



Jaarverslag informatiebeveiliging 2021

Zaaknummer:	HK-0005826
Versiedatum	08-03-2022
Status:	Concept
Opgesteld door:	Tarik Fakir
Vastgesteld door:	College van B&W
V-Classificatie:	Intern document

Inhoudsopgave

1.	INLEIDING	3
2.	MANAGEMENTSAMENVATTING	3
2.1	ALGEMEEN BEELD EN RESULTATEN	4
2.2	VEILIGHEIDSINCIDENTEN	4
2.3	ENSIA	5
2.4	METING VAN DE BIO	6
3.	VERBETERINGEN PER BIO HOOFDSTUK	7

1. Inleiding

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan beheersmaatregelen om de beveiliging van onze informatievoorzieningen te waarborgen. Hierbij houden wij rekening met de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens en kritische processen.

Dit jaarverslag is een verantwoording over de kwaliteit van de informatiebeveiliging over 2021. Met het jaarverslag legt het college verantwoording af aan de gemeenteraad, het Rijk en haar toezichthouders. Het jaarverslag is tot stand gekomen door zelfevaluaties en audits die door een onafhankelijke partij (externe IT-auditor) is uitgevoerd. De kwaliteit van de informatiebeveiliging is beoordeeld aan de hand van de normen van de Baseline Informatiebeveiliging Overheid (BIO)¹ en de NOREA². De BIO en NOREA geven richtlijnen voor beheersing van de informatiebeveiliging door het inrichten en uitvoeren van een set van organisatorische en technische beheersmaatregelen. Dit jaarverslag kan worden gebruikt in het meten van de kwaliteit van de informatiebeveiliging over 2021.

Er is gekozen om de informatiebeveiliging over 2021 op hoofdlijnen te beschrijven aan de hand van een toetsing in hoeverre de normen zijn gerealiseerd en nageleefd. In dit jaarverslag wordt de kwaliteit ten opzichte van het voorgaande jaar vergeleken en toegelicht. Dat geeft inzicht in de inspanningen die de organisatie en haar partners doen om de informatiebeveiliging te vergroten en op de inspanningen die nog te leveren zijn om de informatiebeveiliging naar een nog hoger niveau te brengen.

2. Managementsamenvatting

Dit verslag geeft de uitkomsten weer van de uitgevoerde (zelf)evaluaties informatieveiligheid over het jaar 2021. Deze evaluaties zijn gebaseerd op de Baseline Informatieveiligheid Overheid (BIO) en de ENSIA³. Er wordt op één moment in het jaar gerapporteerd over de huidige status.

Vanuit deze evaluaties is eveneens de verantwoording aan de stelselhouders /toezichthouders afgelegd, de zogenaamde verticale verantwoording. Zo zijn de verantwoordingen (uittreksels) over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) op 11 januari 2022 toegestuurd naar de Rijksdienst voor Identiteitsgegevens, de Autoriteit Persoonsgegevens en het Ministerie van BZK.

De verantwoordingen over de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond en de Basisregistratie Wet waardering

¹ De Baseline Informatiebeveiliging Overheid is een instrument bestaande uit een uitgebreide normen set waarmee gemeenten in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging.

² NOREA is de beroepsorganisatie van IT-auditors in Nederland en beheert het register van gekwalificeerde IT – auditors (Re's)

³ Eenduidige Normatiek Single Information Audit

onroerende zaken zijn tijdig vóór 8 februari 2022 opgeleverd aan het Ministerie van I&W⁴. De verantwoordingen voor Suwinet en DigiD zijn binnen de gestelde deadline aan het ministerie van SZW en Logius aangeleverd. Dit is gedaan door middel van een collegeverklaring, de bevindingen uit onze zelfevaluatie en het Assurance rapport van een externe RE-auditor. De zelfevaluatie is getoetst door deze externe auditor. De auditor heeft de collegeverklaring op juistheid beoordeeld en heeft de uitkomsten van het onderzoek vermeld in het Assurance rapport. Met beide documenten voldoet Hollands Kroon aan de verantwoordingsplicht voor Suwinet en DigiD.

