is vastgesteld.[64]

2.2.1 Verantwoordelijkheidsverdeling in de praktijk

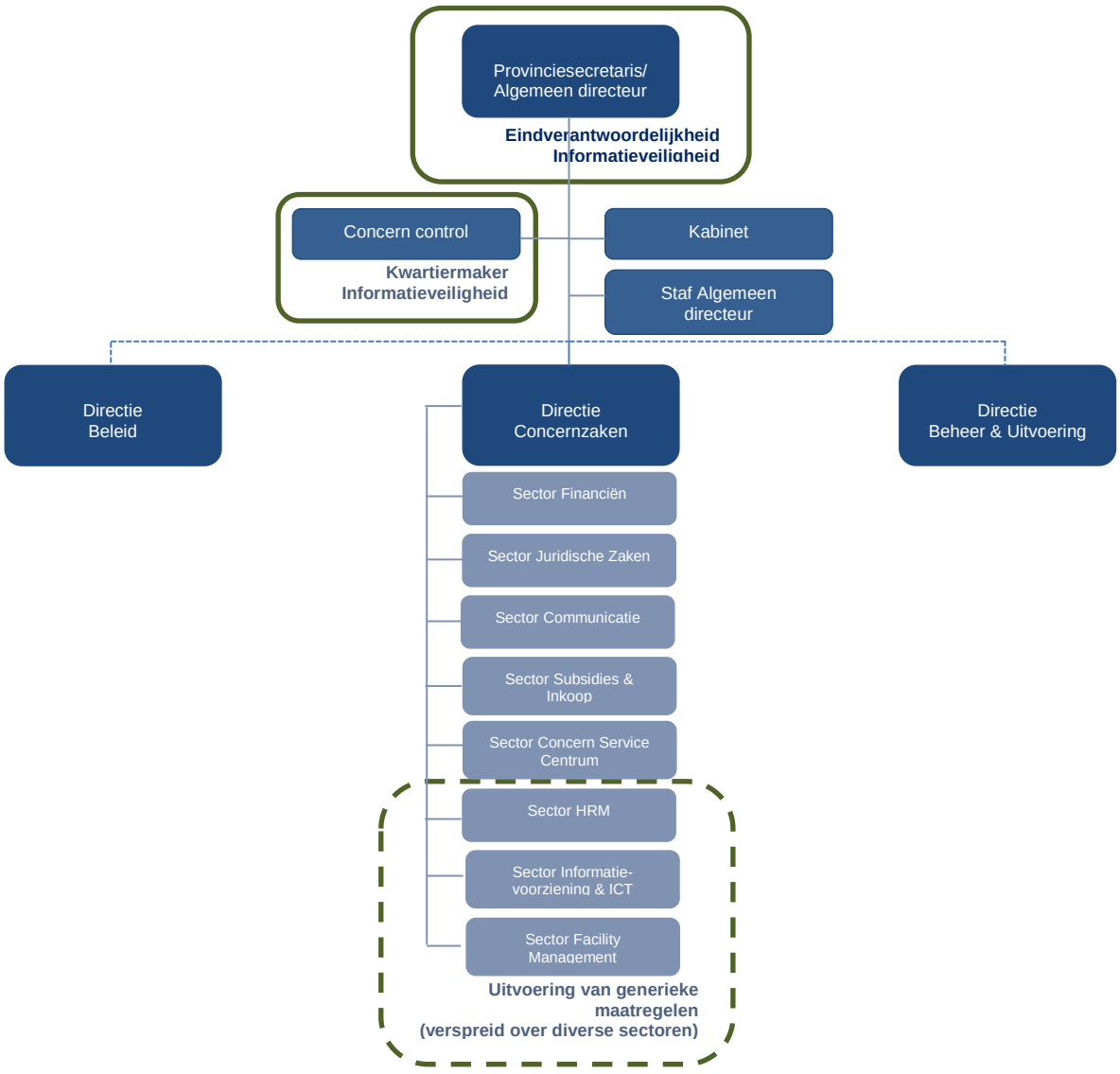
In voorgaande paragraaf is beschreven dat de directie in 2012 het informatieveiligheidsbeleid en het document Inrichten beveiligingsorganisatie (inrichtingsplan) heeft vastgesteld, waarin de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid zijn uitgewerkt. In de paragraaf kwam echter ook naar voren dat de implementatie ervan is vertraagd. Deze paragraaf gaat in op de rollen en verantwoordelijkheden ten aanzien van

[62] Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016

[63] Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016 en Provincie Noord-Holland, e-mail, 16 maart 2016

[64] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari

informatieveiligheid in de huidige praktijk. De verantwoordelijkheden van de directie zijn in voorgaande paragraaf aan de orde gekomen. In deze paragraaf komen respectievelijk de Kwartiermaker informatieveiligheid, de verantwoordelijkheden voor de uitvoering van generieke maatregelen en de rol van de organisatie aan de orde. Figuur 4 geeft weer waar de verantwoordelijkheden zijn belegd binnen de organisatie.



Figuur 4 Verantwoordelijkheden met betrekking tot informatieveiligheid in de huidige praktijk (tot maart 2016)

Kwartiermaker informatieveiligheid

De provincie heeft in 2013 een Kwartiermaker informatieveiligheid aangesteld. De Kwartiermaker was verantwoordelijk voor het tot stand brengen van de beveiligingsorganisatie volgens het inrichtingsplan.[65] Het betrof een tijdelijke functie, belegd bij Concern control.[66] In voorgaande paragraaf kwam echter naar voren dat de implementatie van het inrichtingsplan is vertraagd, de Centrale informatiebeveiligingsfunctionaris nog niet is

[65] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
[66] Provincie Noord-Holland, ambtelijk interview, 3 november 2015

aangesteld en de Kwartiermaker deze rol tot die tijd vervult. Uit gesprekken met de ambtelijke organisatie blijkt dat de Kwartiermaker daardoor meer taken heeft opgepakt dan waar hij volgens zijn functieomschrijving verantwoordelijk voor is.[67] Daarbij heeft hij onvoldoende tijd (8-20 uur per week) om alle taken op het gebied van informatieveiligheid volwaardig uit te voeren.

Sinds 2013 is de Kwartiermaker het centrale aanspreekpunt voor informatieveiligheid en richt zich op de volgende aspecten:

- het uitvoeren, coördineren en controleren van acties en maatregelen op het gebied van informatieveiligheid;
- het zorgen voor definitieve belegging van informatieveiligheid binnen de organisatie;
- het versterken van de bewustwording van medewerkers op het gebied van informatieveiligheid;
- het onderhouden van het beleid en de baseline via deelname aan het Cibo.

De ambtelijke organisatie heeft aangegeven dat informatieveiligheid in de huidige praktijk teveel leunt op één functie.[68] Bovendien voert de Kwartiermaker zowel uitvoerende, coördinerende als controlerende taken uit. Met de implementatie van het nieuwe voorstel voor de verantwoordelijkheidsverdeling komt hier verandering in: de verantwoordelijkheid voor informatieveiligheid wordt belegd over meer functies en er komt een duidelijke scheiding tussen kaderstelling, uitvoering en controle. Dit wordt nader toegelicht in paragraaf 2.2.2.

Uitvoering van generieke maatregelen met betrekking tot informatieveiligheid

De provincie heeft het merendeel van de kantoorautomatisering uitbesteed aan een externe leverancier. Voor de uitvoering van het gros van de ICT-gerelateerde maatregelen betekent dit dat deze maatregelen niet door de provincie, maar door de externe leverancier worden uitgevoerd. Deze leverancier wordt aangestuurd door de sector Informatievoorziening & ICT.[69] Daarnaast voert de provincie zelf een aantal maatregelen met betrekking tot informatieveiligheid uit. Dit betreffen maatregelen op het gebied van mens & organisatie, basisinfrastructuur en het resterende deel van de ICT-gerelateerde maatregelen. De uitvoering van deze maatregelen vindt verspreid over verschillende sectoren van de directie Concernzaken plaats. Zo voert de sector Informatievoorziening & ICT het resterende deel van de ICT-gerelateerde maatregelen uit, de sector HRM maatregelen op het gebied van mens & organisatie en de sector Facility Management maatregelen gericht op de basisinfrastructuur.[70] De Rekenkamer heeft niet onderzocht of de maatregelen daadwerkelijk zijn uitgevoerd.[71]

Rol van proceseigenaren in informatieveiligheid

Volgens het inrichtingsplan uit 2012 hebben proceseigenaren (lijnmanagers) een centrale rol in informatieveiligheid. De ambtelijke organisatie heeft aangegeven dat de mate waarin proceseigenaren invulling geven aan deze verantwoordelijkheid varieert: een aantal proceseigenaren is zich bewust van zijn of haar verantwoordelijkheid ten aanzien van informatieveiligheid en geeft daar actief invulling aan. Er zijn ook proceseigenaren die zich nog niet volledig bewust zijn van het belang van informatieveiligheid en hun verantwoordelijkheid daarin.[72] Eén van de geïnterviewden geeft aan dat dit komt doordat de implementatie van het inrichtingsplan vertraging heeft opgelopen, waardoor de verantwoordelijkheden met betrekking tot informatieveiligheid niet voor iedereen helder zijn.[73] Dat niet alle proceseigenaren actief invulling geven aan hun verantwoordelijkheid ten aanzien van informatieveiligheid blijkt bijvoorbeeld uit de constatering dat ICT-adviseurs

[67] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[68] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[69] Provincie Noord-Holland, ambtelijke interviews, 3 november en 7 december 2015
[70] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[71] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[72] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[73] Provincie Noord-Holland, ambtelijk interview, 7 december 2015

van de directie Concernzaken doorgaans het initiatief nemen om Business Impact Analyses (BIA's) uit te voeren.[74] Volgens het model van integraal management dat de provincie hanteert, is dat de verantwoordelijkheid van de proceseigenaar (zie paragraaf 3.2).

