Provincie Noord-Holland

Onderzoeksplan

Audit informatiebeveiliging/ BIO bij PNH

Aan: Gedeputeerde Staten

Ambtelijk opdrachtgever: Dhr. J. Bierhuizen

Sector: Concerncontrol
Datum: 14-07-2022
Versie : Concept 1.0
1881050/1879159

Colofon

Projectnaam
Audit Informatiebeveiliging/BIO

In opdracht van
Dhr. E.P. Stigter
Gedeputeerde met ICT in portefeuille
Namens het college van Gedeputeerde Staten (GS)
Provincie Noord-Holland

Ambtelijk opdrachtgever
Dhr. J. Bierhuizen
Concerncontroller
Namens het college van Gedeputeerde Staten (GS)
Concerncontrol | Provincie Noord-Holland

Eindverantwoordelijke opdrachtnemer
Dhr. R. van Burk
Programmamanager Interne audit
Interne audit | Concerncontrol | Provincie Noord-Holland

Contactpersoon
Mw. A.E. Reijne, Senior Auditor
✉ annelies.reijne@noord-holland.nl

☎ 06 29678447Interne audit | Concerncontrol | Provincie Noord-Holland

Auditteam
Mw. A.E. Reijne, Senior Auditor

Dhr. J.Klappe, Senior Auditor

Dhr. R van Burk, programmamanager Audit

Kopie aan begeleidingsgroep

Inhoudsopgave

1 Opdrachtformulering 4
1.1 Inleiding en context 4
1.2 Auditdoelstelling 5
1.3 Onderzoeksvragen 5
1.4 Scope van onderzoek 56
1.5 Werkwijze 6
1.6 Referentiekader 8

2 Beheersaspecten 10
2.1 Organisatie 10
2.2 Informatie 10
2.3 Tijd 11
2.4 Kwaliteit 12
2.5 Geld 12
2.6 Informatie 12

1 Opdrachtformulering

1.1 Inleiding en context

In het auditjaarplan 2022 is informatiebeveiliging als onderwerp voor een onderzoek opgenomen. Op 21 december 2021 heeft Gedeputeerde Staten besloten om een onderzoek uit te laten voeren naar de informatiebeveiliging bij de provincie. Voor dat onderzoek kijken we naar de implementatie van het information security management system (ISMS). Een ISMS is randvoorwaardelijk voor een duurzame borging van de Baseline informatiebeveiliging overheid (BIO). De BIO is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen).

Gedeputeerde Staten hebben de volgende onderzoeksopdracht vastgesteld:

> *Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid [1](BIO) van kracht. De BIO is de voorgeschreven baseline binnen de overheid gebaseerd op de internationale norm voor informatiebeveiliging ISO 27001. Deze heeft de bestaande baselines informatieveiligheid voor Rijk, gemeenten, waterschappen en provincies vervangen.*
>
> *Startpunt van het onderzoek zijn de afspraken die gemaakt zijn tussen de provincies, als één van de overheidslagen. Wij onderzoeken of de provincie, gezien de genomen en geplande maatregelen, de afspraken kan nakomen en in hoeverre zij kan voldoen aan de BIO. Afhankelijk van de uitkomst van het onderzoek geven wij adviezen voor het voldoen aan de BIO.*

De BIO is een doorontwikkeling van de verschillende baselines die al langer binnen de overheid bestonden. De Interprovinciale Baseline Informatiebeveiliging (IBI) was de voorganger van de BIO waaraan provincies moesten voldoen. De BIO heeft een sterke focus op governance en risicomanagement.

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Dit proces kan worden ondersteund door een managementsysteem voor informatiebeveiliging (ISMS).

De BIO bevat een set met beheersmaatregelen waar overheden minimaal aan moeten voldoen. Het is, de naam zegt het al, een ‘baseline’. ISO 27001 biedt de systematiek voor een managementsysteem dat overheden en leveranciers kunnen gebruiken om informatiebeveiliging te beheersen. Dit kan betekenen dat overheden een managementsysteem voor informatiebeveiliging (ISMS) in kunnen richten volgens de standaarden van ISO 27001 en daarbij de beheersmaatregelen uit de BIO van toepassing verklaren.

De Provincie heeft gekozen voor het inrichten van een ISMS waarbij de BIO van toepassing is.[2]

---

[1] BIO versie 1.04zv

[2] Datastrategie 2021-2023 en Beleidskader informatiebeveiliging, juli 2021

Binnen het kwaliteitssysteem zijn de eerste stappen het maken van een beleidskader en een uitvoeringskader. Daarin zijn de verantwoordelijkheden vastgelegd en beschreven en hoe het uitvoeringskader zal moeten worden toegepast.

Onderdeel van het uitvoeringskader is het beveiligingsproces. Hierin wordt een risicoafweging gemaakt. Daarbij wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen de overheid beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

1.2 Auditdoelstelling

Het onderzoek heeft de volgende doelen:

1. Inzicht in de (bestuurlijke) afspraken gemaakt over de implementatie van de BIO en de mate waarin wordt voldaan aan die afspraken.
2. Inzicht in de status van de implementatie van het managementsysteem voor informatiebeveiliging (ISMS) per 1 juli 2022 bij de PNH.
3. Bij eventuele tekortkomingen bij de implementatie van de BIO en het ISMS volgen aanbevelingen om dit op te lossen.

1.3 Onderzoeksvragen

De centrale onderzoeksvraag voor dit onderzoek is:

In hoeverre kan de PNH, gezien de huidige status van de implementatie van het ISMS en met de gemaakte afspraken, voldoen aan de Baseline Informatiebeveiliging Overheid (BIO)?