2.1 Algemeen beeld en resultaten

De organisatie heeft qua meting ten opzichte van het jaar daarvoor stappen voorwaarts gezet. Dat heeft te maken met een aantal doorgevoerde maatregelen vanuit het BIO normenkader. Op het moment van schrijven liggen er nog een aantal geprioriteerde maatregelen die nog uitgevoerd moeten worden. Er is vooruitgang geboekt in het vormgeven van vastgesteld beleid, processen (procesbeschrijvingen, vastgestelde richtlijnen en werkinstructies) en eigenaarschap. De onderwerpen bedrijfscontinuïteit, “logging” en zichtbare interne controles zijn van groot belang willen wij onze digitale weerbaarheid vergroten. Het is daarnaast van groot belang om de lage bezetting van onze ICT-organisatie te compenseren door de dagelijkse beheer activiteiten te documenteren. Dat is nodig in het geval van uitval, vervanging. Maar ook om een goed beeld te krijgen bij alle ICT-risico’s die wij lopen en de ICT-kwaliteit die moet worden behouden.

2.2 Veiligheidsincidenten

In 2021 hebben zich, gelijk aan voorgaande jaren, een aantal veiligheidsincidenten voorgedaan. Deze waren snel te mitigeren maar hadden een verwaarloosbare impact op onze bedrijfsvoering. Deze incidenten hadden voornamelijk te maken met software en hardware waarin een kwetsbaarheid is geconstateerd. Onze connecties met de informatiebeveiligingsdienst (IBD) en de rijksoverheid ‘s eigen ‘computer emergency response team’ (CERT) hebben bijgedragen aan het tijdig mitigeren en handelen bij deze incidenten. Het Computer Emergency Response Team maakt onderdeel uit van het NCSC (Nationaal Cyber Security Centrum) dat onder het Ministerie van Justitie en Veiligheid valt. De CERT is een 24-uurshulp, die behulpzaam is bij beveiligings (cyber) incidenten en daarbij ondersteuning en advisering biedt.

In december 2021 werd de wereld geconfronteerd met een kwetsbaarheid onder de noemer ‘log4j’. Deze kwetsbaarheid had een wereldwijde impact. Het stelt kwaadwillende in staat om op afstand een stukje code te injecteren om toegang tot systemen te krijgen. Het Nationaal Cyber Security Centrum heeft deze kwetsbaarheid op 10 december 2021 aan ons gemeld. Wij hebben daarna direct onze ICT-omgeving hierop gescand. Ook hebben wij onze ICT-partners gevraagd ons te informeren mocht het lek invloed

⁴ De BAG, BGT, BRO en WOZ kennen elk in ENSIA ook een domein specifieke vragenlijst en een specifieke verantwoordingsrapportage. Deze is separaat ter vaststelling aan het College voorgelegd en aangeboden aan het Ministerie van I&W en de Waarderingskamer.

hebben op diensten en services die wij afnemen. Uit onze eigen scans kwam naar voren dat wij een aantal updates moesten doorvoeren, maar dat het lek verder geen impact had op onze infrastructuur en dienstverlening.

Verder hebben zich incidenten voorgedaan die veroorzaakt zijn door de menselijke factor. In een omgeving waar gewerkt wordt kunnen nu eenmaal fouten gemaakt worden. Er is wederom weer een stijging waargenomen van geregistreerde meldingen. Dit heeft naar alle waarschijnlijkheid te maken met een verhoging van bewustwording. Collega's worden zoveel mogelijk geïnformeerd via de gebruikelijke communicatiekanalen over verschillende informatiebeveiligingsonderwerpen en actualiteiten rondom fraude, phishing, hack en ransomware risico's. Daarnaast worden er via het 'my learning factory' leerplatform trainingen en workshops aangeboden in het kader van informatiebeveiliging en privacy.

2.3 ENSIA

Het ENSIA-traject dient verder te worden doorontwikkeld in relatie tot het ISMS⁵. De inspanningen voor ENSIA vinden jaarlijks onder hoge tijdsdruk plaats, daar willen we vanaf en dat kan ook door een betere afstemming met het ISMS.

Waar we bij de introductie van ENSIA in 2017 zagen dat de focus op het gebied van informatiebeveiliging vooral lag bij ENSIA is er een duidelijke kanteling naar het ISMS. Het ISMS dat gebaseerd is op de BIO is gericht op continu verbeteren en is immers onze basis voor het sturen en afleggen van verantwoording op het gebied van informatiebeveiliging. ENSIA is vooral bedoeld om het ministerie van BZK en de IT-auditor te voorzien van informatie voor hun eigen informatiebehoefte waarbij op onderdelen een audit plaatsvindt. Hierbij gaat het voornamelijk om Suwinet en DigiD dat nog geen 10% uitmaakt van het totaal aantal ENSIA-vragen.