Om proceseigenaren te faciliteren in het geven van invulling aan hun verantwoordelijkheid in informatieveiligheid, krijgen zij ondersteuning van medewerkers met expertise op het gebied van informatieveiligheid, zoals ICT-adviseurs. De CIO en de Centrale Informatiebeveiligingsfunctionaris – die op dit moment wordt geworven – zullen hier tevens een rol in gaan krijgen.[75]

2.2.2 Verantwoordelijkheidsverdeling volgens het nieuwe voorstel

Zoals beschreven in paragraaf 2.1, heeft de directie op 4 februari 2016 een aangepast voorstel voor de rollen en verantwoordelijkheden op het gebied van informatieveiligheid vastgesteld. In dit voorstel is een duidelijke scheiding gemaakt tussen kaderstelling, uitvoering en controle ten aanzien van informatieveiligheid. Er zijn tevens financiële middelen beschikbaar gesteld.[76] Op dit moment (mei 2016) worden de rollen en verantwoordelijkheden geïmplementeerd.[77] In deze paragraaf worden de voorgestelde rollen en verantwoordelijkheden kort beschreven.

(Eind)verantwoordelijkheid informatieveiligheid

In het informatieveiligheidsbeleid en inrichtingsplan uit 2012 werd uitgegaan van directe sturing door de algemeen directeur.[78] Eén van de ontwikkelingen die de provincie in het kader van de Houtskoolschetsen heeft doorgemaakt, is dat kaderstelling op het gebied van bedrijfsvoering een primaire verantwoordelijkheid is geworden van de directie Concernzaken. Voor informatieveiligheid betekent dit dat een aantal bevoegdheden op het gebied van informatieveiligheid wordt gemandateerd aan de directeur Concernzaken. De algemeen directeur blijft eindverantwoordelijk voor informatieveiligheid.[79]

Chief Information Officer (CIO) en informatiemanagers

In het kader van de ontwikkeling van informatiemanagement heeft de provincie per 1 februari 2016 een CIO aangesteld.[80] Ook is de positionering van informatiemanagers verstevigd. Gezien de overlap tussen informatieveiligheid en informatiemanagement, wordt informatieveiligheid langs dezelfde lijnen georganiseerd als informatiemanagement. De coördinerende taken op het gebied van informatieveiligheid worden ondergebracht in een zogeheten CIO office. De CIO – die direct onder de directeur Concernzaken valt – is verantwoordelijk voor de beleidsdoelstellingen op het gebied van informatiemanagement en informatieveiligheid.[81]

Centrale en decentrale informatiebeveiligingsfunctionaris

Er wordt een Centrale informatiebeveiligingsfunctionaris aangesteld, die een coördinerende en faciliterende rol heeft ten aanzien van informatieveiligheid.[82] De ambtelijke organisatie heeft aangegeven dat deze functionaris op

[74] Provincie Noord-Holland, ambtelijke interviews, 3 november en 7 en 22 december 2015
[75] Provincie Noord-Holland, e-mail, 3 juni 2016
[76] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari
[77] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[78] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid en Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
[79] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari en Provincie Noord-Holland, e-mail, 5 februari 2016
[80] Provincie Noord-Holland, bestuurlijk interview, 28 april 2016
[81] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari
[82] Provincie Noord-Holland, ambtelijk interview, 16 december 2015 en Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari

dit moment (juni 2016) wordt geworven.[83] De Kwartiermaker informatieveiligheid zal te zijner tijd zijn beleids- en uitvoerende taken overdragen aan deze coördinator.[84] Daarnaast wordt binnen elke directie de rol van Decentrale informatiebeveiligingsfunctionaris belegd. Deze functionaris initieert en coördineert informatieveiligheid vanuit de directies en bewaakt de algemene beleidslijnen ten aanzien van informatieveiligheid. De Centrale informatiebeveiligingsfunctionaris wordt gepositioneerd binnen het CIO office. De Decentrale informatiebeveiligingsfunctionarissen blijven op hun huidige positie in de directies.

Sectoren binnen de directie Concernzaken
De sectoren binnen de directie Concernzaken zijn verantwoordelijk voor de uitvoering van de generieke maatregelen.

Rol van de organisatie
In het kader van integraal management zijn proceseigenaren (lijnmanagers) verantwoordelijk voor de informatieveiligheid van hun proces. Dit betekent dat directies en sectoren verantwoordelijk zijn voor uitvoerende activiteiten, zoals het uitvoeren van risicoanalyses en het bepalen van maatregelen. Daarnaast is de hele organisatie verantwoordelijk voor de uitvoering van het beleid.

Concern control
Concern control is verantwoordelijk voor het toezicht op de naleving van de kaders voor informatieveiligheid en de toetsing van de effectiviteit van de maatregelen en het beleid. Zo is Concern control verantwoordelijk voor het plannen en (laten) uitvoeren van audits, het controleren van de uitvoering van maatregelen en het uitvoeren van voortgangscontroles op beveiligingsplannen.[85]

[83] Provincie Noord-Holland, e-mail, 3 juni 2016
[84] Provincie Noord-Holland, e-mail, 29 april 2016
[85] Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari

| 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, heeft tot doel om de vraag te beantwoorden 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. Deze onderzoeksvraag is voor de provincie Noord-Holland echter niet in het onderzoek betrokken. Dit wordt in paragraaf 3.3 nader toegelicht.

3.1 Informatieveiligheidsbeleid in opzet

Criterium 3
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.

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 is in 2012 vastgesteld door de directie en GS en ter kennisname aangeboden aan PS. In het document is aangegeven dat het informatieveiligheidsbeleid samenhangt met het (destijds nog op te stellen) informatiebeleid. Het informatiebeleid is echter pas in mei 2016 vastgesteld. Het informatieveiligheidsbeleid verwijst naar de IBI. De ambtelijke organisatie heeft aangegeven dat in 2016 een geactualiseerde versie van het informatieveiligheidsbeleid zal worden vastgesteld.

Toelichting op de bevinding

Het informatieveiligheidsbeleid[86] is vastgesteld door de directie in de vergadering van 28 juni 2012.[87] GS hebben het beleid daarna vastgesteld in de vergadering van 17 juli 2012.[88] Op 21 december 2012 is het document vervolgens ter kennisname aangeboden aan PS.[89] Eén van de aanleidingen voor het opstellen van het informatieveiligheidsbeleid was een nulmeting van informatieveiligheid, uitgevoerd door Concern control in 2011. Uit deze nulmeting kwam naar voren dat een integraal informatieveiligheidsbeleid met een duidelijke positie binnen de organisatie en een samenhangende set aan beveiligingsmaatregelen ontbrak.[90]

Het doel van het informatieveiligheidsbeleid is als volgt geformuleerd: *"…het vaststellen van de organisatie en het proces voor informatiebeveiliging binnen de provincie Noord-Holland*."[91] De provincie hanteert een brede definitie van informatieveiligheid: "*Het is een zaak voor de hele organisatie en vereist maatregelen op het gebied van techniek, processen, procedures en gedrag*."[92]

Het informatieveiligheidsbeleid biedt op hoofdlijnen de kaders voor de inrichting van de organisatie van informatieveiligheid. Dit is nader uitgewerkt in het document Inrichten beveiligingsorganisatie[93], dat is vastgesteld door de directie (zie Figuur 5).[94] De inrichting van de organisatie van informatieveiligheid is besproken in hoofdstuk 2. Ook beschrijft het informatieveiligheidsbeleid richtlijnen voor de beheersing van informatieveiligheid. Hierbij worden de processen met betrekking tot informatieveiligheid, beveiligingsincidenten en calamiteitenmanagement geschetst. De processen met betrekking tot de uitvoering van generieke maatregelen, Business Impact Analyses en aanvullende maatregelen zijn uitgewerkt in het document Beleidsimplementatie acties en professionaliteitsstappen[95], dat tevens is vastgesteld door de directie. Deze processen worden in paragraaf 3.2 toegelicht.