Om antwoord te geven op de doelstelling zijn de volgende vragen geformuleerd.

1. *Welke afspraken zijn er gemaakt om te voldoen aan de BIO?*
2. *Welk implementatieplan cq. stappen heeft PNH vastgesteld om aan de BIO te voldoen?*
3. *Wat is de status van de implementatie van het managementsysteem van informatiebeveiliging (ISMS)?*
4. *Waar staat de PNH met betrekking tot informatiebeveiliging?*
5. *Indien PNH niet of deels voldoet aan de BIO: welke acties kunnen er genomen worden om (stapsgewijs) te voldoen aan de BIO?*

1.4 Scope van onderzoek

De BIO vormt het kader voor informatiebeveiliging bij de Overheid. Een werkend managementsysteem voor informatiebeveiliging (ISMS) is nodig om duurzaam te

kunnen voldoen aan de normen van de BIO. Dit onderzoek richt zich op de BIO. Daarbij onderzoeken we welke activiteiten zijn/worden ondernomen om aan de BIO normen te kunnen voldoen. En of de voorwaarden om te kunnen voldoen aan de BIO normen aanwezig zijn. In de ISO 27001 hoofdstuk 4 tot en met 10 zijn de normen voor de implementatie van informatiebeveiliging opgenomen, dit zijn vereisten voor een werkende ISMS. Daarom vormen deze het referentiekader voor dit onderzoek. We beoordelen het proces en de voorwaarden om te kunnen voldoen aan de BIO.

Wij gaan niet beoordelen of de specifieke beveiligingsmaatregelen van de BIO werken. Ook kijken we niet inhoudelijk naar de uitgevoerde BIA-toetsen[3]

1.5 Werkwijze

Het onderzoek wordt uitgevoerd door documentanalyse, interviews en het (laten) invullen van het selfassessment informatiebeveiliging. Het selfassessment met volwassenheidsmodel is een praktisch toepasbaar model. Het instrument helpt om het gesprek over informatiebeveiliging in de organisatie te voeren.

De aanpak om de onderzoeksvragen te beantwoorden is als volgt:

1. *Welke afspraken zijn er gemaakt om te voldoen aan de BIO?*

Inventariseren welke afspraken er zijn gemaakt door en voor de provincie om aan de baselines informatiebeveiliging te voldoen. Dit zijn de IBI (de voorloper van de BIO) en de BIO. Hiervoor doen wij onderzoek naar de afspraken op rijksniveau, interprovinciaal (IPO) en de afspraken bij de PNH.

2. *Welk implementatieplan cq. stappen heeft PNH vastgesteld om aan de BIO te voldoen?*

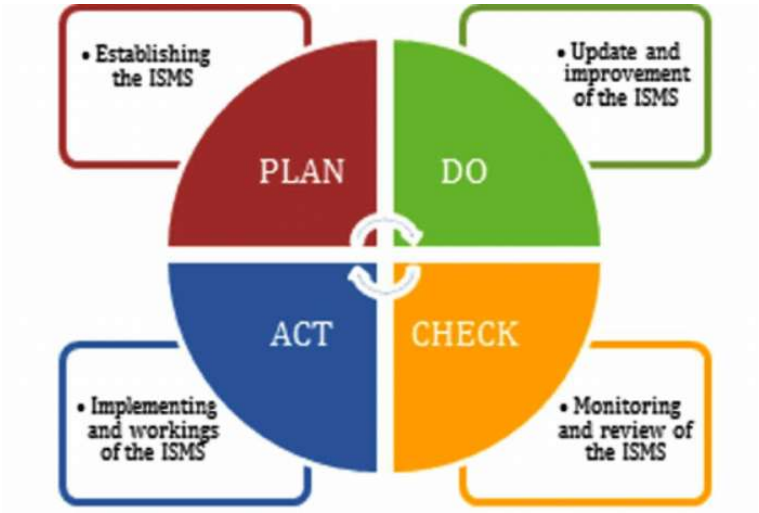
We onderzoeken welke concrete stappen PNH heeft gedefinieerd om aan de BIO te voldoen. Daarbij kijken we ook naar de projectorganisatie voor de implementatie van de ISO 27001, de BIO normen en de ISMS. In het referentiekader zijn de criteria voor de inrichting van een projectorganisatie opgenomen. (zie bijlage 1)

3. *Wat is de status van de implementatie van het managementsysteem van informatiebeveiliging (ISMS)?*

Een werkende ISMS is voorwaardelijk om duurzaam aan de BIO te kunnen voldoen. In een werkend systeem voor informatiebeveiliging wordt de PDCA cirkel per onderdeel periodiek doorlopen. Om te beoordelen wat de huidige status is van de implementatie van de ISMS, maken we gebruik van de door een externe auditor (DigiTrust) uitgevoerde nul en een-meting bij alle provincies naar ISO 27001: 2017 en de BIO eisen. De rapportage van de externe audit is opgeleverd in september 2021. We onderzoeken bij de uitvoerders van deze meting of we voldoende kunnen steunen op de een-meting.

[3] BIA: Business impact analyse: De BIA is vervangen door de BBN-toets. De BBN-toets dient hetzelfde doel als de BIA: juiste informatiebeveiligingsmaatregelen nemen ter bescherming van de betrouwbaarheid van systemen

Indien er in de tussentijd op onderdelen verbeteracties zijn uitgevoerd, zullen we die onderdelen opnieuw beoordelen. Dit stemmen we af met de (plaatsvervangend) CISO.



