VERDONCK KLOOSTER & ASSOCIATES

ONDERZOEK TOEZICHT EN VERANTWOORDING INFORMATIEVEILIGHEID OVERHEID

Horizontaal en verticaal toezicht in balans

ONDERZOEK TOEZICHT EN VERANTWOORDING INFORMATIEVEILIGHEID OVERHEID

Horizontaal en verticaal toezicht in balans

Joep Janssen, Sander Vols, Martijn Hunsche, Mark Vermeulen en Cleo van Engelen

DATUM	**28-2-2019**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20185594
INTERNE TOETS	Pim Schouten

MANAGEMENTSAMENVATTING

Binnen het openbaar bestuur vindt een verdergaande digitalisering plaats van de overheids-dienstverlening. Daarmee groeit het belang van informatieveiligheid. Dit onderzoeksrapport is het resultaat van een verkenning naar de organisatie van de verantwoording over en het toezicht op de informatieveiligheid van de decentrale overheden: de provincies, gemeenten en water-schappen. De centrale vraag hierbij is op welke wijze BZK vanuit haar stelselverantwoordelijkheid voor informatieveiligheid in het openbaar bestuur de verantwoording over en het toezicht op informatieveiligheid kan organiseren en welke instrumenten daarvoor ingezet kunnen worden.

Op alle bestuurslagen is het bewustzijn over informatieveiligheid en de digitale weerbaarheid de afgelopen jaren toegenomen. Initiatieven zijn genomen om informatieveiligheid een onderdeel uit te laten maken van de reguliere planning en control-cyclus. Tussen de verschillende bestuurs-organen en tussen de bestuurslagen bestaan desondanks nog verschillen in de mate waarin informatieveiligheid een integraal onderdeel uitmaakt van die planning en control-cyclus. Ditzelfde beeld is ook zichtbaar in een aantal met Nederland vergelijkbare Europese landen. De program-matische aanpak in Denemarken, waar tussen de bestuurslagen meerjarenafspraken zijn gemaakt over de sturing op informatieveiligheid, kan als voorbeeld dienen voor de Nederlandse situatie.

De wet- en regelgeving die relevant is voor de inrichting van verantwoording en toezicht op informatieveiligheid, met name het wetsvoorstel Digitale Overheid, legt het primaat bij horizontaal toezicht op informatieveiligheid binnen een bestuurslaag. Het interbestuurlijke verticale toezicht sluit hier op aan.

Op basis van onderzochte ontwikkelingen en visies bij de verschillende bestuurslagen en ontwikkeling van wetgeving zijn vier varianten voor verantwoording en interbestuurlijk toezicht op informatieveiligheid opgesteld, variërend van zelfregulering/horizontaal toezicht per bestuurslaag tot verticaal interbestuurlijk toezicht op de naleving van specifieke regelingen. De variant die horizontaal toezicht van het bestuursorgaan combineert met generiek toezicht door het rijk op de naleving van het gebruik van de generieke digitale infrastructuur scoort daarbij het beste, met name waar het de transparantie betreft over de naleving van de afspraken in de keten van de generieke digitale infrastructuur.
Geconstateerd is dat het kennis en bewustzijn rondom informatieveiligheid groeit, maar dat voornamelijk bestuurders nog handelingsverlegen zijn. Lokale bestuurders en toezichthouders hebben een handelingsperspectief nodig om beter sturing te kunnen geven aan informatieveiligheid. Collegiale visitatie en sturing op groei in volwassenheid van de planning en control-cyclus zijn daarbij belangrijke instrumenten.

Om het gewenste volwassenheidsniveau te bereiken en balans te vinden tussen horizontaal en verticaal toezicht op informatieveiligheid zal een meerjarige interbestuurlijke programmatische inspanning noodzakelijk zijn. Hiervoor kan lering getrokken worden uit de Deense programmatisch aanpak voor informatieveiligheid.

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

"*Toezicht houden is het verzamelen van informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich vervolgens vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren*[1]".

Deze definitie heeft het Ministerie van Binnenlandse Zaken (hierna BZK) verbonden aan het woord "Toezicht". Aanleiding voor dit onderzoek is de vraag over hoe toezicht en verantwoording over informatieveiligheid ingericht kan worden. De start van dit onderzoek ligt in de Agenda Digitale Overheid: "NL DIGIbeter" en beschrijft de gezamenlijke digitale agenda van alle overheden met belangrijke publieke en private partners.

Met deze achtergrond is aan Verdonck Klooster en Associates (hierna VKA) gevraagd een verkenning te starten naar de inrichting van toezicht en verantwoording van informatieveiligheid binnen de overheid.

