REKENKAMER ZEELAND

Startnotitie Onderzoek

Better safe than sorry!

Onderzoek naar de cyberveiligheid van provinciale diensten en gegevensopslag

Versie	status	t.b.v.	Datum
0.1	concept	Bespreken rekenkamerbestuur	15/07/2022
0.8	concept	Afstemmen portefeuillehouder	7/09/2022
0.9	concept	Afstemmen rekenkamerbestuur	8/09/2022
1	concept	Afstemmen GS-organisatie	15/09/2022
2	concept	Klankborden met Programmaraad	4/11/2022
3	definitief	Definitieve versie vaststellen door bestuur Rekenkamer Toesturen Gedeputeerde Staten en Provinciale Staten	25/11/2022

Versie 3 – definitief

29 november 2022

Colofon

De rekenkamer Zeeland voert onafhankelijk onderzoek uit naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het door de Provincie Zeeland gevoerde beleid. Daarmee versterkt de rekenkamer de kaderstellende en controlerende rol van Provinciale Staten. Het vergt voor Provinciale Staten veel tijd en deskundigheid om (beleids)onderzoek uit te voeren. Daarom ondersteunt de rekenkamer hierbij met als doel om de rol van Provinciale Staten binnen het dualisme op Provinciaal niveau te versterken. De rekenkamer Zeeland is een onafhankelijk instituut en bestaat uit een bestuur, een ambtelijk secretaris en medewerkers.

De bestuursleden van de rekenkamer Zeeland zijn: mevrouw mr. G.A.A. van Rijswijk - van Mook**,** de heer drs. H.J.W. Verdellen en mevrouw T. Groenendijk-de Vos MA. Portefeuillehouder van het onderzoek naar cyberveiligheid is de heer drs. H.J.W. Verdellen.

Deze startnotitie is geschreven door een onderzoeksteam bestaande uit: de heer ing. M.L.M. Dobbelaer MSc (projectleider) en de heer drs. A. Maas (secretaris rekenkamer Zeeland).

INHOUDSOPGAVE

1. Inleiding

In het onderzoeksprogramma 2022 van de rekenkamer Zeeland is het voornemen opgenomen om een onderzoek te doen naar cyberveiligheid. In deze startnotitie is dit voornemen uitgewerkt tot een plan van aanpak. We bedoelen met cyberveiligheid het volgende.

Definitie cyberveiligheid

Cyberveiligheid is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.[1]

2. Waarom dit onderzoek?

Provinciale Staten zijn als kadersteller en controleur van het dagelijks bestuur medeverantwoordelijk voor een goede en stabiele dienstverlening en gegevensbescherming. Een cyberaanval brengt de continuïteit van de werkzaamheden van de Provincie Zeeland en het geheim houden van gegevens in gevaar. Goed cyberveiligheidsbeleid is daarom cruciaal in deze tijd waarin cyberaanvallen helaas veel voorkomen en dat blijft actueel. Digitale processen vormen het zenuwstelsel van het Provinciaal bestuur, haar dienstverlening en opslag van gegevens in het kader daarvan. In de corona pandemie nam het digitaal werken sterk toe en dat effect is deels blijvend, ook nu de pandemie wat minder op de voorgrond staat. Bovendien is de cyberdreiging vanwege geopolitieke spanningen opgelopen. Recent werd bijvoorbeeld nog de Vlissingse woningcorporatie L'Escaut gehackt door een criminele organisatie met Russische banden.[2]

In het cyberveiligheidswerkveld is het over het algemeen niet de vraag óf je kwetsbaar bent, maar wanneer je geraakt wordt door een aanval. Adequaat cyberveiligheidsbeleid richt zich zowel op crisismanagement als er een aanval is geweest (warme kant) als weerbaarheidsmaatregelen om voldoende weerbaar te zijn tegen een aanval (koude kant).

3. Doelstelling

Met dit onderzoek wil de rekenkamer het volgende bereiken.