ENSIA raakt een groot deel van de BIO-normen niet terwijl deze een belangrijk onderdeel uitmaken van het verbeteren van onze digitale weerbaarheid. Daarnaast zien we dat ENSIA steeds breder wordt ingezet voor onderwerpen met vooral inhoudelijke vragen die niets of weinig te maken hebben met informatiebeveiliging. Een voorbeeld hiervan is de introductie van de WOZ nog even los van de BAG, BRO en BGT die eveneens weinig met informatiebeveiliging te maken hebben en vooral inhoudelijk (domein specifiek) van aard zijn.

Hoewel we zorgvuldig rekening houden met ENSIA, moet dit proces volgend zijn op het ISMS voor zover het de BIO-normen raakt. Voor al het overige is ENSIA leidend en behoort de ENSIA-coördinator daarvoor belast te zijn. De CISO blijft dan beter in staat om te blijven focussen op informatiebeveiliging zoals bedoeld vanuit de BIO. Uiteraard is dan afstemming nodig tussen de taken vanuit het ISMS en de ENSIA-coördinator. De taak van de ENSIA-coördinator is ervoor te zorgen dat het ENSIA-portaal tijdig voorzien wordt van de benodigde gegevens. Dat vereist een jaarlijkse afstemming met de CISO voor het ISMS-deel en met de collega's die belast zijn met het beheer van de BRP, reisdocumenten, Suwinet, DigiD, BAG, BRO,

⁵ Information security management system. Een continu verbeterproces in de vorm van een systeem of applicatie.

BGT en WOZ. Een goede afstemming zorgt er ook voor dat daarmee de jaarlijkse druk aan het einde van het jaar als gevolg van ENSIA geminimaliseerd wordt.

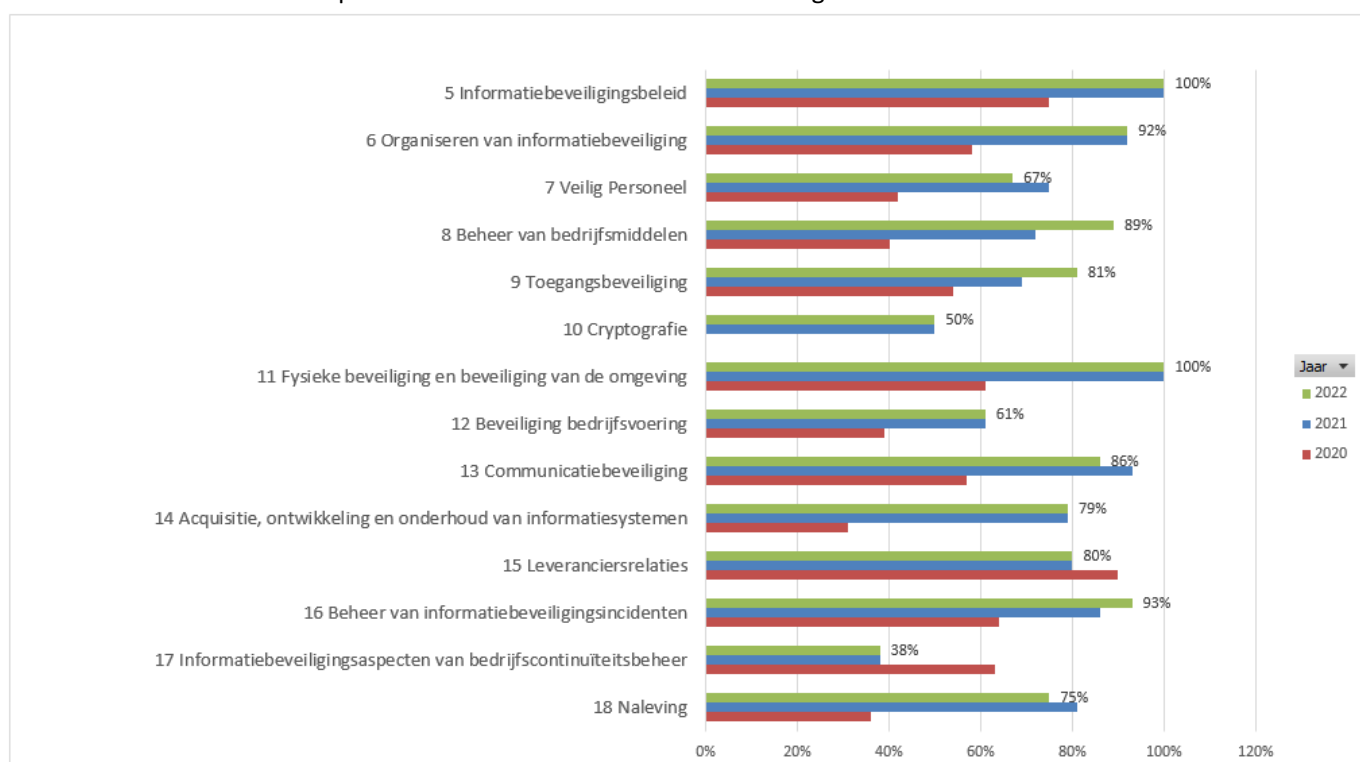
Er wordt een voorstel gemaakt voor een betere afstemming tussen ENSIA en het ISMS waarbij de jaarlijkse druk als gevolg van ENSIA beperkt kan blijven en de focus gericht blijft op continu verbeteren vanuit het ISMS.