1.2 Vraagstelling

Het Directoraat-Generaal Overheidsorganisaties, directie Informatiesamenleving & Overheid (DIO) van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (hierna: BZK) heeft voor de volgende tranche van de Wet Digitale Overheid behoefte aan een onderzoek naar het vraagstuk "toezicht en verantwoording informatieveiligheid overheid".

De onderzoeksopdracht is tweeledig:

1. BZK vraagt om een verkenning naar de wijze waarop zij, vanuit haar specifieke stelselverantwoordelijkheid voor informatieveiligheid, in het openbaar bestuur de verantwoording over en het toezicht op informatieveiligheid dient te organiseren. De verkenning is specifiek gericht op de informatieveiligheid bij de medeoverheden: provincies, gemeenten en waterschappen. Buiten het onderzoek blijft hoe dit toezicht zich verhoudt tot de verantwoordelijkheid naar het Rijk en de uitvoeringsinstanties van andere ministeries. De verkenning geeft inzicht in:
    a. De maatschappelijke ontwikkelingen waaronder de toenemende digitale overheidsdienstverlening en het belang van adequate informatieveiligheid. Daarbij wordt ook nagegaan hoe dit vraagstuk bij overheden in het buitenland wordt beantwoord.
    b. De ontwikkelingen op het gebied van wet- en regelgeving, zoals de nieuwe Wet beveiliging netwerk- en informatiesystemen, de Wet Digitale Overheid, het generiek (interbestuurlijk) toezicht op grond van de Gemeente-/Provincie-/ Waterschapswet en de wijze waarop de huidige verantwoording is geregeld per bestuurslaag (uitgezonderd het Rijk).

[1] Toezicht bij BZK, 2013, p.3

c. De gevolgen voor de verantwoording door bestuursorganen over informatieveiligheid, de wijze waarop het horizontaal en verticaal toezicht is vormgegeven en de rol van audits daarbij.

2. Het onderzoek geeft tevens een advies over de wijze waarop:
   a. Het kennisniveau bij medewerkers en bestuurders in het openbaar bestuur kan worden verhoogd t.a.v. informatieveiligheid, zodat lokale bestuurders en lokale toezichthouders het werk (beter) kunnen volbrengen;
   b. Welke waarborgen/instrumenten in de rede liggen zodat informatieveiligheid op orde is.

1.3 Doel van dit document

Het doel van dit document is een antwoord te geven op de vragen die aan VKA gesteld zijn. Daarnaast biedt dit document de noodzakelijke context, beschrijft het de randvoorwaarden die relevant zijn om keuzes te kunnen maken tussen de toezichtvarianten en geeft inzicht in de manier waarop VKA tot de resultaten gekomen is. Ten slotte biedt dit document een handvat voor de opdrachtgever om een weloverwogen keuze te maken bij de inrichting van toezicht en verantwoording op informatieveiligheid binnen de overheid.

1.4 Leeswijzer

Wij hebben gekozen voor een opbouw waarin logisch wordt toegewerkt naar de beantwoording van de vragen die de basis vormen van dit onderzoek. Hoofdstuk 1 schets de achtergrond en de vraagstelling van dit onderzoek. Hoofdstuk 2 geeft een toelichting over de onderzoeksopzet, de methode die door VKA is gebruikt om tot resultaat te komen. Hoofdstuk 3 beschrijft de scope van dit onderzoek (onderzoeksobject) en gaat ook in op wat er buiten scope is geplaatst. Hoofdstuk 4 beschrijft de belangrijkste kaders voor verantwoording, toezicht en auditing die relevant zijn binnen de scope van dit onderzoek. Hoofdstuk 5 beschrijft de huidige inrichting van verantwoording toezicht en auditing bij de onderzochte bestuurslagen. Dit hoofdstuk is samengesteld op basis van informatie uit verschillende beleidsstukken, notities en de informatie verzameld tijdens de interviews met vertegenwoordigers van de bestuurslagen. Hoofdstuk 6 geeft een overzicht van de meest relevante wettelijke kaders voor toezicht op informatieveiligheid, meer specifiek de Wet Revitalisering Generiek Toezicht, de Wet Digitale Overheid, en de Wet Beveiliging Netwerk- en Informatiesystemen.

Op basis van deze beschrijvingen zijn de belangrijkste beleidsuitgangspunten voor toezicht op informatieveiligheid geformuleerd. Deze uitgangspunten worden toegepast op vier mogelijke toezichtvarianten, allen beschreven in hoofdstuk 7. In hoofdstuk 8 presenteren we onze conclusies en aanbevelingen.

Als bijlage is een bronnenlijst toegevoegd met een korte beschrijving van de bronnen, een lijst met geïnterviewden en een lijst met de leden van begeleidingscommissie.

2 ONDERZOEKSOPZET

2.1 Inleiding

De onderstaande onderzoekaanpak is gehanteerd om tot een juiste en complete beantwoording van de vraag van de Opdrachtgever te komen.