Doelstelling onderzoek

Bijdragen aan de kaderstellende en controlerende rol van Provinciale Staten waar het gaat om de cyberveiligheid van Provinciale diensten en gegevensbeheer, door inzicht te geven in welke mate Gedeputeerde Staten, provinciale organisatie en een aantal verbonden partijen adequaat uitvoering geven aan cyberveiligheidsbeleid en verantwoording daarover.

4. Focus en reikwijdte

Baseline informatie overheid

De focus in het onderzoek ligt op de implementatie van de Baseline informatie overheid. De baseline informatie overheid (BIO) is een gemeenschappelijk normenkader dat gebaseerd is op de ISO 27001/2 als internationale actuele standaard op het gebied van informatieveiligheid.[3] In het Interprovinciaal Overleg is besloten dat alle Provincies voldoen aan het BIO per 1 januari 2023.

De BIO concretiseert een aantal normen naar concrete maatregelen die verplicht door alle bestuurslagen moeten worden nageleefd. In de BIO zijn basisveiligheidsniveaus opgenomen gebaseerd op generieke schades en dreigingen voor de overheid. Per veiligheidsniveau zijn in de BIO opgenomen welke

[1] Deze definitie is ontleend aan het Nationaal Cyber Security Centrum: www.ncsc.nl

[2] L'Escaut en andere woningcorporaties gehackt door criminele groepering met Russische banden | Walcheren | pzc.nl

[3] Staatscourant 2020, 7857 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

beheersmaatregelen uit de ISO 27001/2 van toepassing zijn. Bij alle beheersmaatregelen dient op basis van individuele risicoafweging bepaald te worden hoe er aan de beveiligingsdoelstelling kan worden voldaan.

De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.[4]

Provinciale organisatie

Het onderzoek beschrijft hoe het met de implementatie van het BIO gesteld is binnen de provinciale organisatie. Het onderzoek is op dit terrein algemeen verkennend van aard en beschrijft aan de hand van reeds beschikbare monitoring en evaluatie informatie de stand van zaken. Daarnaast worden de resultaten van zogeheten pentesten die in opdracht van Gedeputeerde Staten in het najaar van 2022 worden uitgevoerd betrokken bij het rekenkameronderzoek (zie kader).

PENTEST

Pentest is een afkorting van 'penetration testing'. Bij een pentest kruipen onderzoekers in de huid van een hacker. Ze proberen op allerlei manieren en met alle mogelijke middelen toegang te krijgen tot de geteste IT-omgeving. Op die manier leggen ze zwakke plekken bloot van een website, applicatie of de gehele IT-infrastructuur. Na afloop van de pentest kunnen met gerichte maatregelen kwetsbaarheden zo goed mogelijk verholpen worden.

De provinciale organisatie bevindt zich momenteel in een extern certificeringstraject voor ISO 270001/2. Daarin wordt voor de complete organisatie al door een derde partij geanalyseerd op beheersmaatregelniveau of de informatiebeveiliging voldoet aan de standaard die daarvoor geldt. Ook betrekt de rekenkamer de resultaten van interne audits die periodiek uitgevoerd worden bij haar onderzoek.

Het rekenkameronderzoek gaat niet per beheersmaatregel uit de BIO opnieuw controleren of er al dan niet wordt voldaan aan de gestelde eisen als dat al onderzocht is in het kader van een recent ander traject.

Leveranciersmanagement

Voor een burger maakt het niet uit vanaf welke ICT-systemen provinciale informatie wordt gebruikt en/of is opgeslagen. Als die systemen buiten de provinciale organisatie zijn gelegen, dan is het een kwestie van leveranciersmanagement om als Provincie ook binnen de mogelijkheden die er zijn - te sturen op een goed cyberveiligheidsniveau. Dit leveranciersmanagement valt binnen de scope van het onderzoek en is onderdeel van de BIO. Het kan bij leveranciersmanagement gaan om het outsourcen van ICT. Ook het beheer op het uitvoeren van provinciale taken door derde organisaties, waarbij er informatie uitwisseling van provinciale gegevens is of gegevensopslag door derde organisaties plaatsvindt, is een vorm van leveranciersmanagement.