Het verantwoordingsproces over 2021 is anders verlopen dan voorheen. Dit had te maken met de overgang naar een andere kernapplicatieleverancier (Pink Roccade). Om het ENSIA-proces te voltooien dienden er een aantal nieuwe DigiD aansluitingen te worden aangevraagd. De toegangsbeveiliging en verdere inrichting op het gebied van beveiliging verliep zoals was verwacht. Een uitzondering hierop was de applicatie die ingezet wordt t.b.v. de taken binnen het sociaal domein. Hieruit bleek tijdens het verantwoordingsproces dat er een aantal applicatietoegangsfunctionaliteiten misten. Deze waren nodig om aan de auditor te kunnen tonen dat wij grip hebben op de toegangsbeveiliging binnen deze applicatie. Het gemis van deze functionaliteiten is d.m.v een tussentijdse werkwijze opgelost. Pink Roccade heeft aangegeven dat deze functies binnen de applicatie in 2022 zullen worden toegevoegd. Het organiseren van de alternatieve werkwijze heeft ertoe geresulteerd dat het ENSIA-traject vertraging heeft opgelopen in het verticale en horizontale verantwoordingsproces. Deze is in week 21 (2022) afgerond.

2.4 Meting van de BIO

De eerste meting op basis van de BIO is in februari 2020 uitgevoerd met een gemiddelde score van 50%. De tweede meting is uitgevoerd in maart 2021 met een gemiddelde score van 71%. De derde meting is in februari 2022 uitgevoerd en levert een gemiddelde score op van 80%.

Grafisch ziet de score op de 14 hoofdstukken uit de BIO er als volgt uit:



In dit jaarverslag wordt ingegaan op datgene waar de focus op lag in 2021. Deze prioritering maakt ook onderdeel uit van het 'jaarplan informatiebeveiliging 2021-2022'.

Deze meting betreft een momentopname en geeft enkel weer hoe wij ervoor stonden aan het begin van 2021. In dit jaarverslag wordt een eerste vergelijking gemaakt ten opzichte van de meting die in 2020 is uitgevoerd. Voor de volledigheid is de meting van 2022 qua statistiek ook zichtbaar gemaakt. Over de meting van 2022 wordt verder inhoudelijk niet ingegaan. Het jaarverslag over 2022 dat in 2023 opgesteld gaat worden geeft inhoudelijke informatie en biedt inzicht in de meting(en) over 2022.

Op hoofdstukken 7, 13, en 18 er slechter wordt gescoord ten opzichte van het jaar daarvoor. Dit heeft te maken met de verandering die heeft plaatsgevonden in het kernapplicatie landschap en het ontbreken van de eerder benoemde functionaliteiten. Naar verwachting zal deze score consolideren zodra deze functionaliteiten beschikbaar worden gemaakt later dit jaar.

3. Verbeteringen per BIO hoofdstuk

De focus voor verbetering richt zich vooral op de hoofdstukken in de BIO die volgens de meting lager dan 70% scoren. Dat zijn de hoofdstukken 6 t/m 10, hoofdstuk 15 en 17.