2.2 Onderzoekaanpak

Het onderzoek heeft bestaan uit drie fasen. Onderstaand een schematische weergave van deze fasen en bijbehorende stappen. Het onderzoek is gestart op 2 oktober 2018 en de eindrapportage is opgeleverd op 21 december 2018.
Het onderzoek is begeleid door een begeleidingsgroep van het ministerie van BZK.

Fase	Activiteit	Deliverable
Voorbereiding	Kick-Off	Afgestemde onderzoekopzet
		Generieke vragenlijst voor interviews
		Afgestemde lijst te interviewen personen
		Object onderzoek vastgesteld
	Voorbereiding onderzoek	Documentstudie
		Ingeplande interviews
Uitvoering	Interviews afnemen	15 interviews
	Aanvullende documentstudie	Aanvullende documenten (n.a.v. interviews) verzameld en opgenomen in documentstudie
	Uitwerken rapportage	Conceptrapportage opgesteld
Afronding	Afstemmen concept rapportage	Conceptrapportage afgestemd, inclusief verbetervoorstellen opdrachtgever
	Definitieve rapportage	Definitieve rapportage opgeleverd
	Afronding onderzoek	Presentatie resultaten onderzoek

3 SCOPE VAN HET ONDERZOEK: HET OBJECT

3.1 Binnen scope

De scope van het onderzoek is bepaald door de stelselverantwoordelijkheid van het ministerie van BZK voor informatieveiligheid in het openbaar bestuur bij een verdergaande digitalisering van overheidsdienstverlening en daarmee een toenemend belang voor informatieveiligheid. Meer specifiek de organisatie van de generieke verantwoording over en het generieke toezicht op de informatieveiligheid van de medeoverheden: de provincies, gemeenten en waterschappen en welke onderdelen van informatieveiligheid zich daarbij lenen voor horizontaal toezicht dan wel verticaal toezicht.

In het onderzoek zijn de maatschappelijke ontwikkelingen meegenomen die voor informatieveiligheid relevant zijn. Het betreft hier onder andere de toenemende digitale overheidsdienstverlening en het belang van adequate informatieveiligheid. Ook zijn de ontwikkelingen op het gebied van wet- en regelgeving (zoals de Wet Digitale Overheid, de nieuwe Wet beveiliging netwerk- en informatiesystemen, het generiek (interbestuurlijk) toezicht op grond van de Gemeente-/ Provincie-/Waterschapswet) beschreven.

Onderdeel van het onderzoek is op welke wijze de huidige verantwoording is geregeld per bestuurslaag exclusief Rijk), hierbij is het ENSIA initiatief inbegrepen en de functie van (interne en externe) audits. Eveneens beschrijft het onderzoek op welke wijze het kennisniveau over informatieveiligheid onder medewerkers en bestuurders in het openbaar bestuur kan worden verhoogd, op welke wijze het lokaal bestuur en lokale toezichthouders hun werk (beter) kunnen uitvoeren en welke waarborgen (c.q. instrumenten) hierbij in de rede liggen. Ten slotte is een beeld gegeven van de organisatie van het toezicht en de verantwoording t.a.v. informatieveiligheid binnen overheden in het buitenland, meer specifiek Denemarken, Oostenrijk, België en de Duitse deelstaat Noord-Rijnland Westfalen.

3.2 Buiten scope

De vraag hoe het generieke toezicht zich verhoudt tot het specifieke toezicht binnen de uitvoeringsinstanties op beleidsdomeinen van andere ministeries (Rijk) is door de opdrachtgever in dit onderzoek buiten scope geplaatst.

4 KADER: VERANTWOORDING, TOEZICHT EN AUDITING

4.1 Inleiding

In dit onderzoek staat de relatie tussen verantwoording, auditing en toezicht centraal. Deze relatie is in meerdere studies beschreven en in alle gesprekken aan de orde gekomen.

De kern van de relatie wordt bepaald door de governance-structuur en de aanwezige checks and balances binnen het openbaar bestuur, zowel door zelfregulering binnen het bestuursorgaan als door interbestuurlijk toezicht. Hieronder een beknopte beschrijving van de meest gangbare zienswijzen.

4.2 Het fundament: stelselverantwoordelijkheid

De minister van BZK draagt de stelselverantwoordelijkheid voor informatieveiligheid. Stelselverantwoordelijkheid betekent hier dat ieder van de betrokken overheden medeverantwoordelijkheid draagt voor het stelsel als geheel en dat elk van deze overheden daarop kan worden aangesproken. Deze definiëring is meerdere malen door de minister en staatssecretaris verwoord in brieven aan de Kamer en komt voort uit een advies van de Afdeling advisering van de Raad van State (AaRvS)[2].