Het onderzoek brengt in beeld wat het beleid van de Provincie is op het gebied van leveranciersmanagement, of er in de praktijk conform dat beleid wordt gewerkt en of het toezicht op de uitvoering intern bij de provincie adequaat is.

Verbonden partijen

Verbonden partijen vormen een speciale categorie organisaties voor de Provincie. Verbonden partijen zijn publiekrechtelijke (gemeenschappelijke regelingen) of privaatrechtelijke rechtspersonen (verenigingen, stichtingen, BV's en NV's), waarin de Provincie Zeeland én een bestuurlijk én een financieel

[4] bio-versie-104zv_def.pdf (bio-overheid.nl)

belang heeft. Verbonden partijen is een speciale categorie. Gedeputeerde Staten kunnen naast afspraken in overeenkomsten, ook invloed uitoefenen op risico's in relatie tot veiligheidsaspecten via de aandeelhoudersrol (bij privaatrechtelijke verbonden partijen) of de rol die er is in het dagelijks en/of het algemeen bestuur van een gemeenschappelijke regeling (bij publiekrechtelijke verbonden partijen).[5] Verbonden partijen kunnen leverancier zijn in het kader van de BIO. Dat is afhankelijk van het feit of zij provinciale gegevens gebruiken of beheren.

Privaatrechtelijke verbonden partijen

Ter illustratie kiezen we ervoor om een tweetal privaatrechtelijke verbonden partijen onderdeel te laten uitmaken van het onderzoek.

De privaatrechtelijke verbonden partijen waar de rekenkamer onderzoek naar doet zijn de Westerscheldeferry BV en de NV. Westerscheldetunnel. Bij deze organisaties is de Provincie 100% aandeelhouder.

Publiekrechtelijke verbonden partijen

Het onderzoek richt zich op de RUD Zeeland. Er wordt in beeld gebracht hoe cyberveiligheid van provinciale informatie is geborgd in het kader van verlengd lokaal bestuur in deze gemeenschappelijke regeling. Het onderzoek brengt verkennend in beeld wat in de praktijk de stand van zaken is bij de RUD Zeeland op het gebied van Cyberveiligheid. Hierbij wordt zoveel mogelijk gebruik gemaakt van reeds beschikbare onderzoeksinformatie, zoals interne en externe audits, alsmede pentesten. We zullen zelf ook ter indicatie een pentest uitvoeren ter controle.

Provinciale Staten

De focus van het onderzoek ligt tot slot ook op de cyberveiligheid van specifiek aan Provinciale Staten gekoppelde activiteiten. De cyberveiligheid wordt bezien door een mystery guest die fysiek onderzoek heeft gedaan op een Statendag (zie kader). Ook beschouwt het onderzoek de rol die Provinciale Staten hebben tot het onderwerp en hoe deze wordt ingevuld.

Mystery guest

Een mystery guest probeert fysiek binnen te komen en kan bijvoorbeeld achter een computer te gaan zitten zonder dat iemand dit opmerkt. Een mystery guest is vrijgesteld om alle mogelijkheden van onderzoeken om zich toegang te verschaffen op fysiek en technisch vlak.

5. VRAAGSTELLING

Centrale vraag:

Streeft de Provincie Zeeland er voldoende naar dat ICT gebruikt voor provinciale dienstverlening en/of gegevensgebruik en opslag beveiligd is tegen schade door verstoring, uitval of misbruik en deze te kunnen herstellen als dat toch gebeurt en zijn Provinciale Staten daarbij voldoende in positie gebracht?

Deelvragen:

De centrale vraag valt uiteen in de volgende deelvragen gezien de focus die is aangebracht in het vorige hoofdstuk.