Figuur 5 **Het informatieveiligheidsbeleid is uitgewerkt in 1) Inrichten beveiligingsorganisatie[96] en 2) Beleidsimplementatie acties en professionaliteitsstappen[97]**

[86] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
[87] Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
[88] Provincie Noord-Holland (2012), Openbare besluitenlijst van de vergadering van gedeputeerde staten van Noord-Holland, 17 juli 2012
[89] Provincie Noord-Holland (2012), Brief van GS aan PS, betreft: informatiebeveiligingsbeleid, 21 december
[90] Provincie Noord-Holland (2011), Onderzoeksrapport Nulmeting Informatiebeveiliging
[91] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid, p. 3
[92] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid, p. 4
[93] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
[94] Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
[95] Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen
[96] Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
[97] Provincie Noord-Holland (2012), Beleidsimplementatie actie en professionaliteitsstappen

In het informatieveiligheidsbeleid is beschreven dat het informatieveiligheidsbeleid samenhangt met het informatiebeleid. Het informatiebeleid was destijds (2012) echter nog niet opgesteld. In het feitelijk wederhoor heeft de provincie aangegeven dat het informatiebeleid uiteindelijk in mei 2016 is vastgesteld.[98] Het informatieveiligheidsbeleid verwijst naar de IBI: in het informatieveiligheidsbeleid staat beschreven dat de provincie beschikt over een standaard beveiligingsniveau, dat (mede) is gebaseerd op de IBI.[99]

Het informatieveiligheidsbeleid dient elke vier jaar te worden vastgesteld. De ambtelijke organisatie heeft aangegeven dat in 2016 een geactualiseerde versie van het informatieveiligheidsbeleid zal worden vastgesteld. In het Cibo zijn de provincies bezig met het opstellen van een nieuwe IBI voor informatieveiligheid. Volgens de huidige planning zal deze in 2016 van kracht worden.[100] De ambtelijke organisatie heeft aangegeven dat zij de intentie heeft om de veranderingen ten aanzien van de nieuwe IBI te verwerken in het opnieuw vast te stellen informatieveiligheidsbeleid.[101]

3.2 De uitvoering van informatieveiligheidsmaatregelen

3.2.1 Uitvoering van generieke maatregelen

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

Toelichting op het criterium
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. In de IBI zijn de generieke en aanvullende maatregelen ingedeeld in elf verschillende categorieën, die betrekking hebben op de aandachtsgebieden mens & organisatie, basisinfrastructuur en ICT. Deze categorieën zijn toegelicht in Tabel 4.

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.

[98] Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[99] Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
[100] Provincie Noord-Holland, e-mail, 16 februari 2016
[101] Provincie Noord-Holland, ambtelijk interview, 16 december 2015

Tabel 4 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	Onder andere 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

De provincie heeft het merendeel van de kantoorautomatisering uitbesteed aan een externe leverancier. Dit betekent dat een groot aantal ICT-gerelateerde generieke maatregelen door deze leverancier wordt uitgevoerd. De provincie controleert niet of de leverancier de maatregelen daadwerkelijk uitvoert. In de aanbestedingseisen heeft de provincie opgenomen dat de leverancier in het bezit moet zijn van een geldig ISO 27001 certificaat. Met het bezit van dit certificaat gaat de provincie ervan uit dat de leverancier de maatregelen uitvoert. Na de opdrachtverstrekking controleert de provincie niet of de leverancier in bezit blijft van een geldig certificaat. Sinds 2016 voert de provincie overleg met de leverancier over de uitvoering van de generieke maatregelen.

De provincie voert de overige generieke maatregelen zelf uit, verspreid over diverse sectoren van de directie Concernzaken. Volgens de ambtelijke organisatie hebben de sectoren zelf een nadere concretisering van de generieke maatregelen gemaakt. De provincie heeft geen registratiesysteem waarin de uitvoering van de maatregelen wordt bijgehouden. De stand van zaken van de uitvoering wordt bijgehouden in de interprovinciale monitoringtool van het Cibo. Dit betreft een inschatting en geen controle of de maatregelen daadwerkelijk zijn uitgevoerd. Hierdoor heeft de provincie volgens de Rekenkamer geen zicht of de maatregelen daadwerkelijk zijn uitgevoerd.

Toelichting op de bevinding

Onderstaande toelichting gaat achtereenvolgens in op de generieke maatregelen die worden uitgevoerd door een externe leverancier en de generieke maatregelen die de provincie zelf uitvoert.

Generieke maatregelen uitgevoerd door externe leverancier

De provincie heeft het merendeel van de kantoorautomatisering uitbesteed aan een externe leverancier. Voor de uitvoering van het gros van de ICT-gerelateerde generieke maatregelen betekent dit dat deze maatregelen niet door de provincie, maar door de externe leverancier worden uitgevoerd. De leverancier wordt aangestuurd door de sector Informatievoorziening & ICT van de provincie. In het najaar van 2015 bevond de provincie zich in een overgangsfase naar een andere leverancier.[102] Desgevraagd heeft de ambtelijke organisatie aangegeven dat de eindverantwoordelijkheid voor informatieveiligheid nog altijd bij de provincie ligt: *"het doen is uitbesteed, het denken niet"*.[103]

De ambtelijke organisatie heeft aangegeven dat in de aanbestedingseisen is opgenomen dat de externe leverancier in het bezit moet zijn van een ISO 27001 certificaat.[104] Dit is hetzelfde normenkader waarop de IBI is gebaseerd.[105] Met het bezit van dit certificaat gaat de provincie ervan uit dat de leverancier de generieke maatregelen uit de IBI uitvoert.[106] Het ISO certificaat is voor een bepaalde periode geldig, maar de provincie controleert niet of de leverancier ná de opdrachtverstrekking in het bezit blijft van een geldig certificaat.[107]

In 2012 heeft de provincie in samenwerking met een externe partij een inschatting gemaakt van de uitvoering van de generieke maatregelen. Hierbij is ingeschat:

- of de maatregel is gedefinieerd;
- in welke mate de maatregel is geïmplementeerd;
- of de maatregel wordt gemonitord.

Op basis van de bevindingen zijn aanbevelingen opgesteld, die de directie heeft vastgesteld.[108] Eén van de aanbevelingen was om goede afspraken te maken met externe leveranciers en toe te zien op de naleving van deze afspraken.

De ambtelijke organisatie heeft aangegeven dat de provincie nog niet heeft gecontroleerd of de externe leverancier de generieke maatregelen daadwerkelijk heeft uitgevoerd.[109] Dit geldt zowel voor de huidige als de voorgaande leverancier. De huidige leverancier heeft in het najaar van 2015 wel voor alle maatregelen uit de ISO 27001 een inschatting gemaakt wie voor de uitvoering van welke generieke maatregel verantwoordelijk is: de leverancier, de provincie of gezamenlijk. Ook heeft de leverancier een inschatting gemaakt van de stand van zaken van de uitvoering van de maatregelen waar de leverancier zelf verantwoordelijk voor is.[110] De ambtelijke organisatie heeft aangegeven dat zij de intentie heeft om deze inschatting te bespreken met de leverancier en

[102] Provincie Noord-Holland, ambtelijke interviews, 3 november en 7 december 2015
[103] Provincie Noord-Holland, ambtelijk interview, 7 december 2015
[104] Provincie Noord-Holland, ambtelijke interviews, 3 november en 7 en 22 december 2015
[105] Cibo en IPO (2010), Interprovinciale Baseline Informatiebeveiliging
[106] Provincie Noord-Holland, ambtelijk interview, 22 december 2015 en e-mail, 5 februari 2016
[107] Provincie Noord-Holland, ambtelijke interviews, 3 november en 22 december 2015
[108] Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen en Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
[109] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[110] Provincie Noord-Holland, ambtelijk interview, 7 december 2015 en e-mail, 5 maart 2016

vervolgstappen te formuleren.[111] In het feitelijk wederhoor heeft de provincie aangegeven dat deze afspraak inmiddels heeft plaatsgevonden.[112]

In het contract met de leverancier zijn bepalingen opgenomen over het (laten) uitvoeren van audits.[113] De ambtelijke organisatie heeft aangegeven het voornemen te hebben om een ICT penetratietest te laten uitvoeren op de kantoorautomatisering, nadat de migratie naar de huidige leverancier is afgerond en de systemen in een stabiele situatie terecht zijn gekomen.[114] In het feitelijk wederhoor heeft de provincie aangegeven dat de penetratietest inmiddels is uitgevoerd en dat de resultaten in mei 2016 zijn opgeleverd.[115]

Generieke maatregelen uitgevoerd door provincie
Daarnaast voert de provincie zelf een aantal generieke maatregelen met betrekking tot informatieveiligheid uit. Dit betreffen maatregelen op het gebied van mens & organisatie, basisinfrastructuur en het deel van de ICT-gerelateerde maatregelen dat niet de verantwoordelijkheid is van de externe leverancier. De uitvoering vindt verspreid over verschillende sectoren van de directie Concernzaken plaats. Het resterende deel van de ICT-gerelateerde maatregelen wordt uitgevoerd door de sector Informatievoorziening & ICT. Maatregelen met betrekking tot mens & organisatie zijn de verantwoordelijkheid van de sector HRM en maatregelen gericht op de basisinfrastructuur worden uitgevoerd door de sector Facility Management.[116] Desgevraagd heeft de ambtelijke organisatie aangegeven dat de betreffende sectoren zelf – vanuit het principe van integraal management – een concretisering (nadere uitwerking) van de generieke maatregelen hebben gemaakt.[117]