Figuur 1: PDCA cirkel van het managementsysteem van informatiebeveiliging (ISMS)

4. *Waar staat de PNH met betrekking tot informatiebeveiliging?*

Om te onderzoeken waar PNH staat met betrekking tot de informatiebeveiliging maken we gebruik van het selfassessment informatiebeveiliging met daarin een volwassenheidsmodel informatiebeveiliging[4]. Het selfassessment geeft de organisatie inzicht waar zij staat met informatiebeveiliging en wat er allemaal moet gebeuren.

We faciliteren het invullen van het selfassessment informatiebeveiliging door betrokken collega's van de PNH. Dit zijn de auditees die we ook zullen interviewen. De auditors geven vooraf tijdens de interviews een toelichting over het invullen van de vragenlijst. Na het verwerken van alle respons organiseren de auditors samen met het CIP (Centrum voor informatiebeveiliging en privacybescherming) een workshop waarin de verschillen worden besproken. Op deze manier krijgen we een afgestemd beeld over waar de organisatie staat met betrekking tot informatiebeveiliging. De namen van collega's die we hiervoor willen uitnodigen zijn opgenomen in bijlage 2.

5. *Indien PNH niet of deels voldoet aan BIO: welke acties kunnen er genomen worden om (stapgewijs) te voldoen aan de BIO?*

We onderzoeken welke activiteiten aantoonbaar zijn genomen en gepland om te voldoen aan de BIO. Daarbij onderzoeken we in hoeverre PNH met het realiseren van deze activiteiten kan komen tot een werkend ISMS, als voorwaarden voor de borging van de BIO normen. Wanneer de PNH niet of deels voldoet, onderzoeken we of er

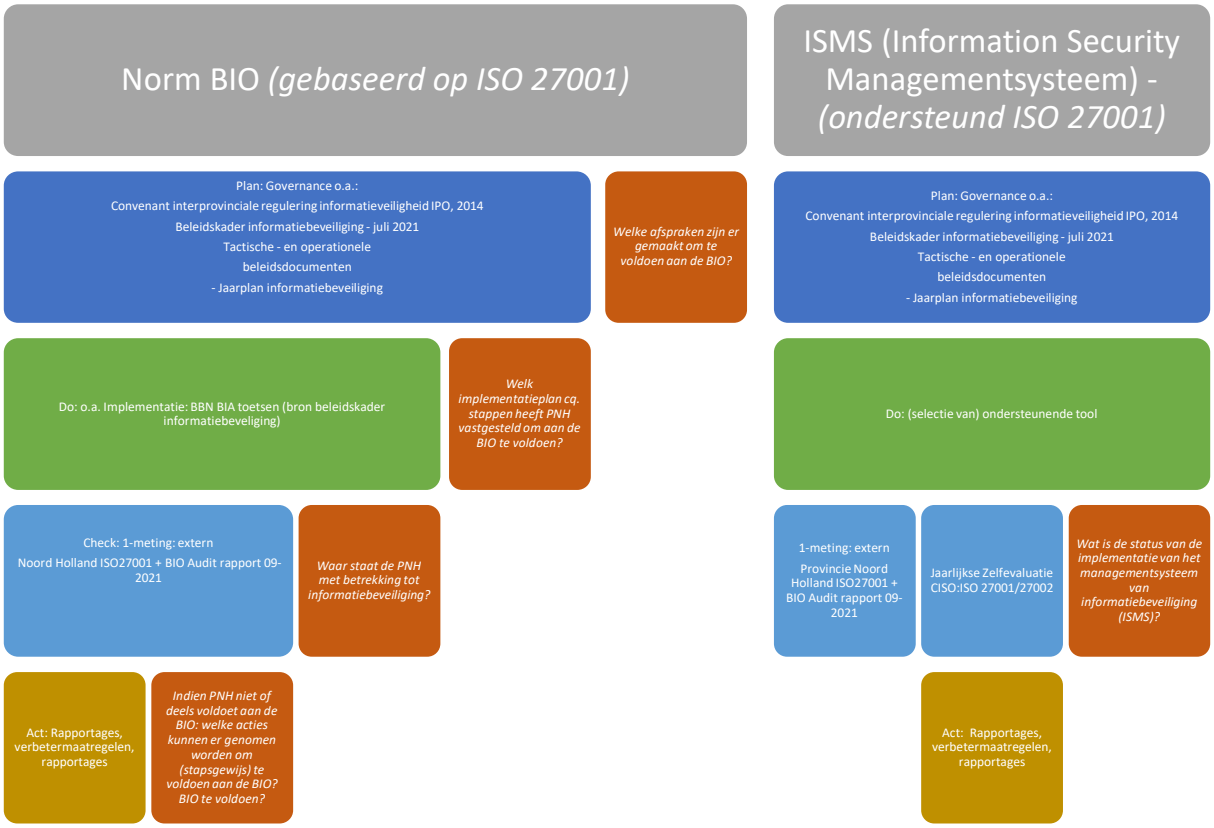
[4] Model is opgesteld door het CIP centrum informatiebeveiliging en privacybescherming, januari 2021.

activiteiten zijn of worden gepland om stapsgewijs aan de normen te voldoen. En of deze voldoende zijn om aan de BIO te voldoen.

Op basis van de bevindingen uit de deelvragen, beantwoorden we de centrale onderzoeksvragen:

In hoeverre kan de PNH, gezien de huidige status van de implementatie van het ISMS en met de gemaakte afspraken, voldoen aan de BIO?