Thema provinciale organisatie

[5] Voor een meer uitvoerige beschrijving van de rol van Gedeputeerde en Provinciale Staten wordt verwezen naar het hoofdstuk over verbonden partijen in de rapportage van het onderzoek naar externe inhuur en uitbesteding. Link

De onderstaande onderzoeksvragen worden kwalitatief beantwoord door zoveel mogelijk gebruik te maken van reeds beschikbare resultaten uit onderzoeken die recent zijn of worden uitgevoerd in opdracht van de Provincie, zoals interne audits, het ISO 270001/2 certificeringstraject, pentesten, pfishingonderzoek en inzet van mystery guests in het recente verleden (2 jaar). Deze informatie wordt aangevuld met informatie uit interviews mocht informatie op onderdelen ontbreken in de reeds beschikbare documentatie.

1. Wat is de stand van zaken met betrekking tot de opzet en uitvoering van het beleidskader op het gebied van cyberveiligheid binnen de provinciale organisatie en hoe verhoudt zich dat tot de Baseline Informatie Overheid?

Thema leveranciersmanagement

De onderstaande onderzoekvragen worden kwalitatief beantwoord. Om vraag 2c te beantwoorden worden een aantal cases onderzocht op basis van een selecte steekproef uit het totaaloverzicht aan leveranciers die diensten uitvoeren en/of gegevens opslaan voor de Provincie. De aard en totale omvang van de selecte steekproef is nog nader te bepalen.

2. Wat is de stand van zaken met betrekking tot cyberveiligheid in leverancierrelaties (inkoop en niet-inkoop gerelateerd), het beheer daarvan en hoe verhoudt zich dat tot de BIO?

    a. Waar dienen leveranciers die diensten voor de Provincie uitvoeren en/of gegevens opslaan aan te voldoen conform het provinciale beleid op het gebied van Cyberveiligheid en wat is daarbij het beheerskader? (BIO Hoofdstuk 15.2)
    b. Hoe houdt de provinciale organisatie intern toezicht op de monitoring en beoordeling in het kader van cyberveiligheid bij leveranciers?
    c. Wat blijkt specifiek uit een selecte steekproef (deelwaarneming) in een aantal casussen over monitoring, beoordeling en het auditen van dienstverlening van leveranciers om het overeengekomen niveau van informatiebeveiliging en dienstverlening in leveranciersovereenkomsten te handhaven?

Thema Verbonden partijen

De onderstaande onderzoeksvraag wordt kwalitatief beantwoord door zoveel mogelijk gebruik te maken van reeds beschikbare resultaten uit onderzoeken die recent zijn of worden uitgevoerd in opdracht van de Provincie, zoals interne audits, het ISO 270001/2 certificeringstraject, pentesten, pfishingonderzoek en inzet van mystery guests in het recente verleden (2 jaar). Deze informatie wordt aangevuld met informatie uit interviews mocht informatie op onderdelen ontbreken in de reeds beschikbare documentatie. Met inzet van een pentest beoogt de rekenkamer het inzicht te vergroten.

3. Wat is de stand van zaken met betrekking tot cyberveiligheid bij de verbonden partijen RUD Zeeland, NV. Westerscheldetunnel en Westerscheldeferry BV in relatie tot het provinciale beleid en hoe verhoudt zich dat tot door de Provincie Zeeland gestelde kaders?

Thema provinciale Staten

4. Hoe zijn Provinciale Staten in positie gebracht met betrekking tot kaderstelling en controle op het gebied van cyberveiligheid van dienstverlening en gegevensbeheer en hoe cyberveilig is de provinciale organisatie specifiek op een Statendag?
    a. Wat is er in de begroting en jaarstukken opgenomen over cyberveiligheid?
    b. Hoe worden Provinciale Staten anderszins geïnformeerd?
    c. Wat blijkt specifiek over de cyberveiligheid van de Provincie op een Statendag uit onderzoek door een mystery guest?