De provincie heeft geen registratiesysteem waarin de uitvoering van de generieke maatregelen wordt bijgehouden. Hierdoor heeft de provincie geen zicht of de maatregelen worden uitgevoerd. Wel wordt de stand van zaken van de uitvoering bijgehouden in de interprovinciale monitor van het Cibo. Dit is een instrument voor zelfevaluatie en wordt jaarlijks door elke provincie ingevuld. De bevindingen worden interprovinciaal besproken in het Cibo. In de interprovinciale monitor geeft elke provincie per maatregel een eigen inschatting van de stand van zaken.[118] Dit betreft volgens de Rekenkamer geen controle of de maatregelen *daadwerkelijk* zijn uitgevoerd. De Kwartiermaker informatieveiligheid van de provincie geeft een inschatting op basis van gesprekken met medewerkers (proceseigenaren) die verantwoordelijk zijn voor de uitvoering van de betreffende maatregel en zijn eigen oordeel.[119] Dit doet hij voor zowel de maatregelen die de provincie uitvoert als de maatregelen die door de externe leverancier worden uitgevoerd.[120] De interprovinciale monitor wordt verder toegelicht in hoofdstuk 5.

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.

[111] Provincie Noord-Holland, ambtelijk interview, 7 december 2015
[112] Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[113] Provincie Noord-Holland, ambtelijk interview, 22 december 2015 en Provincie Noord-Holland, e-mail, 16 maart 2016
[114] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 1 en Provincie Noord-Holland, e-mail, 5 februari 2016
[115] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[116] Provincie Noord-Holland, ambtelijke interviews, 7 en 16 december 2015
[117] Provincie Noord-Holland, e-mail, 16 maart 2016
[118] Provincie Noord-Holland (2014), Monitoringtool Cibo
[119] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[120] Provincie Noord-Holland (2014), Monitoringtool Cibo

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.

Bevinding 5

In 2012 heeft de provincie BIA's uitgevoerd op vijf processen, waarvoor tevens verdiepende risicoanalyses zijn uitgevoerd. Op basis van deze risicoanalyses zijn aanvullende maatregelen opgesteld. Volgens de ambtelijke organisatie wordt de voortgang hierop gemonitord binnen de sectoren waar de BIA is uitgevoerd.

Sinds 2012 voert de provincie – op enkele uitzonderingen na – geen BIA's uit op het niveau van bedrijfsprocessen als geheel, maar in het geval van wijziging van een systeem óf voorafgaand aan de implementatie van een nieuw systeem. Vaak wordt gewerkt met een ingekorte versie van de BIA. In veel gevallen worden de maatregelen uitgevoerd door externe partijen. De provincie maakt hierover afspraken in het contract. De provincie coördineert niet óf en op welke wijze aanvullende maatregelen worden uitgevoerd. Het is hierdoor niet goed in beeld of alle aanvullende maatregelen daadwerkelijk worden uitgevoerd.

In het kader van de verbijzonderde interne controle is de provincie van plan om in 2016 BIA's uit te voeren op de processen die de provincie als meest risicovol beschouwt.

Toelichting op de bevinding

In onderstaande toelichting wordt achtereenvolgens ingegaan op BIA's die in 2012 zijn uitgevoerd en BIA's die sinds dat jaar zijn uitgevoerd.

BIA's uitgevoerd in 2012

Zoals beschreven in paragraaf 3.1, heeft de directie in 2012 tegelijkertijd met het vaststellen van het informatieveiligheidsbeleid het document Beleidsimplementatie acties en professionaliteitsstappen vastgesteld.[121] In dit document worden de processen met betrekking tot het uitvoeren van BIA's nader uitgewerkt. Eén van de stappen die ten behoeve van dit document is genomen, is het uitvoeren van BIA's. De provincie heeft in 2012 vijf processen geselecteerd waarop BIA's zijn uitgevoerd:

- Vergunningverlening
- Subsidieverlening
- Verkeersmanagement
- Aanbesteding
- Salaris & Beloning

De selectie is tot stand gekomen op basis van interviews met de directie, Concern control, directiecontrol Middelen (nu: Concernzaken) en de sectormanagers ICT Regie, Facilitaire Dienstverlening en Personele Dienstverlening.[122] De BIA's zijn uitgevoerd tijdens een workshop op 10 mei 2012, waarbij proceseigenaren en inhoudelijk experts aanwezig waren. Voor elk van de vijf processen is de impact van de mate van beveiliging op de beschikbaarheid, integriteit en vertrouwelijkheid ingeschat op laag, midden of hoog.

Op basis van de resultaten van de BIA's zijn twee processen geselecteerd waarvoor verdiepende risicoanalyses zijn uitgevoerd: Aanbesteding en Verkeersmanagement. Voor beide processen zijn de risico's van verschillende aandachtsgebieden afgezet tegen de risicobereidheid. De risicobereidheid is bepaald door het gezamenlijk vaststellen van de maximaal toelaatbare waarden voor de kans van optreden van een gebeurtenis en de hoogte van de impact. De risicoanalyses hebben geleid tot een overzicht van maatregelen die genomen moeten worden.[123] De ambtelijke organisatie heeft aangegeven dat de maatregelen voor het proces Aanbesteding zijn verwerkt in procedures en de sector die verantwoordelijk is voor het proces Verkeersmanagement zelfstandig aan de slag is gegaan met de implementatie van de maatregelen. Volgens de provincie wordt de voortgang hierop binnen de sector gemonitord.[124]

De ambtelijke organisatie heeft aangegeven dat er tevens verdiepende risicoanalyses zijn uitgevoerd voor de processen Vergunningverlening, Subsidieverlening en Salaris & Beloning. Deze risicoanalyses zijn niet opgenomen in het document Beleidsimplementatie acties en professionaliteitsstappen. Volgens de ambtelijke organisatie hebben deze risicoanalyses geleid tot aanscherping van de procesbeschrijvingen. De ambtelijke organisatie heeft aangegeven dat de processen via interne controles worden getoetst aan de procesbeschrijvingen.[125]

BIA's uitgevoerd sinds 2012

Eén van de aanbevelingen uit het document Beleidsimplementatie acties en professionaliteitsstappen was om het uitvoeren van BIA's voort te zetten op andere processen.[126] Sinds 2012 is het proces met betrekking tot het uitvoeren van BIA's echter veranderd en worden BIA's doorgaans uitgevoerd in het geval van een wijziging van

[121] Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen
[122] Sinds 1 januari 2016 zijn de namen van deze sectoren gewijzigd in respectievelijk Informatievoorziening & ICT, Facility Management en HRM
[123] Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen
[124] Provincie Noord-Holland, e-mail, 16 maart 2016
[125] Provincie Noord-Holland, e-mail, 16 maart 2016
[126] Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen

een systeem óf voorafgaand aan de implementatie van een nieuw systeem.[127] Dit betekent dat BIA's achteraan in de keten worden uitgevoerd en er geen BIA's worden uitgevoerd op het niveau van bedrijfsprocessen als geheel.[128] De ambtelijke organisatie heeft aangegeven dat er enkele uitzonderingen zijn. Zo zijn er BIA's uitgevoerd op de processen Burgemeestersbenoemingen en de wet BIBOP.[129]

In veel gevallen wordt gewerkt met een ingekorte versie van de BIA, onder andere omdat het uitvoeren van een volledige BIA als tijdsintensief wordt ervaren. In de ingekorte versie wordt een aantal basisvragen gesteld, gericht op de eisen aan informatieveiligheid ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid.[130]

Volgens het informatieveiligheidsbeleid zijn de directies verantwoordelijk voor het periodiek uitvoeren van risicoanalyses binnen hun directie en het nemen van besluiten met betrekking tot het al dan niet accepteren van risico's. De directies dienen volgens dit beleid proceseigenaren aan te stellen die gedelegeerd verantwoordelijk zijn voor de beveiliging van het proces.[131] Dit betekent dat het initiatief om een BIA uit te voeren bij de proceseigenaar ligt. In paragraaf 2.2 kwam echter naar voren dat niet alle proceseigenaren actief invulling geven aan hun verantwoordelijkheid ten aanzien van informatieveiligheid en dat ICT-adviseurs van de directie Concernzaken doorgaans het initiatief nemen om BIA's uit te voeren.[132] Naast de proceseigenaar en de ICT-adviseur zijn de projectmanager, informatiemanager en functioneel beheerder doorgaans betrokken bij het uitvoeren van een BIA. De betrokkenen geven gezamenlijk aan welke risico's er zijn en welke aanvullende maatregelen er moeten worden genomen.[133]

De proceseigenaar bepaalt uiteindelijk of risico's worden geaccepteerd of dat aanvullende maatregelen worden genomen.[134] De ambtelijke organisatie heeft aangegeven dat een groot deel van de aanvullende maatregelen wordt uitgevoerd door externe leveranciers. Volgens de ambtelijke organisatie worden de eisen met betrekking tot aanvullende maatregelen opgenomen in het contract met de betreffende leverancier. Ook is in de eisen opgenomen dat de leverancier in het bezit moet zijn van een ISO 27001 certificaat dat gedurende de looptijd van het contract geldig is en dat de provincie een onafhankelijke audit mag laten uitvoeren.[135] De provincie coördineert niet óf en op welke wijze de proceseigenaren aanvullende maatregelen (laten) uitvoeren.[136] Het is hierdoor niet goed in beeld of alle aanvullende maatregelen daadwerkelijk worden uitgevoerd.