3.1 Cryptografische beheersmaatregelen (hoofdstuk 10 van de BIO)

Ter bescherming van informatie is er beleid opgesteld voor het gebruik van crypto grafische beheersmaatregelen. Beleid voor het gebruik van crypto grafische beheersmaatregelen is nodig om de voordelen van het gebruik van crypto grafische technieken zo groot mogelijk en de risico's zo klein mogelijk te maken en om ongepast en onjuist gebruik te voorkomen.

Het beheer van crypto grafische sleutels is essentieel voor een doeltreffend gebruik van crypto grafische technieken Het beleid over het gebruik van crypto grafische beheersmaatregelen bevat eisen voor het beheren van crypto grafische sleutels tijdens hun gehele levenscyclus met inbegrip van het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van sleutels.

Binnen de gemeente is er een functionaris aangesteld die het beheer van crypto grafische sleutels uitvoert. De processen die hiermee gepaard gaan dienen nog formeel te worden gedocumenteerd.

3.2 Beveiliging bedrijfsvoering (hoofdstuk 12 van de BIO)

Zoals in paragraaf 2.1 is aangegeven, is aandacht nodig voor het documenteren van de dagelijkse beheeractiviteiten van ICT-beheer in de vorm van procedures, richtlijnen en werkinstructies. Het is niet uitgesloten dat hiervoor extra middelen nodig zijn voor het opstellen van deze documentatie. Deze documentatie is daarnaast van belang voor het verder professionaliseren van BCM ofwel bedrijfscontinuïteitmanagement waarin ICT-beheer een cruciale rol speelt.

De teams die hier een rol in spelen dienen aan te geven in hoeverre ruimte is voor het verder professionaliseren op dit gebied. De teams die hier een rol in spelen zijn immers de hoeders op het gebied van informatiebeveiliging voor de informatiesystemen en middelen die onder hun beheer vallen. Dat geldt dan vooral voor onze kritische applicaties waar sprake is van vertrouwelijke en privacygevoelige gegevens. Samen met deze teams zal er een voorstel gedaan worden voor een algehele procedure/werkinstructie die hen ondersteunt bij alle dagelijkse werkzaamheden.

3.3 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (hoofdstuk 17 van de BIO)

Wij scoren laag op dit onderdeel. Bedrijfscontinuïteit gaat niet alleen over ICT, maar raakt de hele organisatie. BCM is een proces gericht op het continu verbeteren van het vermogen van een organisatie om potentiële gevaren en de gevolgen van deze gevaren te identificeren, het hoofd te bieden en daarmee de continuïteit en het voortbestaan van een organisatie te waarborgen onder alle omstandigheden. Het gaat dan vooral om het treffen van preventieve maatregelen en het onderhouden van beheersmaatregelen en bekwaamheden om de bedrijfsactiviteiten tijdens een storing, ramp of calamiteit voort te zetten en de schade als gevolg hiervan zo beperkt mogelijk te houden.

In 2021 is aandacht gevraagd om BCM structureel te borgen in de organisatie. We hebben hiervoor een managementsysteem voor bedrijfscontinuïteit beschikbaar (BCMS) dat op dezelfde beheersingsprincipes is gebaseerd als het ISMS. Daarmee bereiken we een vorm van standaardisering als het gaat om interne beheersing over deze twee domeinen die onderling ook raakvlakken hebben. Er wordt gestart met een nulmeting om inzicht te krijgen waar we als organisatie staan op het gebied van BCM. Over de uitkomsten hiervan en de uitkomsten van een inventarisatie van alle kritieke processen over alle programma's, wordt een rapport opgesteld ten behoeve van de directie en het college. In dit rapport worden ook verbeter voorstellen gedaan.

Het is overigens niet de CISO die belast is met BCM, maar dit onderwerp wel op de bestuurlijke agenda kan zetten omdat de CISO wel belast is met de beveiligingsaspecten rond BCM zoals opgenomen in hoofdstuk 17 van de BIO.

Bijlagen: (met uitzondering van de bedrijf kritische verantwoordingen Suwinet en DigiD)

- 1a. Uittreksel Reisdocumenten (PUN);
- 1b. Uittreksel BRP;
- 1c. Verantwoording BAG, BGT, BRO;
- 1d. Verantwoording WOZ.