5. ONDERZOEKSMETHODE

Om de vraagstelling te beantwoorden, wordt gekozen voor een combinatie van documentenanalyse, interviews en het uitvoeren van pentest(en) en onderzoek met inzet van een mystery guest. De pentest en mystery guest worden uitgevoerd door een externe partij, het overige deel van het onderzoek voert de rekenkamer uit in eigen beheer, met ondersteuning van een externe partij op inhoud.

Bij het onderzoek maakt de rekenkamer nadrukkelijk gebruik van gegevens die al aanwezig zijn bij de organisaties die worden onderzocht, zoals audits, pentesten en overige evaluaties en onderzoek.

Het onderzoek is opgedeeld in 3 fasen.

Fase 1. Verkrijgen van overzicht

Het onderzoek begint met verkennende gesprekken. Daarmee wordt geïnventariseerd welke beleids- en werkdocumenten (bijvoorbeeld afwegingskaders en protocollen) er van toepassing zijn op het onderwerp en welke mensen/actoren er betrokken zijn bij het onderwerp.

Fase 2. Verkrijgen van inzicht

In deze fase wordt er verdieping aangebracht in het onderzoek. De beleids- en werkdocumenten die in fase 1 in beeld zijn gebracht worden geanalyseerd. Ook worden interviews gehouden met relevante betrokken personen en wordt de pentest uitgevoerd. De pentesten worden uitgevoerd.

Fase 3. Oordeelsvorming en sturing

In deze fase worden de bevindingen langs de meetlat van een normenkader gelegd. Dit normenkader is gebaseerd op wetgeving, beleid van de Provincie Zeeland en algemene beginselen van behoorlijk bestuur. De toets aan het normenkader geeft input voor sturingsaspecten die er mogelijk zijn om het beleid van de Provincie en de uitvoering daarvan verder te verbeteren.

6. NORMENKADER

De Baseline Informatie Overheid vormt het normenkader voor dit onderzoek. Zie bio-versie-104zv_def.pdf (bio-overheid.nl). De normen zijn als volgt:

Deelvraag 1. ICT Provinciale organisatie

Deelonderwerpen	Normen
1a. Informatieveiligheidsbeleid	• Er zijn beleidsregels vastgesteld door de directie die ten minste voldoen aan de in de BIO genoemde punten. (BIO 5.1.1) • Het beleid is gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. (BIO 5.1.1)
1b. Doelen en Budget	• De Provincie heeft doelen gesteld om cyberveiligheid te borgen • Er is beredeneerd vanuit de doelstelling onderbouwd een apart budget beschikbaar gesteld voor cyberveiligheid.

1c. Interne organisatie	• Alle rollen en verantwoordelijkheden bij informatiebeveiliging zijn gedefinieerd en toegewezen. (BIO 6.1.1) • Er worden passende contacten met relevante overheidsinstanties onderhouden. (BIO 6.1.3)
1d. Mobiele apparatuur en telewerken	• Er zijn beleid en ondersteunende beveiligingsmaatregelen vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengen te beheren. (BIO 6.2.1) • Beleid en ondersteunende beveiligingsmaatregelen zijn geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen. (BIO 6.2.2)
1e. Veilig personeel	• Er wordt gewaarborgd dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen (screening en tijdens dienstverband) (BIO-hoofdstuk 7)
1f. Beheer van bedrijfsmiddelen	• De bedrijfsmiddelen van de organisatie zijn geïdentificeerd en er zijn passende verantwoordelijkheden ter bescherming gedefinieerd. (BIO-hoofdstuk 8)
1g. Informatieclassificatie	• Er is bewerkstelligd dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.
1h. Toegangsbeveiliging	• Er is beleid voor toegangsbeveiliging vastgesteld, gedocumenteerd en beoordeeld. (BIO 9.1.1) • Toegang voor bevoegde gebruikers wordt bewerkstelligd, onbevoegde toegang tot systemen en diensten wordt voorkomen. (BIO-hoofdstuk 9.2 t/m 9.4)
1i. Cryptografie	• Ter bescherming van informatie is er beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd conform het BIO. (BIO-hoofdstuk 10)
1j. Bescherming tegen malware	• Beheersmaatregelen ter bescherming van malware zijn geïmplementeerd en gebruikers zijn daarover voorgelicht. (BIO-hoofdstuk 12.2)
1k. Informatiebeveiliginggebeurtenissen en - incidenten	• Gebeurtenissen worden vastgelegd en bewijs wordt verzameld. (BIO Hoofdstuk 12.4) • De aanpak is bewerkstelligd voor het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en