Het proces met betrekking tot BIA's in 2016

In 2016 zal een verbijzonderde interne controle op informatieveiligheid worden uitgevoerd. Dit betreft een interne controle die zal worden uitgevoerd door iemand buiten het proces, bijvoorbeeld een directiecontroller. De verbijzonderde interne controle zal onder andere gericht zijn op het uitvoeren van BIA's. In het verbijzonderde interne controleplan 2016 staat beschreven dat de provincie BIA's zal uitvoeren op de processen die de provincie thans als meest risicovol beschouwt: Inkopen en aanbesteden, Treasury, Subsidieverlening, Belasting en leges, Grondzaken en Personeel. Volgens het plan zal de provincie op termijn alle processen aan een BIA

[127] Provincie Noord-Holland, ambtelijke interviews, 16 en 22 december 2015
[128] Provincie Noord-Holland, ambtelijk interview, 22 december 2015
[129] Provincie Noord-Holland, ambtelijk interview, 7 december 2015
[130] Provincie Noord-Holland, ambtelijk interview, 22 december 2015
[131] Provincie Noord-Holland (2012), informatiebeveiligingsbeleid
[132] Provincie Noord-Holland, ambtelijke interviews, 3 november en 7 en 22 december 2015
[133] Provincie Noord-Holland, ambtelijk interview, 22 december 2015 en Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[134] Provincie Noord-Holland, ambtelijke interviews, 7 en 22 december 2015
[135] Provincie Noord-Holland, ambtelijk interview, 22 december 2015
[136] Provincie Noord-Holland, ambtelijke interviews, 16 en 22 december 2015

onderwerpen. Ook staat in het plan beschreven dat de provincie een oordeel zal geven over de opzet, het bestaan en de werking van het informatiebeveiligingsproces binnen de genoemde processen.[137]

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? Oftewel, dit criterium gaat na of de informatie in de praktijk daadwerkelijk voldoende is beschermd tegen toegang door onbevoegden.

Bevinding 6

De Rekenkamer heeft de praktijktoets niet uitgevoerd, omdat de provincie zich in de beginfase van het onderzoek in de overgangsfase van de ene naar de andere leverancier van de kantoorautomatisering bevond. Het uitvoeren van een praktijktoets wordt door het Nationaal Cyber Security Centrum van het ministerie van Veiligheid en Justitie afgeraden in een dergelijke kritieke periode, waarin het systeem substantiële veranderingen ondergaat. Ook in de maanden na de overstap blijft het kwetsbaar.

Zoals eerder naar voren kwam, heeft de provincie een groot deel van de kantoorautomatisering uitbesteed aan een externe leverancier. In de beginfase van het onderzoek bevond de provincie zich in de overgangsfase van de ene naar de andere leverancier. Dit is op zichzelf al een kwetsbare periode wanneer het gaat om de beschikbaarheid van de systemen. Het uitvoeren van een praktijktoets naar het functioneren van deze systemen wordt in een dergelijk kritieke periode, waarin het systeem substantiële veranderingen ondergaat, door het Nationaal Cyber Security Centrum van het ministerie van Veiligheid en Justitie afgeraden.[138] Daarom heeft de Rekenkamer de praktijktoets in deze provincie niet uitgevoerd. Aangezien het een aantal maanden kan duren voordat de systemen na een dergelijke overstap in een stabiele situatie terechtkomen, heeft de Rekenkamer ook later in het onderzoeksproces geen mogelijkheid gezien om een dergelijke praktijktoets verantwoord te laten plaatsvinden.

Uit de Concernmanagementrapportage van periode 1 van 2014 blijkt dat de provincie het voornemen heeft om een ICT penetratietest te laten uitvoeren op de kantoorautomatisering, nádat de migratie is afgerond en de systemen in een stabiele situatie terecht zijn gekomen.[139] In het feitelijk wederhoor heeft de provincie aangegeven dat de penetratietest inmiddels is uitgevoerd en dat de resultaten in mei 2016 zijn opgeleverd.[140]

[137] Provincie Noord-Holland (2015), Verbijzonderde Interne Controleplan 2016
[138] Govcert.nl (2010), Pentesten doe je zo. Een handleiding voor opdrachtgevers [sinds 2012 is Govcert onderdeel van het Nationaal Cyber Security Centrum van het ministerie van Veiligheid en Justitie]
[139] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 1
[140] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016

| 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
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 heeft de Rekenkamer onderzocht hoe alle medewerkers[141] 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.

[141] Met 'alle medewerkers' bedoelt de Rekenkamer het bestuur, het management, medewerkers, ingehuurd personeel en externe gebruikers

Bevinding 7

De provincie heeft in 2013, 2014 en 2015 aandacht besteed aan het versterken van de bewustwording van het belang van informatieveiligheid van medewerkers. De bewustwordingsactiviteiten in 2015 waren voornamelijk gericht op communicatie over een mystery guest-onderzoek. Dit had een informerend en interactief karakter. Het betrof een herhaling van een mystery guest-onderzoek uitgevoerd in 2013. De resultaten van het onderzoek in 2015 tonen aan dat de bewustwording van medewerkers is verbeterd ten opzichte van 2013, hoewel het onderzoek ook een aantal kwetsbaarheden aantoont die gelijkenissen hebben met de bevindingen van 2013. De provincie besteedt in 2016 opnieuw aandacht bewustwording. Daarnaast heeft de provincie diverse documenten in de organisatie verspreid waarmee medewerkers bekend worden gemaakt met hun verantwoordelijkheden in informatieveiligheid.

Toelichting op de bevinding

In onderstaande paragrafen wordt achtereenvolgens ingegaan op de uitvoering van bewustwordingsprogramma's en de documenten en richtlijnen waarmee medewerkers bekend worden gemaakt met de verantwoordelijkheden die zij hebben op het gebied van informatieveiligheid.

4.1.1 Uitvoering van bewustwordingsprogramma

De provincie heeft in 2013, 2014 en 2015 aandacht besteed aan het versterken van bewustwording van medewerkers.[142] In 2015 is hiervoor een communicatieplan opgesteld, waarin de doelstellingen, strategie, communicatiemiddelen en een planning van activiteiten gericht op het versterken van bewustwording zijn opgenomen. De doelstellingen zijn als volgt beschreven:

- Alle medewerkers zijn zich bewust van mogelijke risico's op het gebied van informatieveiligheid;
- Medewerkers zien dat zij hierin zelf ook een belangrijke rol vervullen;
- Medewerkers nemen hierdoor zelf verantwoordelijkheid om alert te zijn, risico's te signaleren en indien nodig zelf actie te ondernemen.[143]

Het communicatieplan en de bewustwordingsactiviteiten zijn uitgevoerd door de Kwartiermaker informatieveiligheid, in samenwerking met de sector Communicatie.[144] De activiteiten zijn zowel gericht op het informeren van medewerkers, het interactief betrekken van medewerkers als op het bieden van inzicht in hun eigen handelen.[145]

Mystery guest-onderzoek

De bewustwordingsactiviteiten waren voornamelijk gericht op communicatie over een *mystery guest*-onderzoek, dat in 2015 is uitgevoerd. Dat is een onderzoek waarbij een externe, onafhankelijke partij de opdracht heeft gekregen om zichzelf als onbevoegd persoon toegang te verschaffen tot een aantal locaties van de provincie. Het doel van het onderzoek was het testen van de weerbaarheid van de organisatie tegen onbevoegden, die toegang probeerden te krijgen tot informatie van de provincie. Het gaat hierbij niet alleen om digitale en papieren informatie, maar ook om informatie die berust bij medewerkers en ingehuurde personen.[146] Het onderzoek had daarnaast tot doel om de bewustwording van medewerkers te vergroten, door inzicht te geven in hun eigen handelen ten aanzien van informatieveiligheid.[147] Het mystery guest-onderzoek van 2015 was een herhaling van

[142] Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015 en Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[143] Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015
[144] Provincie Noord-Holland, ambtelijk interview, 10 november 2015
[145] Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015
[146] LBVD (2015), Managementsamenvatting mystery guest, 23 april
[147] Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015

een mystery guest-onderzoek in 2013 en liet verbeteringen zien. Toch toont het onderzoek van 2015 ook een aantal kwetsbaarheden aan die gelijkenissen hebben met het onderzoek van 2013.[148]