Stelselverantwoordelijkheid vereist een heldere rolverdeling binnen het stelsel, waarbij ieder bestuursorgaan afzonderlijk duidelijk omschreven verplichtingen heeft die het in nauwe samenwerking met andere bestuursorganen vervult. Concreet betekent dit dat in het geval wettelijke taken in medebewind bij een andere bestuurslaag zijn neergelegd, zoals bij informatieveiligheid, de rijksoverheid zich terughoudend opstelt in de interbestuurlijke verhoudingen. De rijksoverheid en individuele ministers houden op hun beleidsterrein wel een ‘restverantwoordelijkheid’. Deze restverantwoordelijkheid vloeit voort uit de bevoegdheid om als ministers wetgeving te initiëren en aan te passen, om daarmee bijvoorbeeld een ongewenste situatie aan te passen en een gewenste situatie te creëren. De minister kan dus ook worden aangesproken om deze verantwoordelijkheid te nemen.

4.3 Zelfregulering en horizontaal toezicht

Het kabinet hanteert het basisprincipe dat afzonderlijke overheidsorganisaties zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Zelfregulering binnen het bestuursorgaan, dat uit dit principe voortkomt, wordt gekenmerkt door een werkende planning en control-cyclus en horizontale verantwoording aan de gekozen vertegenwoordiging. In de verantwoording geeft het bestuur aan op welke wijze het informatieveiligheidsbeleid is gerealiseerd, welke afwijkingen er zijn, de risicoafweging daarbij en de verbeteringen die worden doorgevoerd.

[2] Afdeling advisering van de Raad van State, W04.15.0367/I, 4e periodieke beschouwing over interbestuurlijke verhoudingen: *“En nu verder!”*, 30-09-2016.

Voorgaande is naar analogie met het financieel beheer en de financiële verantwoording. De internationale audit praktijk sluit zich hierbij aan. De auditor geeft een verklaring van getrouwheid bij de verantwoording door de organisatie over het gevoerde beheer. In dit specifieke geval is dat het beheer over de informatieveiligheid. Dit vereist een mate van volwassenheid van het kwaliteitssysteem van het verantwoordelijke bestuursorgaan, waar informatieveiligheid en digitalisering een integraal onderdeel van uitmaakt.

Steeds meer publieke organisaties werken met instrumenten van integrale kwaliteitszorg, zoals visitaties, benchmarking, bestuursafspraken of kwaliteitshandvesten. Deze kwaliteitsinstrumenten zijn geen formele vormen van toezicht of verantwoording en stellen het leereffect van de organisatie voorop. Ze geven een prikkel tot beter presteren en vormen een bron van informatie voor onder andere belanghebbende burgers en ondernemingen.

Concrete voorbeelden van zelfregulering en horizontaal toezicht is het ENSIA initiatief voor verantwoording bij gemeenten, waarmee het gemeentebestuur meer overzicht krijgt over de informatieveiligheid en hierop beter kan sturen. Uitgangspunt hierbij is dat aangesloten wordt op de gemeentelijke Planning & Control cyclus.

Voorbeelden van kwaliteitsinstrumenten zijn de visitatiecommissie Informatieveiligheid ‘Durven leren’ en het dashboard Waarstaatjegemeente.nl van de Vereniging Nederlandse Gemeenten (VNG). Voorbeelden bij de waterschappen zijn de verantwoording en auditing over informatieveiligheid en het vergelijkend onderzoek ‘Waterschapsspiegel’ welke gehanteerd wordt om prestaties van de waterschappen onderling te vergelijking en de dienstverlening te verbeteren.

4.4 Verticaal toezicht

Interbestuurlijk (verticaal) toezicht wordt omschreven als ‘het geheel van processen dat plaatsvindt in het kader van de rechtsbetrekkingen tussen Rijk, de provincies, de gemeenten, de Wgr-regio’s en de waterschappen die gaan over de beoordeling van de taakbehartiging van de lagere door de hogere overheden’.

In het kader van interbestuurlijk toezicht wordt een onderscheid gemaakt tussen generiek en specifiek toezicht. De Wet revitalisering generiek toezicht (Wet RGT) beoogt een einde te maken aan de vele regelingen voor specifiek toezicht en de toenemende toezichtlasten die in de loop der jaren zijn ontstaan.

Het belangrijkste uitgangspunt van de Wet RGT is (onderling) vertrouwen. Aandachtspunt daarbij is het evenwicht tussen het onderlinge toezicht en de beleidsvrijheid van de overheidsorganisaties. Ten behoeve het behoud van die balans zijn er twee generieke instrumenten:

1. Indeplaatsstelling bij taakverwaarlozing en
2. Schorsing en vernietiging.

Deze instrumenten zijn een ultimum remedium en worden pas toegepast nadat per instrument eerst een ‘interventieladder’ is doorlopen van ‘signaleren’ tot en met het definitief toepassen van

het betreffende toezichtinstrument. Een veel genoemd motto bij daarbij is: “Zo licht als mogelijk, zo zwaar als noodzakelijk”. Dit hangt veelal af van de risicoafweging die gemaakt wordt.