	zwakke plekken in de beveiliging. (BIO-hoofdstuk 16.1)
1l. Beheer van technische kwetsbaarheden	• Informatie over technische kwetsbaarheden van gebruikte informatiesystemen worden tijdig verkregen, geëvalueerd en passende maatregelen genomen om het risico dat ermee samenhangt aan te pakken. (BIO 12.6) • Er zijn regels vastgesteld en geïmplementeerd voor het door gebruikers installeren van software. (BIO 12.6)
1m. Beheer van netwerkbeveiliging	• De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten zijn gewaarborgd. (BIO Hoofdstuk 13.1)
1n. Beveiliging informatietransport	• Ter bescherming van informatietransport zijn formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht. (BIO-hoofdstuk 13.2)
1o. Continuïteitsbeheer	• De continuïteit van informatieveiligheid bij ongunstige situaties zoals bijvoorbeeld een crisis of een ramp is ingebed in de organisatie (BIO-hoofdstuk 17.1)
1p. Informatiebeveiligingsbeoordelingen	• Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check act-cyclus op gestructureerde wijze wordt afgedekt. • Er een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welke soort beveiligingsaudits worden uitgevoerd. • Er wordt in de P&C gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring over de informatiebeveiliging • Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid, bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten?

Deelvraag 2. Leveranciersmanagement

Deelonderwerpen	Normen
2a. Beleidskader	• Het beleidskader van de Provincie streeft naar het waarborgen van bedrijfsmiddelen van de organisatie in leveranciersrelaties conform de BIO a. Eisen bij offerteaanvragen stellen b. Beheersmaatregelen op basis van risicoafweging c. Afsluiten van verwerkersovereenkomsten persoonsgegevens
2b. intern toezicht	• De provinciale organisatie houdt intern toezicht op de monitoring, beoordeling en het beheer van leveranciersovereenkomsten
2c. Implementatie BIO	• Beveiligingsaspecten bij leveranciers worden in de praktijk gesteld, gemonitord, beoordeeld en waar nodig geaudit om het overeengekomen niveau van cyberveiligheid te handhaven.

Deelvraag 3. Verbonden partijen

Deelonderwerpen	Normen
3. Stand van zaken	De verbonden partijen voldoen aan de door de Provincie Zeeland gestelde kaders op het terrein van cyberveiligheid.

Deelvraag 4. Positie Provinciale Staten

Deelonderwerpen	Normen
5a. Sturing PS	• Provinciale Staten sturen op cyberveiligheid in de P&C cyclus.
5b. Verantwoording	• Provinciale Staten ontvangen tijdig en voldoende informatie
5c. Praktijk	• De beveiliging op Statendagen is adequaat blijkt uit onderzoek van een mystery guest.

7. Opzet eindrapportage

De rekenkamer staat een beknopte bestuurlijke nota voor ogen met de kern van de analyse (beantwoorden centrale vraag en toets aan het normenkader), inclusief de conclusies en aanbevelingen. Een uitgebreider rapport (nota van bevindingen) wordt opgesteld als technisch achtergronddocument. In de nota van bevindingen worden de deelvragen beantwoord. Dit document maakt geen onderdeel uit van de publicatie, maar is wel opvraagbaar.