De provincie heeft op verschillende manieren gecommuniceerd over de resultaten van het mystery guest-onderzoek van 2015. Zo is er een bericht op het intranet verschenen over de bevindingen.[149] De ambtelijke organisatie heeft daarnaast aangegeven dat de directeuren de bevindingen en aandachtspunten hebben besproken in de managementteams.[150]

Overige bewustwordingsactiviteiten
Naast de bewustwordingsactiviteiten in het kader van het mystery guest-onderzoek, heeft de provincie in 2015 gecommuniceerd over het veilig gebruiken van smartphones.[151] Hiervoor heeft de provincie gebruikgemaakt van een factsheet van het Nationaal Cyber Security Centrum.[152]

De ambtelijke organisatie heeft aangegeven dat er in 2016 opnieuw bewustwordingsactiviteiten zullen worden uitgevoerd, waaronder het ophangen van posters in het provinciehuis en actieve communicatie over richtlijnen voor het delen van bestanden.[153] In het feitelijk wederhoor heeft de provincie aangegeven dat er inmiddels een phishingmail-actie is uitgevoerd, waarover is gecommuniceerd via het intranet, en dat er promotiemateriaal is gemaakt voor bewustwordingsactiviteiten.[154]

Er is geen bewustwordingsprogramma voor Statenleden.[155] Tijdens het inwerkprogramma voor Statenleden is wel aandacht besteed aan informatieveiligheid: Statenleden hebben een training gevolgd over veilig digitaal werken.[156] Ook is aandacht besteed aan informatieveiligheid tijdens een training over het gebruik van de applicatie iBabs.[157]

4.1.2 Documenten en richtlijnen m.b.t. verantwoordelijkheden informatieveiligheid
Naast de uitvoering van de bewustwordingsactiviteiten die zijn beschreven in voorgaande paragraaf, heeft de provincie verschillende documenten in de organisatie verspreid waarmee zij medewerkers bekendmaken met de verantwoordelijkheid die zij hebben in hun dagelijks handelen op het gebied van informatieveiligheid. Tabel 5 geeft een overzicht van deze documenten, met een korte toelichting op het document en de doelgroep.

[148] LBVD (2013), Managementsamenvatting mystery guest, 3 oktober
[149] Provincie Noord-Holland (2015), Mysterieuze bezoekers [bericht op het Plein], 3 april
[150] Provincie Noord-Holland, e-mail, 16 maart 2016
[151] Provincie Noord-Holland (2015), Communicatie informatieveiligheid
[152] Nationaal Cyber Security Centrum (2014), Veilig gebruik van smartphones en tablets. Risico's en maatregelen
[153] Provincie Noord-Holland, e-mail, 16 maart 2016
[154] Provincie Noord-Holland, e-mail, 3 juni 2016
[155] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[156] AVK (2015), Veilig digitaal werken, training security awareness
[157] Provincie Noord-Holland, e-mail, 25 februari 2016

Tabel 5 Overzicht van documenten met betrekking tot verantwoordelijkheden van medewerkers op het gebied van informatieveiligheid

Document	Toelichting	Doelgroep
Privacyreglement e-mail en internetgebruik (2002)[158]	Bekendmaken van medewerkers met verantwoordelijkheden en procedures m.b.t. e-mail en internetgebruik	Bestaande / nieuwe medewerkers
Reglement personeelspas (2013)[159]	Bekendmaken van medewerkers met procedures rondom het gebruik van de personeelspas	Bestaande / nieuwe medewerkers
Richtlijnen gebruik social media (2013)[160]	Handreiking voor zakelijk en privégebruik van social media	Bestaande / nieuwe medewerkers
Richtlijn wachtwoordgebruik (2013)[161]	Handreiking voor het instellen en gebruiken van wachtwoorden	Bestaande / nieuwe medewerkers
Tips voor veilig digitaal samenwerken (2013)[162]	Handreiking voor het veilig delen van documenten en overdragen van taken	Bestaande / nieuwe medewerkers
Tips voor veilig gebruik van smartphones en tablets (2014)[163]	Bekendmaken van medewerkers met risico's m.b.t. gebruik smartphones en tablets en tips om er veilig mee te werken	Medewerkers
Integriteitverklaring[164]	Verklaring waarin opdrachtnemer zich committeert aan afspraken m.b.t. integriteit.	Externe inhuur

De provincie heeft een intranetpagina over informatieveiligheid, waar is beschreven wat er onder informatieveiligheid wordt verstaan. Ook bevat de pagina een product- en dienstencatalogus, richtlijnen en een vraagbaak.[165]

De provincie heeft een introductieprogramma voor nieuwe medewerkers, dat twee keer per jaar wordt aangeboden. Informatieveiligheid is geen onderdeel van het introductieprogramma. De ambtelijke organisatie heeft aangegeven dat zij de intentie heeft om informatieveiligheid in het programma op te nemen. Nieuwe medewerkers leggen tijdens het introductieprogramma de ambtseed af.[166]

Extern ingehuurd personeel tekent bij aanvang van de opdracht een integriteitsverklaring (zie Tabel 5).

[158] Provincie Noord-Holland (2002), Privacyreglement e-mail en internetgebruik
[159] Provincie Noord-Holland (2008), Reglement personeelspas 2008
[160] Provincie Noord-Holland (2013), Richtlijnen gebruik sociale media
[161] Provincie Noord-Holland (2013), Richtlijn wachtwoordgebruik
[162] Provincie Noord-Holland (2013), Tips voor veilig digitaal samenwerken
[163] Nationaal Cyber Security Centrum (2014), Veilig gebruik van smartphones en tablets. Risico's en maatregelen
[164] Provincie Noord-Holland, Integriteitsverklaring
[165] Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015
[166] Provincie Noord-Holland, ambtelijke interviews, 3 en 10 november 2015

| 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 & control 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.[167]

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
In de Programmabegroting 2016 wordt informatieveiligheid expliciet genoemd in de paragraaf Bedrijfsvoering. In eerdere jaren was dit niet het geval. De ambtelijke organisatie heeft aangegeven dat zij de intentie heeft om informatieveiligheid in de jaarstukken van 2016 op te nemen. Daarnaast is informatieveiligheid opgenomen in de concernmanagementrapportages van 2014 en 2015.

Toelichting op de bevinding

Rapportage aan GS en PS
In de Programmabegroting 2016 wordt informatieveiligheid expliciet genoemd in de paragraaf Bedrijfsvoering.[168] In de begroting staat vermeld dat de activiteiten uit het informatieveiligheidsbeleidsplan uit 2012 verder ter hand worden genomen en zijn geclusterd in drie verantwoordelijkheidsgebieden:

- Activiteiten binnen de directies;
- Activiteiten binnen het concern;
- (Systeem)toetsende activiteiten

[167] Cibo en IPO (2014), Agenda voor ontwikkeling informatieveiligheid provincies 2014
[168] Provincie Noord-Holland (2015), Programmabegroting 2016

In voorgaande jaren werd informatieveiligheid niet genoemd in de Programmabegroting. Ook werd niet over informatieveiligheid gerapporteerd in de jaarstukken. Desgevraagd heeft de ambtelijke organisatie aangegeven dat zij de intentie heeft om informatieveiligheid op te nemen in de jaarstukken 2016.[169]

In paragraaf 2.1 is beschreven dat GS het informatieveiligheidsbeleid in de vergadering van 17 juli 2012 hebben vastgesteld en dat het document ter kennisname naar PS is gezonden. Ook is in deze paragraaf beschreven dat er nog geen periodieke rapportages specifiek over informatieveiligheid aan GS zijn.

Rapportage aan directie
Informatieveiligheid is opgenomen in de concernmanagementrapportages van 2014 (periode 1[170], 2[171] en 3[172]) en 2015 (periode 1[173] en 2[174]).[175] In elke rapportage staat een aantal specifieke aandachtsgebieden of activiteiten op het gebied van informatieveiligheid genoemd, met daarbij een planning, de stand van zaken ten opzichte van de planning en een toelichting op het aandachtsgebied of de activiteit. Zoals beschreven in paragraaf 2.1, zijn er nog geen periodieke rapportages specifiek over informatieveiligheid gericht aan de directie. Dergelijke schriftelijke rapportages vinden ad hoc plaats.[176]

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.[177]

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.