In een publiek-privaat stelsel, waarbij ook marktpartijen een rol spelen bij de publieke dienstverlening, hanteert de overheid veelal een specifieke vorm van toezicht. Zo heeft het Agentschap Telecom in het kader van de Telecomwet als toezichthouder de wettelijke bevoegdheid om bij niet naleving door een markpartij in te grijpen en bijvoorbeeld de vergunning in te trekken. Steeds meer vormen van publieke dienstverlening krijgen vorm in een publiek-privaat stelsel. Daarbij kan een overweging zijn dat voor bestuursorganen hetzelfde toezichtregime geldt als voor marktpartijen.

Ministerieel toezicht vereist een beleidsvisie op nut en noodzaak van toezicht op een beleidsterrein. Uitgaande van die toezichtvisie moet voorafgaand aan het daadwerkelijke toezicht een toezichtbeleid worden geformuleerd, dat voldoende duidelijk en richtinggevend is voor de feitelijke uitvoering van het toezicht. Verticaal toezicht is dienend aan de ministeriële verantwoordelijkheid en kan daarom niet worden vervangen door zelfregulering en horizontaal toezicht. In het kader van de ministeriële verantwoordelijkheid kan de minister of toezichthouder ook gebruik maken van de resultaten van het horizontale toezicht, bijvoorbeeld horizontale verantwoordingsinformatie. Deze verantwoordingsinformatie dient betrouwbaar, valide en relevant te zijn. Bestuursorganen zijn zelf verantwoordelijk voor de betrouwbaarheid van de informatie. In de verantwoording kan de instelling expliciet aangeven hoe zij deze aspecten van de verantwoordingsinformatie waarborgt. De minister moet immers na kunnen gaan hoe de informatie tot stand is gekomen. In het toezichtbeleid dienen duidelijke afspraken gemaakt te zijn over de over de betrouwbaarheid en validiteit van de informatie. De verklaring van getrouwheid van de auditor bij de verantwoording kan daarbij een belangrijke rol spelen. Dit naar de analogie van verklaring van de accountant bij het financiële jaarverslag. Het verticale toezicht kan verder aan doelmatigheid winnen door aan te sluiten op andere vormen van checks and balances zoals de informatie vanuit belanghebbenden of betrokkenen of informatie afkomstig uit visitaties en uitgevoerde benchmarks.

Concrete voorbeelden van verticaal toezicht op het gebied van informatieveiligheid zijn op dit moment waar te nemen in de gemeentelijke ENSIA rapportages aan BZK/Logius voor DigiD en aan de Inspectie Sociale Zaken en Werkgelegenheid in het kader van het opvragen van persoonsgegevens door gemeentelijk sociale diensten via SUWInet.

4.5 Kennis, inzicht en instrumentarium

De afgelopen jaren heeft de kennis over informatieveiligheid op operationeel en tactisch niveau een belangrijke sprong voorwaarts gemaakt binnen alle bestuurslagen en –organen. Binnen de verschillende overheidslagen worden de nodige inspanningen verricht om kennis en inzicht in technische en organisatorische informatieveiligheid te vergroten.

Zoals ook het rapport van Taskforce BID aangeeft blijft de bestuurlijke aandacht voor informatieveiligheid daarbij achter. Meerdere initiatieven zijn genomen om het bestuurlijk bewustzijn te vergroten, zeker binnen de gemeenten. Een voorbeeld hiervan is de visitatiecommissie informatieveiligheid (met als eindrapport “Durven Leren”). Als volgende stap in dit proces willen betrokkenen meer werken aan het ‘Bestuurlijk handelingsperspectief’.

Geconstateerd is dat het bewustzijn er steeds meer is, maar dat de bestuurders nog handelingsverlegen zijn. Om bestuurlijk handelingsperspectief op het gebied van informatieveiligheid te creëren is het noodzakelijk een taal te spreken die aansluit bij de rol van bestuurders in de overheid. Deze taal is nog niet aanwezig. Het gaat daarbij nadrukkelijk niet over de techniek van informatieveiligheid, maar om de gevolgen van de digitalisering van de samenleving voor de informatieveiligheid. Welke risico’s dienen zich aan en hoe moeten burgers, ondernemers en overheid daarop reageren? De taal moet herkenbaar zijn voor de bestuurders en aansluiten op reeds bestaande bestuurlijke praktijken in het publieke domein, zoals fysieke veiligheid, bestuurlijke weerbaarheid, integriteit van overheidshandelen en crisismanagement.