8. Organisatie

Portefeuillehouder: drs. H.J.W. Verdellen

Projectteam: ing. M.L.M. Dobbelaer MSc. (Projectleider-onderzoeker), drs. A. Maas QC (secretaris-onderzoeker)

De rekenkamer voert het onderzoek in eigen beheer uit. Voor de uit te voeren pentest(en) wordt externe expertise ingehuurd. Het bedrijf dat deze opdracht zal uitvoeren is DONGIT uit leiden. Tevens wordt een externe partij gevraagd om een review te geven op de onderzoeksaanpak, nota van bevindingen en bestuurlijke nota. Deze partij is 2-Control uit Breda.

9. Planning

Wanneer	Wat	Wie
11-2022	• vaststellen definitieve startnotitie • besluit tot toesturen definitieve startnotitie GS en PS.	bestuur rekenkamer
Nov 22-feb 23	• interviews/documentenanalyse/pentest/mystery guest • Opstellen nota van bevindingen	onderzoeksteam
Maart 2023	• afronden nota van bevindingen • verzoek tot ambtelijk wederhoor • Afstemmen bevindingen met programmaraad	bestuur rekenkamer
April 2023	• vaststellen Bestuurlijke nota • besluit tot toesturen bestuurlijke nota aan GS en DB RUD Zeeland voor bestuurlijk commentaar	bestuur rekenkamer en Programmaraad bestuur rekenkamer
Mei 2023	• publicatie en externe communicatie	Bestuur rekenkamer
Juni 2023	• beantwoorden vragen in Commissie Bestuur	portefeuillehouder rekenkamer

10. Communicatie

Op een aantal momenten communiceren wij over het onderzoek. Deze paragraaf geeft hiervan een overzicht.

<u>Startnotitie</u>

- Ter afstemming ontvangt de Programmaraad een conceptversie van de Startnotitie.
- De portefeuillehouder van het onderzoek namens de rekenkamer heeft een startgesprek met de verantwoordelijke gedeputeerde(n) namens Gedeputeerde Staten.

- De rekenkamer stuurt de definitieve startnotitie ter kennisname aan Gedeputeerde en Provinciale Staten

Nota van bevindingen

- De ambtelijke organisatie van de Provincie Zeeland en RUD Zeeland ontvangen de concept nota van bevindingen voor ambtelijk wederhoor en worden geïnformeerd over wijzigingen als gevolg daarvan.

Eindrapport (bestuurlijke nota)

- De rekenkamer betrekt de programmaraad bij de analyse van de bevindingen.
- Het Dagelijks Bestuur van de RUD Zeeland en Gedeputeerde Staten worden in de gelegenheid gesteld om bestuurlijk commentaar te geven op de bestuurlijke nota.

Publicatie

- Gedeputeerde Staten en Provinciale Staten ontvangen de definitieve bestuurlijke nota.
- De definitieve bestuurlijke nota wordt tevens toegestuurd aan de betrokken verbonden partijen: NV Westerscheldetunnel, Westerscheldeferry BV en RUD Zeeland
- De bestuurlijke nota wordt verstuurd aan alle geïnterviewde personen.

Persbericht en woordvoering

Het bestuur van de rekenkamer Zeeland stelt een persbericht vast. Het persbericht wordt verstuurd aan de reguliere perscontacten. De woordvoering over het onderzoek naar de pers geschiedt door de voorzitter van de rekenkamer Zeeland, mevrouw mr. G.A.A. van Rijswijk - van Mook.

11. SLOTOPMERKING

Deze startnotitie is opgesteld op basis van een globale verkenning van het onderwerp. Op basis van het verzamelde onderzoeksmateriaal kan de aanpak gedurende het onderzoek worden bijgesteld. Als deze bijstelling naar ons oordeel tot majeure aanpassingen van de opzet leidt, zal dit door ons worden gecommuniceerd.