[169] Provincie Noord-Holland, ambtelijk interview, 3 november 2015
[170] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 1
[171] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 2
[172] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 3
[173] Provincie Noord-Holland (2015), Concernmanagementrapportage, viermaandsrapportage 2015, periode 1
[174] Provincie Noord-Holland (2015), Concernmanagementrapportage, viermaandsrapportage 2015, periode 2
[175] De Concernmanagementrapportage periode 3 van 2015 was begin 2016 nog niet gereed.
[176] Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[177] Cibo en IPO (2014), Convenant Interprovinciale Regulering Informatieveiligheid

Bevinding 9

De provincie heeft in 2013 en 2015 mystery guest-onderzoeken laten verrichten door een extern bureau. De resultaten van het onderzoek in 2015 laten verbeteringen zien ten opzichte van het onderzoek in 2013. Het onderzoek van 2015 toont ook een aantal kwetsbaarheden aan, die gelijkenissen vertonen met de bevindingen van 2013. De resultaten van beide onderzoeken zijn onder de aandacht gebracht van de directie en hebben tot vervolgacties geleid. De Concernmanagementrapportage van periode 1 2014 gaf aan dat de provincie voornemens was om een ICT penetratietest te laten uitvoeren op de kantoorautomatisering, maar dat deze vertraging heeft opgelopen vanwege overstap naar een andere leverancier. De penetratietest is in 2016 uitgevoerd. Verder heeft de externe accountant een toets uitgevoerd op informatieveiligheid in het kader van de jaarrekeningcontrole. De aandachtspunten van de onafhankelijke onderzoeken zijn besproken met GS en de directie en hebben tot vervolgacties geleid. In 2016 zal de provincie een verbijzonderde interne controle op informatieveiligheid uitvoeren.

Toelichting op de bevinding

In onderstaande toelichting wordt ingegaan op de onafhankelijke onderzoeken naar informatieveiligheid die de provincie sinds 2013 heeft uitgevoerd of laten uitvoeren.

Mystery guest-onderzoeken 2013 en 2015

Zoals beschreven in hoofdstuk 4, heeft de provincie in 2013 en 2015 mystery guest-onderzoeken laten verrichten door een extern bureau. Hierbij heeft het externe bureau de opdracht gekregen om zichzelf als niet-bevoegd persoon toegang te verschaffen tot een aantal locaties van de provincie. Het doel was het testen van de weerbaarheid van de organisatie tegen onbevoegden die toegang proberen te krijgen tot provinciale informatie.[178]

De resultaten van het onderzoek in 2013 – die kritisch waren – zijn onder de aandacht gebracht van de directie. Volgens de ambtelijke organisatie is er naar aanleiding van het onderzoek extra aandacht geweest voor schermbeveiliging en richtlijnen voor het ontvangen van bezoekers en voor de beveiliging bij de receptie. De ambtelijke organisatie heeft aangegeven dat de omgangsregels voor het dagelijks gebruik van de gebouwen worden gemonitord door de sector Facilitaire Dienstverlening.[179]

De resultaten van het mystery guest-onderzoek in 2015 laten verbeteringen zien ten opzichte van het onderzoek in 2013. Toch komen uit het onderzoek kwetsbaarheden naar voren die gelijkenissen vertonen met de bevindingen van 2013.[180] De resultaten van het onderzoek van 2015 zijn onder de aandacht gebracht van de directie. Naar aanleiding van de bevindingen is één technische beheersmaatregel geformuleerd. De ambtelijke organisatie heeft aangegeven dat deze maatregel is uitgevoerd. Daarnaast heeft de provincie op verschillende manieren gecommuniceerd over de resultaten van het mystery guest-onderzoek om de bewustwording van medewerkers te vergroten (zie hoofdstuk 4). De ambtelijke organisatie heeft aangegeven de intentie te hebben om het onderzoek in 2017 te herhalen.[181]

ICT Penetratietest

De Concernmanagementrapportage van periode 1 van 2014 geeft aan dat de provincie een ICT penetratietest wil laten uitvoeren op de kantoorautomatisering, maar dat deze vertraagd is.[182] Zoals beschreven in hoofdstuk 3,

[178] LBVD (2013), Managementsamenvatting mystery guest, 3 oktober en LBVD (2015), Managementsamenvatting mystery guest, 23 april
[179] Provincie Noord-Holland, e-mail, 16 maart 2016
[180] LBVD (2015), Managementsamenvatting mystery guest, 23 april
[181] Provincie Noord-Holland, e-mail, 16 maart 2016
[182] Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 1

heeft de provincie de kantoorautomatisering uitbesteed aan een derde partij en bevond de provincie zich in de tweede helft van 2015 in de overgangsfase van de ene naar de andere leverancier. Volgens de Concernmanagementrapportage zal de test worden uitgevoerd nádat de overstap van de ene naar de andere leverancier is afgerond. In het feitelijk wederhoor heeft de provincie aangegeven dat de penetratietest inmiddels is uitgevoerd en dat de resultaten in mei 2016 zijn opgeleverd.[183]

Toets op informatieveiligheid in kader van jaarrekeningcontrole
Daarnaast heeft de externe accountant in 2013 een toets uitgevoerd op informatieveiligheid in het kader van de jaarrekeningcontrole.[184] De provincie heeft aangegeven dat de externe accountant deze toets jaarlijks uitvoert. De bevindingen worden besproken met zowel de directie als de gedeputeerde. De aandachtspunten zijn vervolgens door sectoren binnen de directie Concernzaken en door Concern control opgepakt.[185]

Verbijzonderde interne controles
Zoals beschreven in paragraaf 3.2, zal de provincie in 2016 een verbijzonderde interne controle uitvoeren op informatieveiligheid. Dit betreft een interne controle die wordt uitgevoerd door iemand buiten het proces. De provincie heeft voor 2016 hiervoor een concernbreed verbijzonderde interne controleplan opgesteld[186], dat op 21 december 2015 is vastgesteld door de directie.[187] De provincie zal in het kader van de verbijzonderde interne controle BIA's uitvoeren op de processen die als meest risicovol worden beschouwd. Ook zal de provincie een oordeel geven over de opzet, het bestaan en het resultaat van de informatieveiligheid binnen deze processen.[188]

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 door 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 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.[189]

[183] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[184] Provincie Noord-Holland (2014), Doorwerking IT Management Letter 2013
[185] Provincie Noord-Holland, reactie feitelijk wederhoor, 27 mei 2016
[186] Provincie Noord-Holland (2015), Verbijzonderde Interne Controleplan 2016
[187] Provincie Noord-Holland (2015), Nota directie, betreft: concernbreed verbijzonderde interne controleplan 2016
[188] Provincie Noord-Holland (2015), Verbijzonderde Interne Controleplan 2016
[189] Provincie Zuid-Holland (2014), Monitoringtool Cibo

Het oordeel wordt gegeven door middel van een cijfer 1 tot en met 4. De betekenis van deze cijfers is weergegeven in Tabel 6.

Tabel 6 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 daadwerkelijk heeft uitgevoerd. En als dit het geval is, of de resultaten van deze monitor zijn besproken met de directie, welke acties daaruit zijn voortgekomen en of deze ook zijn uitgevoerd.

Bevinding 10

De provincie heeft in 2014 en 2015 de zelfevaluatie uitgevoerd. In de interprovinciale monitor 2014 heeft de provincie per maatregel een inschatting gegeven van de mate van implementatie. Het is voor de Rekenkamer niet navolgbaar óf en welke acties de provincie op basis van de resultaten zal ondernemen. Wel worden de maatregelen met de laagste scores omgezet als speerpunt in het concernjaarplan. De interprovinciale monitor 2015 is veel uitgebreider ingevuld dan de monitor 2014, waardoor het navolgbaar is waarop het oordeel is gebaseerd. Ook heeft de provincie voor meer maatregelen acties gedefinieerd. De bevindingen van de monitor worden niet besproken met de directie.

Toelichting op de bevinding

In onderstaande toelichting wordt achtereenvolgens ingegaan op de interprovinciale monitor in 2014, de interprovinciale monitor in 2015 en de opvolging van de bevindingen uit de monitor.

Interprovinciale monitor (zelfevaluatie) 2014

De interprovinciale monitor (zelfevaluatie) 2014 is ingevuld door de Kwartiermaker informatieveiligheid. Per maatregel heeft hij een inschatting gegeven van de stand van zaken van de uitvoering. Zoals aangegeven in paragraaf 3.2, betreft dit volgens de Rekenkamer geen controle of de maatregelen daadwerkelijk zijn uitgevoerd. De Kwartiermaker heeft een inschatting gegeven op basis van gesprekken met medewerkers (waaronder proceseigenaren) die verantwoordelijk zijn voor de uitvoering van de betreffende maatregel en zijn eigen oordeel.[190]

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 ‘fysieke beveiliging en beveiliging van de omgeving’ en ‘beheer van communicatie- en bedieningsprocessen’. Van de elf categorieën scoort de provincie het laagst op ‘beheer van informatiebeveiligingsincidenten’ en ‘bedrijfscontinuïteitsbeheer’.[191]

In totaal zijn er 133 maatregelen opgenomen in de monitor. De monitor biedt voor elke maatregel ruimte voor opmerkingen of een toelichting op het gegeven oordeel. De provincie heeft bij 8 van de 133 maatregelen een

[190] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[191] Provincie Noord-Holland (2014), Monitoringtool Cibo

toelichting gegeven op het oordeel. Voor de overige 125 maatregelen is het voor de Rekenkamer niet navolgbaar waarop het oordeel is gebaseerd en of het oordeel volgens de provincie goed genoeg is. Ook is er per maatregel ruimte voor een toelichting op de te nemen acties naar aanleiding van het oordeel. De Kwartiermaker heeft deze acties bij 6 van de 133 maatregelen ingevuld. Voor het merendeel van de maatregelen is het voor de Rekenkamer niet navolgbaar óf en welke acties de provincie op basis van het oordeel zal ondernemen. Wel heeft de ambtelijke organisatie aangegeven dat de maatregelen met de laagste scores worden omgezet als speerpunt in het concernjaarplan.[192]

Hoewel de bevindingen van de zelfevaluatie interprovinciaal zijn besproken en vergeleken, is het aan de provincies zelf om te bepalen op welke wijze zij de monitor invullen en welke mate van detail daarbij wordt gehanteerd. Hierdoor ontstaan verschillen tussen de provincies in de manier waarop de monitor wordt ingevuld.