Om dit bestuurlijk handelingsperspectief verder te concretiseren hebben bestuurders instrumenten nodig om te kunnen handelen. De volgende voorbeelden komen uit de verschillende beleidsdocumenten en interviews naar voren:

- Visitatie. Geen controlerende visitatie in de klassieke zin, maar in een open gesprek leren van elkaar en er mee aan de slag gaan.
- Benchmarking. Geen lijstjes met koplopers en achterblijvers (‘naming and shaming’), maar positieve voorbeelden en zoeklichten (‘naming en faming’).
- Praktijktraining. Geen theoretische opleiding informatieveiligheid, maar oefenen met het afhandelen van concrete informatieveiligheidsbedreigingen, zoals phishing-mails, DDos aanvallen, computervirussen, onderscheppen mobiele communicatie, etc.
- Leren en groeien in volwassenheid. De volwassenheid van een organisatie bepaalt mede de mate waarin ze in staat is invulling te geven aan zelfregulering. Betrokkenen geven aan dat de verschillende bestuurslagen en –organen nog kunnen leren en groeien in volwassenheid als het gaat om het besturen en beheersen van de informatieveiligheid. Dit geldt voor alle bestuurslagen, ook voor de toezichtrol door het rijk. Een volwassenheidsmodel helpt om te bepalen waar je staat als organisatie, welk ambitieniveau je na wilt streven en welk leerproces doorlopen moet worden om dat niveau te bereiken.

4.6 Trends inrichting toezicht informatieveiligheid buitenland

Drie Europese landen, te weten België, Denemarken en Oostenrijk en de Duitse deelstaat Noordrijn-Westfalen zijn aangezocht om als referentie te dienen voor de Nederlandse situatie. Bij alle vier de landen is er sprake van coördinatie op rijksniveau om de informatie- en cybersecuritywetgeving en bijbehorende maatregelen in te voeren en na te leven.

Hierbij zijn er verschillende varianten te onderscheiden. Van een programma dat planmatig wordt gecoördineerd door het Ministerie van Financiën en vooraf afgestemd met de verschillende overheden (Denemarken) tot een overheid die de daarvoor ingerichte faciliteiten ondersteunt maar niet planmatig coördineert (België).

De **Belgische** nationale strategie voor Cyber- en informatieveiligheid wordt geïmplementeerd, opgevolgd, gecoördineerd en gecontroleerd door de centrale autoriteit: het Centrum voor Cybersecurity België (CCB). Daarnaast doet het CCB ook voorstellen over het regelgevend kader van de Cyberveiligheid en stelt het standaarden, richtlijnen en veiligheidsnormen op. Het beheert ook de verschillende projecten op het gebied van Cyberveiligheid. Het CCB heeft ook de rol om te verzekeren dat de verschillende overheidsdiensten en de verschillende publieke, private en wetenschappelijke instanties in België met elkaar samenwerken en de coördinatie oppakken rondom Cyber veiligheid. Deze instanties bevorderen programma's en projecten op het vlak van Cyber veiligheid binnen hun sector. Het CCB is samen met het Coördinatie-en Crisiscentrum van de Belgische regering verantwoordelijk voor het crisisbeheer van cyberincidenten. De verschillende federale overheidsdiensten binnen de verschillende sectoren zijn verantwoordelijk voor de Cyber- en informatieveiligheid binnen hun eigen dienst (sectorverantwoordelijkheid). Lagere overheden, zoals gemeenten dragen hun eigen verantwoordelijkheid en er vindt ook geen toezicht plaats van rijkswege. In België is een groot gebrek aan (cyber) security en privacy experts en voelt men de noodzaak te investeren in leren en ontwikkelen op dit vlak.

Denemarken verhoogt de laatste jaren haar inspanningen en investeringen op het gebied van cyber- en informatiebeveiliging. Denemarken pakt dit programmatisch aan en heeft dit uitgewerkt in een nationale cyber- en informatiebeveiligingsstrategie voor de komende vier jaar die de verschillende inspanningen met elkaar verbindt. Vanuit het coördinerende ministerie van Financiën zijn 25 projecten in zes gerichte programmalijnen gestart om de cyber- en informatiebeveiliging te verbeteren. Bij de totstandkoming van de strategie zijn alle overheidslagen, sectoren en bedrijven betrokken. De afspraken met betrekking tot de te realiseren resultaten zijn vooraf gemaakt. De betrokken overheden en bedrijven zijn gecommitteerd aan de door hun te behalen resultaten en in te voeren maatregelen. De projecten zijn vooraf gebudgetteerd en worden bestuurd door Financiën.
De doelstelling van de vierjaren strategie is om de meest kritieke sectoren op het gebied van cyber- en informatieveiligheid aan te pakken, de technologische veerkracht van digitale infrastructuur te versterken, de kennis en vaardigheden van burgers, bedrijven en overheden (te verbeteren en de coördinatie en samenwerking op dit gebied te bemoedigen.
Het toezicht en de besturing is in Denemarken gecentraliseerd georganiseerd. Op nationaal niveau is een stuurgroep opgezet die op de cyber- en informatiebeveiliging toeziet, opvolging geeft aan de strategie en nieuwe initiatieven ontwikkelt waar nodig. De stuurgroep komt regelmatig bij elkaar om het implementatieproces van de strategie te volgen. Elke twee jaar wordt er een onderzoek uitgevoerd om te kijken hoe ver het implementatieproces is. Deze stuurgroep wordt ondersteund door het Centrum voor Cyberveiligheid (onderdeel van het Ministerie van Defensie) en het Deens Bureau voor Digitalisering (onderdeel van het Ministerie van Financiën).