Hieronder zijn onderzoeksvragen en de relatie met de BIO, ISO 27001 en ISMS weergegeven.

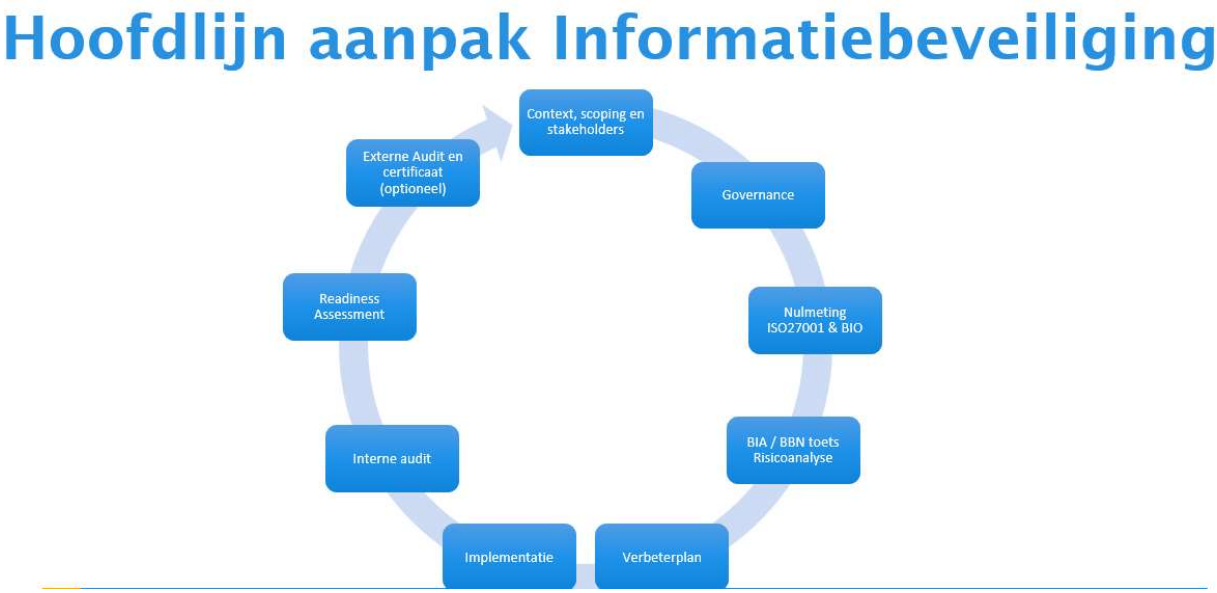


1.6 Referentiekader

Het referentiekader waaraan wordt getoetst zijn de elementen van de 'hoofdlijn aanpak BIO[5]' door de PNH. Voor het beoordelen van de status van de implementatie ISMS zijn deze aangevuld met de normen uit ISO 27001 hoofdstukken 4 tot en met 10. Om de ISMS te kunnen implementeren is een projectorganisatie nodig. De normen hiervoor zijn opgenomen aan begin van het referentiekader. Deze is opgenomen onder bijlage 1.

Daarnaast maken we gebruik van een Selfassessment informatiebeveiliging met Volwassenheidsmodel, zoals opgesteld door het Centrum Informatiebeveiliging en Privacybescherming, uit januari 2021. Dit model laten we invullen door sleutelfiguren in de organisatie. Het volwassenheidsmodel is een groeimodel. Het model geeft inzicht op welk volwassenheidsniveau de provincie gelet op de risico's zich moet bevinden. En waar zij zich momenteel bevindt. En wat er nog moet gebeuren om het gewenste volwassenheidsniveau te bereiken.

[5] Zie figuur 2



Figuur 2: aanpak informatiebeveiliging PNH

2 Beheersaspecten

2.1 Organisatie

Onder eindverantwoordelijkheid van Programmamanager Interne audit R. van Burk zullen de werkzaamheden worden uitgevoerd door Annelies Reijne, Senior Auditor en John Klappe, Senior Auditor.

Contactpersoon

Primair contactpersoon (SPOC; Single Point Of Contact) tijdens voor het auditteam om inhoudelijke/operationele zaken te bespreken is de (plaatsvervangend) CISO.

De begeleidingsgroep bestaat verder uit: Wil van Hooijdonk, concerncontrol adviseur I-domein, Petra Smoes, directiecontroller B&U, Nico Kluwen, directiecontroller CZ, Jeroen van Els, sectormanager CID, Han Roebers, plaatsvervangend directeur B&U, John Arkes, plaatsvervangend directeur Beleid

Wat vragen we aan de auditees?

Voor de interviews plannen we een klein uur, in principe hoeven ze zich hiervoor niet voor te bereiden. (duur 1 uur) Van het gesprek maken we een verslag, waarop we akkoord vragen aan de auditee. Hebben we juist weergegeven wat hij bedoelde? Voor het checken heeft auditee (duur 1 uur).

Aan de auditees vragen we om een selfassessment informatiebeveiliging in te vullen. Tijdens het interview geven we een korte uitleg. Ook zijn de auditors beschikbaar voor vragen (duur 1 uur). De auditors verwerken alle input. De resultaten van het selfassessment bespreken we in een workshop onder leiding van het CIP met auditees. Hiervoor plannen we een dagdeel.

De tijdsbelasting voor dit onderzoek die we aan de auditees vragen is ongeveer 7 uur.

Wat vragen we aan de begeleidingsgroep?