Interprovinciale monitor (zelfevaluatie) 2015
De provincies hadden afgesproken de interprovinciale monitor 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, dan zal het Cibo mogelijk aansturen op het opstellen van een nulmeting op basis van deze nieuwe IBI.[193] De provincie heeft ervoor gekozen om de bestaande monitor ook voor 2015 in te vullen.

Ook in de monitor 2015 is voor elke categorie de totale score van de opzet, het bestaan en de werking van de maatregelen opgeteld. Uit dit totaalbeeld blijkt dat de provincie van de elf categorieën het beste scoort op ‘fysieke beveiliging en beveiliging van de omgeving’ en ‘organisatie’. Van de elf categorieën scoort de provincie het laagst op ‘beheer van beveiligingsincidenten’ en ‘verwerving, ontwikkeling en onderhoud van informatiesystemen’.[194] De monitor 2015 is veel uitgebreider ingevuld dan de monitor 2014: de provincie heeft bij alle maatregelen een toelichting gegeven op het oordeel. Hierdoor is het navolgbaar waarop het oordeel is gebaseerd. Verder heeft de provincie voor meer, maar niet voor alle maatregelen acties gedefinieerd.

Opvolging van bevindingen uit de interprovinciale monitor
De bevindingen van de monitor worden niet besproken met de directie. Wel is het concernjaarplan, waarin de maatregelen met de laagste scores uit de monitor zijn opgenomen, onder de aandacht gebracht van de directie.[195] De ambtelijke organisatie heeft aangegeven dat de bevindingen daarnaast op indirecte wijze onder de aandacht van de algemeen directeur worden gebracht. De algemeen directeur is lid van de Ambtelijke Adviescommissie (AAC) Middelen, die onderdeel is van het IPO. De bevindingen van de monitor worden in het Cibo besproken, waarna de bevindingen naar de AAC Middelen gaan.[196]

[192] Provincie Noord-Holland, ambtelijk interview, 16 december 2015
[193] Provincie Zuid-Holland (2016), e-mail 8 februari 2016 van een Cibo-lid vanuit Zuid-Holland
[194] Provincie Noord-Holland (2015), Monitoringtool Cibo
[195] Provincie Noord-Holland, reactie op feitelijk wederhoor, 27 mei 2016
[196] Provincie Noord-Holland, ambtelijk interview, 16 december 2015

Bijlage A Geraadpleegde bronnen

Algemeen

- AVK (2015), Veilig digitaal werken, training security awareness
- 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
- Govcert.nl (2010), Pentesten doe je zo. Een handleiding voor opdrachtgevers
- LBVD (2013), Managementsamenvatting mystery guest, 3 oktober
- LBVD (2015), Managementsamenvatting mystery guest, 23 april
- Nationaal Cyber Security Centrum (2014), Veilig gebruik van smartphones en tablets. Risico's en maatregelen
- Onderzoeksraad voor de Veiligheid (2012), Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt
- Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
- 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
- iBewustzijn Overheid (2015), www.ibewustzijnoverheid.nl
- Justitia.nl (2016), www.justitia.nl
- Logius (2016), www.logius.nl
- Taskforce BID (2015), www.taskforcebid.nl

Provincie Noord-Holland

- Provincie Noord-Holland, Integriteitsverklaring
- Provincie Noord-Holland (2002), Privacyreglement e-mail en internetgebruik
- Provincie Noord-Holland (2008), Reglement personeelspas 2008
- Provincie Noord-Holland (2011), Onderzoeksrapport Nulmeting informatiebeveiliging, 20 december
- Provincie Noord-Holland (2012), Beleidsimplementatie acties en professionaliteitsstappen
- Provincie Noord-Holland (2012), brief van GS aan PS, betreft: informatiebeveiligingsbeleid, 21 december
- Provincie Noord-Holland (2012), Informatiebeveiligingsbeleid
- Provincie Noord-Holland (2012), Inrichten beveiligingsorganisatie
- Provincie Noord-Holland (2012), Nota directie, betreft: informatiebeveiligingsbeleid, 28 juni
- Provincie Noord-Holland (2012), Openbare besluitenlijst van de vergadering van gedeputeerde staten van Noord-Holland, 17 juli 2012
- Provincie Noord-Holland (2013), Richtlijnen gebruik sociale media
- Provincie Noord-Holland (2013), Richtlijn wachtwoordgebruik
- Provincie Noord-Holland (2013), Tips voor veilig digitaal samenwerken
- Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 1
- Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 2
- Provincie Noord-Holland (2014), Concernmanagementrapportage, viermaandsrapportage 2014, periode 3
- Provincie Noord-Holland (2014), Doorwerking IT Management Letter 2013

- Provincie Noord-Holland (2014), Monitoringtool Cibo
- Provincie Noord-Holland (2015), Communicatie informatieveiligheid 2015
- Provincie Noord-Holland (2015), Concernmanagementrapportage, viermaandsrapportage 2015, periode 1
- Provincie Noord-Holland (2015), Concernmanagementrapportage, viermaandsrapportage 2015, periode 2
- Provincie Noord-Holland (2015), Memo aan Stuurgroep I&I, betreft: wijziging Wet bescherming persoonsgegevens
- Provincie Noord-Holland (2015), Monitoringtool Cibo
- Provincie Noord-Holland (2015), Mysterieuze bezoekers [bericht op het Plein], 3 april
- Provincie Noord-Holland (2015), Nota directie, betreft: concernbreed verbijzonderde interne controleplan 2016
- Provincie Noord-Holland (2015), Plan van aanpak meldplicht datalekken, 2 november
- Provincie Noord-Holland (2015), Programmabegroting 2016
- Provincie Noord-Holland (2015), Verbijzonderde interne controleplan 2016
- Provincie Noord-Holland (2016), Implementatie meldplicht datalekken, voortgangsrapportage periode 1 september 2015 tot en met 15 januari 2016
- Provincie Noord-Holland (2016), Nota directie, betreft: governance informatiebeveiliging, 4 februari

Bijlage B Geraadpleegde personen

Algemeen

- De heer. T. Bosma, Senior Onderzoeker Rekenkamer Den Haag
- De heer H. Wesseling, Voormalig hoofd Taskforce Bestuur en Informatieveiligheid Dienstverlening
- De heer D. Leguit, Voormalig Manager Taskforce Bestuur en Informatieveiligheid Dienstverlening

Provincie Noord-Holland

- Mevrouw K. Grevers, Adviseur interne communicatie, sector Communicatie, directie Concernzaken
- De heer W. Kegel, Medewerker Concern control
- De heer E. Krijgsman, Commissieadviseur Natuur, Landbouw en Milieu
- De heer C. Loggen, Gedeputeerde ICT en Personeel en organisatie
- De heer J. Loggen, Waarnemend Statengriffier
- De heer W. Olijve, Adviseur I&I, sector Informatievoorziening en ICT, directie Concernzaken
- De heer F.D. Ossewaarde, Chief Information Officer, directie Concernzaken
- Mevrouw P. Verbeek, Strategisch ICT adviseur, sector Informatievoorziening en ICT, directie Concernzaken

Bijlage C Afkortingen en begrippen

Afkortingenlijst

BIA	Business Impact Analyse
Cibo	Centraal Informatiebeveiligingsoverleg
GS	Gedeputeerde Staten
IBI	Interprovinciale Baseline Informatiebeveiliging
ICT	Informatie- en Communicatietechnologie
IPO	Interprovinciaal Overleg
P&C	Planning & Control
PS	Provinciale Staten

Begrippenlijst

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.
BIA	De Business Impact Analyse (BIA) is de standaardmethode voor het uitvoeren van een risicoanalyse (zie: Risicoanalyse).
Beschikbaarheid	In het kader van informatieveiligheid betreft Beschikbaarheid de eigenschap dat informatie toegankelijk en bruikbaar is op verzoek van een bevoegde functionaris.
Cibo	Het Cibo is het Centraal Informatiebeveiligingsoverleg (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 Interprovinciale Baseline Informatiebeveiliging (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