Daarnaast hanteert Denemarken de zogenoemde 'sector verantwoordelijkheid' omtrent IT-veiligheid. Dit houdt in dat de betrokken Minister verantwoordelijk is voor de IT-beveiliging binnen zijn of haar Ministerie. Het toezicht op deze IT-beveiliging wordt gedaan door een hiervoor benoemde supervisor.

In **Oostenrijk** coördineert de Federale Kanselarij het beleids- en uitvoeringsplan voor cyber security, de invoering van de NIS-richtlijnen en ziet toe op de naleving. De NIS-richtlijn (EU) 2016/1148), internationaal bekend als de NIS Directive (Directive on security of network and information systems), streeft ernaar een hoog gemeenschappelijk niveau van netwerk- en informatiesystemen in de Unie tot stand te brengen. Oostenrijk is momenteel bezig met het uitzetten van de nieuwe activiteiten en het herijken van de nationale strategie. Knelpunt in Oostenrijk is de beschikbare expertise en capaciteit. Ontwikkeling van security kennis en vaardigheden staat daarom hoog op de agenda. Met name bij decentrale overheden ontbreekt het vaak aan gekwalificeerde functionarissen.

Noordrijn-Westfalen (NRW) gaat mee in de Duitse gezamenlijke strategie van de bestuurlijk niveaus, ondersteund door het Federale Bureau voor Informatiebeveiliging (BSI). Het verantwoordelijkheidsgebied van de BSI wordt bepaald door het 'Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes' (de BSI-wet).De CIO van NRW, opererend vanuit het ministerie van Economische Zaken, werkt samen met de sector georiënteerde ministeries om op basis van eerder opgezette procedures en structuren de informatieveiligheid en cyber security te waarborgen. De CIO zet sterk in op een nieuw pakket aan maatregelen en onder zijn leiding voeren de ministeries een IT-informatiebeveiligings-onderzoek uit als eerste stap om een overzicht te krijgen van de staat van informatieveiligheid bij alle (decentrale) overheden en om de concrete behoefte en noodzaak tot maatregelen te identificeren. Onder leiding van de CIO is de deelstaatoverheid begonnen een centraal en decentraal specifiek informatiebeveiligingsbeheer op te zetten. Bovendien moet het IT-noodteam (CERT NRW), dat al vele jaren in NRW is gevestigd, beter worden ingezet om maatregelen te effecturen. Deze maatregelen zijn gebaseerd op de 'Leidraad voor informatiebeveiliging in openbaar bestuur', aangenomen door de Federale 'IT Planning Raad', bindend voor federale en deelstaatregeringen. Deze procedure onderstreept het belang van informatieveiligheid voor het functioneren van de overheidsadministratie. Momenteel is men bij het ministerie bezig met het opzetten van een Competentienetwerk informatieveiligheid en cybersecurity omdat men in kennis en vaardigheden in zowel het publieke als het private domein een grote behoefte tot ontwikkeling en uitbreiding ervaart.

Het beeld is dat in alle vier de landen kaders worden gesteld en maatregelen genomen om wetgeving met betrekking tot cyber security en informatieveiligheid door te voeren. Er is telkens sprake van een coördinerend en sturend ministerie en een verantwoordelijke functionaris. De coördinatie vindt sectoraal en in samenwerking met andere betrokken ministeries plaats.
Bij alle vier de landen worden in te zetten kennis en kunde als een groot knelpunt beschouwt en voorziet mijn in investeringen in leren en ontwikkelen.

Meer specifiek onderscheidt NRW zich door een 'topdown-benadering' vanuit de Federale overheid en een doorvertaling naar (decentrale) en besturing van de overheden binnen de deelstaat. NRW inventariseert de knelpunten en zorgt ook voor de invoering van de maatregelen.