Met de begeleidingsgroep stemmen we de opzet van het onderzoek af. Aan de begeleidingsgroep presenteren we de voorlopige bevindingen en concept rapport. Zijn wij op de juiste weg? Ook formuleren we samen met hen de aanbevelingen. Voor de aanbevelingen organiseren we een bijeenkomst. Afhankelijk van de bevindingen en agenda's organiseren we tussentijds overlegmomenten of stemmen we per email af.

2.2 Informatie

Resultaat:

Het auditrapport geeft aan welke afspraken zijn gemaakt om te voldoen aan de BIO normen. Daarnaast geeft het rapport inzicht in de status van het managementsysteem van informatiebeveiliging (ISMS), welke voorwaardelijk is om duurzaam te kunnen voldoen aan de BIO. Daarnaast is geïnventariseerd op welk volwassenheidsniveau informatiebeveiliging de organisatie zich zou moeten bevinden. En waar de organisatie zich momenteel bevindt. En wat er nog

stapsgewijs moet gebeuren om de informatiebeveiliging op het gewenste niveau te organiseren.

Het rapport bestaat uit bevindingen, een volwassenheidsscan van huidige en gewenste niveau van informatiebeveiliging en aanbevelingen om stapsgewijs te kunnen voldoen aan het gewenste niveau van informatiebeveiliging.

Verspreiding van rapport

Het rapport wordt besproken in de begeleidingsgroep. Daarbij worden de feiten getoetst en de haalbaarheid van de aanbevelingen.

Interne Audit brengt het rapport uit aan de (ambtelijk) opdrachtgever, J. Bierhuizen. Aan de opdrachtgever wordt een bestuurlijke reactie gevraagd.

Het rapport wordt geagendeerd in de directie en de staven van de Gedeputeerde met ICT in portefeuille.. Het onderzoek is gekenmerkt als een Provinciewet 217a onderzoek. Dit betekent dat Gedeputeerde Staten dit rapport vaststellen en dit rapport ter kennisname verzenden aan Provinciale Staten en het rapport openbaar toegankelijk zal zijn.

2.3 Tijd

De uitvoering van het onderzoek vindt plaats in de periode maart t/m november 2022 De verwachte rapportdatum is in de eerste helft van 2023.

De verschillende fasen van het onderzoek zien er als volgt uit:

Fase	Mijlpalen	Periode
1. **Planning en vooronderzoeksfase**	Onderzoeksplan Referentiekader	maart tot en met juni
2. **Veldwerkfase**	Interviews, uitzetten selfassessment informatiebeveiliging, Analyse van bevindingen	juli tot en met september
	Resultaten selfassessment informatiebeveiliging bespreken	oktober
3. **Rapportagefase**	Auditrapport inclusief reactie auditee/ opdrachtgever	januari2023
4. **Evaluatiefase**	Evaluatie met auditee en of opdrachtgever (optioneel)	februari
5. **Follow-upfase**	Opvolging van aanbevelingen door concern control	6 maanden na publicatie rapport / nader te bepalen in overleg met de opdrachtgever

In deze fase van het onderzoek is de planning indicatief. Er kunnen zich omstandigheden voordoen dat de planning wordt aangepast.

2.4 Kwaliteit

Afstemmen onderzoeksplan en auditrapport

Hoor/wederhoor: Een conceptversie zal zowel met de (ambtelijk) opdrachtgever als met de auditee(s) worden afgestemd (hoor en wederhoor).

Kwaliteitsborging

Interne review: op zowel het onderzoeksplan en het auditrapport vindt er een interne review plaats door de auditmanager.

Draagvlak

Door de inzet van een selfassessment geeft de organisatie aan waar zij staat en wil staan met betrekking tot informatiebeveiliging. Het selfassessment kan worden ingezet om het gesprek met de organisatie te voeren over de informatiebeveiliging. Wat is nodig om te voldoen aan de minimale eisen? Welke randvoorwaarden dienen te worden ingevuld?

Om het draagvlak van de aanbevelingen te vergroten zullen eerst de bevindingen worden besproken en vervolgen de aanbevelingen gezamenlijk met de begeleidingsgroep en opdrachtgever worden geformuleerd.

2.5 Geld

Het onderzoek wordt uitgevoerd door provinciale auditors. Externe inhuur is niet aan de orde.

2.6 Informatie

Een overzicht van de documenten die relevant zijn voor dit onderzoek zijn opgenomen in bijlage 3.

Bijlage 1: referentiekader

Referentiekader om de implementatie van de informatiebeveiligingsnormen te beoordelen. Dit is gebaseerd op het in PNH gecommuniceerde model 'hoofdlijnen aanpak informatiebeveiliging' en ISO 27001 hoofdstukken 4 t/m 10. Om de BIO duurzaam te implementeren is een ISMS nodig. Om deze te implementeren is een projectorganisatie nodig. De vereisten voor de inrichting van een projectorganisatie zijn opgenomen in het referentiekader.

	Onderwerp	Toetspunten
	Projectorganisatie is opgezet	Om de implementatie van de baseline inclusief het ISMS bij PNH te realiseren is een projectorganisatie nodig. De projectorganisatie voor de implementatie is opgezet met: - commitment van leiding; - voldoende capaciteit is beschikbaar; - voldoende middelen zijn beschikbaar; - rollen, taken, bevoegdheden zijn vastgesteld; - mijlpalen zijn benoemd; - planning is aanwezig; - prioriteiten in groeipad BIO zijn vanuit risico's vastgesteld; - communicatieplan is opgesteld; - rapportages over voortgang aan stuurgroep/ verantwoordelijke.
1	Context, scoping en stakeholders *(ISO 27001, hoofdstuk 4* Context van de organisatie*)*	*(context)* **4.1 Inzicht verkrijgen in de organisatie en haar context** De organisatie moet externe en interne onderwerpen vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen. *(stakeholders)* **4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden** De organisatie moet vaststellen: a) welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging, en b) welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging. *(scoping van de ISMS)* **4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen** De organisatie moet de grenzen en toepasselijkheid van het managementsysteem voor informatiebeveiliging bepalen om het toepassingsgebied ervan vast te stellen. Bij het vaststellen van dit toepassingsgebied moet de organisatie: a) de in 4.1 genoemde externe en interne onderwerpen overwegen, evenals; b) de in 4.2 genoemde eisen, en c) raakvlakken en afhankelijkheden tussen de activiteiten die door de organisatie en de activiteiten die door andere organisaties worden verricht. Het toepassingsgebied moet als gedocumenteerde informatie beschikbaar zijn. *(ISMS met PDCA cirkel)* **4.4 Managementsysteem voor informatiebeveiliging** De organisatie moet een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren, in overeenstemming met de eisen van deze Internationale Norm.

2	Governance (ISO 27001, hoofdstuk 5 Leiderschap)	**5.1 Leiderschap en betrokkenheid** De directie moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor Informatiebeveiliging door: a) te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en aansluiten bij de strategische richting van de organisatie; b) te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van de organisatie worden geïntegreerd; c) te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn; d) het belang van een doeltreffend informatiebeveiligings-management en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren; e) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt; f) mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging; g) continue verbetering te bevorderen; en h) andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheids-gebieden.
		5.2 Beleid De directie moet een informatiebeveiligingsbeleid vaststellen dat: a) passend is voor het doel van de organisatie; b) informatiebeveiligingsdoelstellingen bevat (zie 6.2) of het kader biedt voor het vaststellen van informatiebeveiligingsdoelstellingen; c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging; en d) een verbintenis bevat tot continue verbetering van het managementsysteem voor informatiebeveiliging. Het beleid voor informatiebeveiliging moet: e) beschikbaar zijn als gedocumenteerde informatie; f) worden gecommuniceerd binnen de organisatie, en g) beschikbaar zijn voor belanghebbenden, voor zover van toepassing.
		5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd. De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot: a) het bewerkstelligen dat het managementsysteem voor informatiebeveiliging voldoet aan de eisen van deze Internationale Norm; en b) het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging aan de directie.
3	Nulmeting 27001 & BIO	Metingen in hoeverre PNH voldoet aan de baseline(s) zijn uitgevoerd. Uitkomsten zijn gecommuniceerd met verantwoordelijke. Eventueel is implementatieplan bijgesteld.
4	BIA / BBN toets, risicoanalyse (ISO 27001-hoofdstuk 6 Planning)	**6.1 Maatregelen om risico's te beperken en kansen te benutten** *6.1.1 Algemeen* Bij het plannen voor het managementsysteem voor informatiebeveiliging moet de organisatie de in 4.1 genoemde onderwerpen en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden aangepakt om: a) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt; b) ongewenste effecten te voorkomen of te beperken; en

		c) continue verbetering te bereiken. De organisatie moet: d) maatregelen plannen om deze risico's te beperken en kansen te benutten; e) plannen op welke wijze: 1) de maatregelen in haar managementsysteemprocessen voor informatiebeveiliging worden geïntegreerd en geïmplementeerd; en 2) de doeltreffendheid van deze maatregelen moet worden geëvalueerd. *6.1.2 Risicobeoordeling van informatiebeveiliging* De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die: a) risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder: 1) de risicoacceptatiecriteria; en 2) criteria voor het verrichten van risicobeoordelingen van informatiebeveiliging; b) waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, geldige en vergelijkbare resultaten opleveren; c) de informatiebeveiligingsrisico's identificeert: 1) het risicobeoordelingsproces voor informatiebeveiliging toepassen om de risico's in verband met het verlies van vertrouwen in, integriteit van en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en 2) de risico-eigenaren identificeren; d) de informatiebeveiligingsrisico's analyseert: 1) de potentiële gevolgen beoordelen indien de risico's die in 6.1.2 c) 1) zijn vastgesteld, zich zouden voordoen; 2) de realistische waarschijnlijkheid beoordelen van het voorkomen van de risico's die zijn vastgesteld in 6.1.2 c) 1); en 3) de risiconiveaus vaststellen; e) de informatiebeveiligingsrisico's evalueert: 1) de resultaten vergelijken van risicoanalyses met de risicocriteria die zijn vastgesteld in 6.1.2 a); en 2) de geanalyseerde risico's prioriteren voor risicobehandeling. De organisatie moet gedocumenteerde informatie bewaren over het risicobeoordelingsproces van informatiebeveiliging. *6.1.3 Behandeling van informatiebeveiligingsrisico's* De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen om: a) passende opties voor het behandelen van informatiebeveiligingsrisico's te kiezen, rekening houdend met de resultaten van de risicobeoordeling; b) alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor het behandelen van informatiebeveiligingsrisico's te implementeren; c) de beheersmaatregelen die hiervoor in 6.1.3 b) zijn vastgesteld te vergelijken met die in bijlage A, en om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten; d) een verklaring van toepasselijkheid op te stellen die bevat: - de benodigde beheersmaatregelen (zie 6.1.3 b) en c)); - een rechtvaardiging voor het opnemen ervan; - de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet, en - de rechtvaardiging voor het uitsluiten van in bijlage A genoemde beheersmaatregelen. e) een behandelplan voor informatiebeveiligingsrisico te formuleren; en

		f) van de risico-eigenaren goedkeuring te verkrijgen voor het behandelplan voor informatiebeveiligingsrisico en acceptatie van de overblijvende informatiebeveiligingsrisico's. De organisatie moet gedocumenteerde informatie bewaren over de behandelprocedure van informatiebeveiligingsrisico's.
		6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken De organisatie moet voor relevante functies en op relevante niveaus informatiebeveiligingsdoelstellingen vaststellen. De informatiebeveiligingsdoelstellingen moeten: a) consistent zijn met het informatiebeveiligingsbeleid; b) meetbaar zijn (indien praktisch uitvoerbaar); c) rekening houden met van toepassing zijnde informatiebeveiligingseisen en resultaten van risicobeoordeling en -behandeling; d) worden gecommuniceerd; en e) indien van toepassing, worden geactualiseerd. De organisatie moet gedocumenteerde informatie over de informatie-beveiligingsdoelstellingen bewaren. Bij het opstellen van planningen voor het bereiken van de informatiebeveiligingsdoelstellingen moet de organisatie vaststellen: f) wat er moet worden gedaan; g) welke middelen er nodig zijn; h) wie er verantwoordelijk is; i) wanneer het moet zijn voltooid; en j) hoe de resultaten zullen worden geëvalueerd.
	Ondersteuning (ISO 27001- hoofdstuk 7)	**7.1 Middelen** De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging.
		7.2 Competentie De organisatie moet: a) de noodzakelijke competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van de organisatie op het gebied van informatiebeveiliging beïnvloeden; b) bewerkstelligen dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring; c) waar van toepassing, maatregelen nemen om de benodigde competentie te verwerven, en de doeltreffendheid van de genomen maatregelen evalueren; en d) geschikte gedocumenteerde informatie als bewijsmateriaal van competentie bewaren.
		7.3 Bewustzijn Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van: a) het informatiebeveiligingsbeleid; b) hun bijdrage aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging, met inbegrip van de voordelen van verbeterde informatiebeveiligingsprestaties; c) de gevolgen van het niet voldoen aan de eisen van het management-systeem voor informatiebeveiliging.
		7.4 Communicatie De organisatie moet de behoefte vaststellen aan interne en externe communicatie die relevant is voor het managementsysteem voor informatiebeveiliging, waaronder: a) waarover te communiceren;

		b) wanneer te communiceren; c) met wie te communiceren; d) wie moet communiceren; en e) volgens welke processen de communicatie moet plaatsvinden.
		7.5 Gedocumenteerde informatie *7.5.1 Algemeen* Het managementsysteem voor informatiebeveiliging van de organisatie moet onder andere bevatten: a) gedocumenteerde informatie die deze Internationale Norm vereist; en b) de gedocumenteerde informatie die de organisatie vaststelt als noodzakelijk voor de doeltreffendheid van het managementsysteem voor informatiebeveiliging. *7.5.2 Creëren en actualiseren* Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor de/het passende: a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer); b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch); en c) beoordeling en goedkeuring van geschiktheid en adequaatheid. *7.5.3 Beheer van gedocumenteerde informatie* Gedocumenteerde informatie zoals het managementsysteem voor informatiebeveiliging en deze Internationale Norm vereisen, moet worden beheerd om te bewerkstelligen dat: a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is; b) de informatie adequaat is beveiligd (bijv. tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting). Voor het beheren van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten: c) distributie, toegang, het terugvinden alsmede het gebruik; d) opslag en behoud, waaronder behoud van leesbaarheid; e) beheersing van wijzigingen (bijv. versiebeheer); en f) bewaring en vernietiging. Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het managementsysteem voor informatiebeveiliging, moet worden geïdentificeerd voor zover van toepassing en beheerd.
5	Verbeterplan	*Is onderdeel van hoofdstukken 9 en 10*
6	Implementatie (ISO 27001- hoofdstuk 8 Uitvoering)	**8.1 Operationele planning en beheersing** Om te voldoen aan de informatiebeveiligingseisen en om de in 6.1 vastgestelde maatregelen te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen. De organisatie moet ook plannen implementeren om de in 6.2 vastgestelde informatiebeveiligingsdoelstellingen te bereiken. De organisatie moet gedocumenteerde informatie bijhouden in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd. De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan. De organisatie moet bewerkstelligen dat uitbestede processen worden vastgesteld en beheerst.
		8.2 Risicobeoordeling van informatiebeveiliging

		De organisatie moet risicobeoordelingen van informatiebeveiliging met geplande tussenpozen uitvoeren, of als significante veranderingen worden voorgesteld of zich voordoen, rekening houdend met de criteria die zijn vastgesteld in 6.1.2 a). De organisatie moet gedocumenteerde informatie bewaren van de resultaten van de risicobeoordelingen van informatiebeveiliging.
		8.3 Informatiebeveiligingsrisico's behandelen De organisatie moet het behandelplan van informatiebeveiligingsrisico's implementeren. De organisatie moet gedocumenteerde informatie bewaren van de resultaten van het behandelen van informatiebeveiligingsrisico's.
7	Interne audit (ISO 27001 - hoofdstuk 9 Evaluatie van prestaties)	**9.1 Monitoren, meten, analyseren en evalueren** De organisatie moet de informatiebeveiligingsprestaties en de doeltreffendheid van het managementsysteem voor informatiebeveiliging evalueren. De organisatie moet vaststellen: a) wat moet worden gemonitord en gemeten, met inbegrip van informatiebeveiligingsprocessen en -beheersmaatregelen; b) welke methoden worden toegepast voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren, om geldige resultaten te bewerkstelligen; c) wanneer moet worden gemonitord en gemeten; d) wie moet monitoren en meten; e) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd; en f) wie deze resultaten moet analyseren en evalueren. De organisatie moet geschikte gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van het monitoren en meten.
		9.2 Interne audit De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging: a) overeenkomt met: 1) de eigen eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging; en 2) de eisen van deze Internationale Norm; b) doeltreffend is geïmplementeerd en onderhouden. De organisatie moet: c) (een) auditprogramma(s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. Het auditprogramma moet rekening houden met het belang van de betrokken processen en de resultaten van voorgaande audits; d) de auditcriteria voor en de reikwijdte van elke audit definiëren; e) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd; f) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management; en g) gedocumenteerde informatie bewaren als bewijsmateriaal van het auditprogramma en de auditresultaten.
		9.3 Directiebeoordeling De directie moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen, om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling moet onder andere in overweging worden genomen: a) de status van acties als gevolg van voorgaande directiebeoordelingen;

		b) wijzigingen in externe en interne onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging; c) feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in: 1) afwijkingen en corrigerende maatregelen; 2) resultaten van monitoren en meten; 3) auditresultaten; en 4) voldoen aan informatiebeveiligingsdoelstellingen; d) feedback van belanghebbenden; e) resultaten van risicobeoordeling en de status van het risicobehandelplan; en f) kansen voor continue verbetering. De resultaten van de directiebeoordeling moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de noodzaak voor wijzigingen in het managementsysteem voor informatiebeveiliging. De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van de directiebeoordeling.
	ISO 27001 (hoofdstuk 10 Verbetering)	**10.1 Afwijkingen en corrigerende maatregelen** Wanneer zich een afwijking voordoet, moet de organisatie: a) op de afwijking reageren, en indien van toepassing: 1) maatregelen treffen om de afwijking te beheersen en te corrigeren, en 2) de consequenties aanpakken; b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door: 1) de afwijking te beoordelen; 2) de oorzaken van de afwijking vast te stellen, en 3) vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen; c) de benodigde maatregelen implementeren; d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen; e) zo nodig, wijzigingen aanbrengen in het managementsysteem voor informatiebeveiliging. Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen. De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van: f) de aard van de afwijkingen en de vervolgens genomen maatregelen, en g) de resultaten van corrigerende maatregelen.
		10.2 Continue verbetering De organisatie moet continu de geschiktheid, adequaatheid en doeltreffendheid van het managementsysteem voor informatiebeveiliging verbeteren.

Bijlage 2 Selfassessment informatiebeveiliging

De onderstaande personen worden geïnterviewd en gevraagd om het selfassessment informatiebeveiliging in te vullen. De resultaten en afwijkingen worden in een gezamenlijke sessie met hen besproken.

Naam	Functie en Rol
William Kaan	CZ CID – Cybersecurityspecialist
Wil van Hooijdonk	CC - adviseur I-domein concerncontrol
Conny Hems	CZ - Sectormanager HRM- Proceseigenaar Personeelsprocessen
Edith Brandt	CZ - Sectormanager subsidies en inkoop - Proceseigenaar inkoop
Jeroen van Els	CZ – sectormanager CID
Reinier van der Drift	CZ- Adviseur IAM – scrummaster deliveryteam cybersecurity
Ka Yen Chan	CID Vernieuwing
Patrick Siebeling	CID Regie, service en beheer
Gerlien Harthoorn	CID Beleid, advies en vernieuwing
Robert van Burk	CC – programmamanager audit
Petra Smoes	CC – Directiecontroller BU
Nico Kluwen	CC – Directiecontroller CZ
Han Roebers	Plaatsvervangend directeur B&U
John Arkes	Plaatsvervangend directeur Beleid

Bijlage 3: documenten

De onderstaande documenten worden meegenomen in dit onderzoek. Deze lijst kan nog worden aangevuld.

- BIO versie 1.04zonder verwijzingen, interbestuurlijke werkgroep, van kracht sinds 17 juni 2020.
- ISO IEC 27001: 2013: NEN Nederlandse norm. Informatietechnologie, beveiligingstechnieken, managementsystemen voor informatiebeveiliging, eisen.
- ISO IEC 27002:2021, NEN International standard information security, cybersecurity and privacy protection – Information security controls
- Beleidskader informatiebeveiliging, Provincie Noord-Holland, 15 juli 2021
- 16-009 directienota governance informatiebeveiliging, 18 april 2017
- 19-193 directienota Baseline informatiebeveiliging Overheid, 21 november 2019
- 16-055 directienota Concern Informatie Beleidsplan (CIP), 26 mei 2016
- Informatiebeveiligingsbeleid, Provincie Noord-Holland versie 1.1, 28 juni 2012
- Geactualiseerde datastrategie 2021-2023, Provincie Noord-Holland, GS
- Digitaliseringsstrategie 2021-2024, Provincie Noord-Holland (ambtelijk)
- Nulmeting ISO 27001 Provincie Noord-Holland, Digitrust, 17 oktober 2018
- Zelfevaluatie ISO 27001/27002:2013, Provincie Noord-Holland, CISO, november 2021
- BIO selfassessment, informatiebeveiliging, januari 2021, CIP