Denemarken onderscheidt zich door een centraal gecoördineerd programma waarin niet alleen de sectoren en de decentrale overheden worden meegenomen maar ook het Deense bedrijfsleven. De programmatische aanpak van het ministerie van Financiën kenmerkt zich door met alle betrokkenen afspraken te maken op vierjaren basis en de afspraken projectmatig uit te voeren en bij te sturen met behulp van gezamenlijke stuurgroep en specifieke deeldoelstellingen en bijbehorende budgetten.

5 HUIDIGE INRICHTING INFORMATIEVEILIGHEID OP DE BESTUURSLAGEN

5.1 Beschrijving huidige inrichting verantwoording en toezicht bestuurslagen

Het onderzoek is uitgevoerd op basis van enerzijds een documentstudie en anderzijds interviews met verschillende belangrijke actoren. Dit hoofdstuk is een samenvatting van de informatie die wij uit deze beide onderdelen van het onderzoek hebben gehaald. Onderstaand geven wij een uiteenzetting van de huidige inrichting van toezicht en verantwoording binnen de verschillende bestuurslagen.

Als kader voor de beschrijving van inrichting verantwoording en toezicht per bestuurslaag schetsen we de verschillende lagen van wet- en regelgeving die van toepassing is op informatieveiligheid bij de overheid.

5.1.1 Strategische laag

Op landelijk niveau bestaat er wet- en regelgeving of is deze in ontwikkeling. Daarin worden de kaders beschreven van het niveau en invulling van toezicht en verantwoording over informatieveiligheid. Het wetsvoorstel Digitale Overheid (WDO) is in behandeling in de Tweede Kamer en de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) treedt binnenkort in werking. Alvorens de inrichting van het toezicht per bestuurslaag te beschrijven geven we een schets van de samenhang tussen de verschillende niveaus van wet- en regelgeving voor informatieveiligheid.

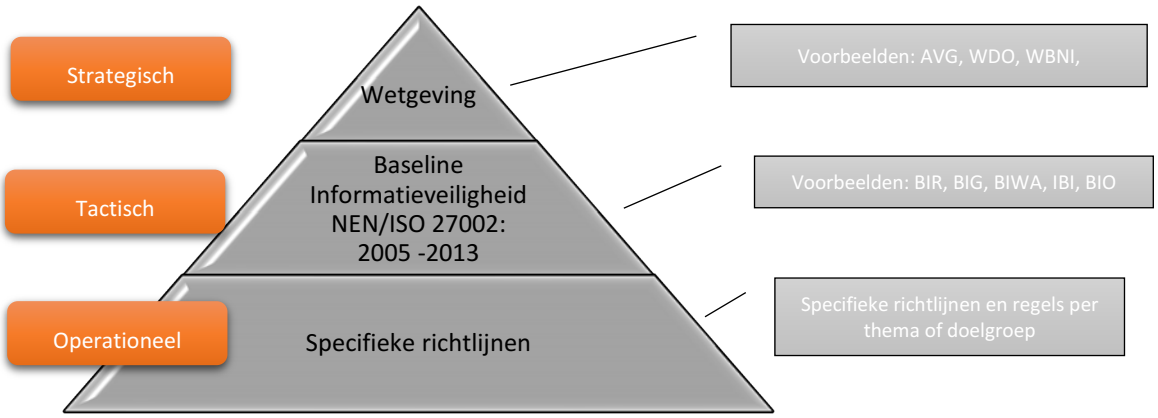
5.1.2 Tactische laag

De landelijke wet- en regelgeving biedt het juridische kader voor te hanteren normenkaders voor informatieveiligheid. Het Rijk, de gemeenten, de waterschappen en provincies hanteren hun eigen respectievelijke normen, de BIR, BIG, BIWA en IBI. Deze normen zijn samen gebracht in de Baseline Informatiebeveiliging Overheid (BIO). Deze baseline wordt het nieuwe normenkader voor alle overheden. De huidige baselines van gemeenten, provincies, waterschappen en het rijk zijn allemaal nog gebaseerd op de NEN/ISO 27002:2005. Den BIO sluit aan op de nieuwe standaard NEN/ISO 27002:2013. De BIO wordt gezamenlijk beheerd, onder regie van het ministerie van BZK.

5.1.3 Operationele laag

Elke bestuurslaag heeft op operationeel niveau specifieke richtlijnen ontwikkeld. Deze variëren in thema en doelgroep.

De gehele structuur is weergegeven in Figuur 1.



Figuur 1: Gelaagdheid in kaders Informatieveiligheid

De manier waarop informatieveiligheid wordt gehandhaafd verschilt per bestuurslaag. Onderstaand een uiteenzetting van de documentatie hierover en beleidsuitgangspunten die zijn opgehaald bij de geïnterviewden.

5.2 Rijksniveau

Verschillende ontwikkelingen hebben de afgelopen jaren invloed gehad op de ontwikkeling van toezicht en verantwoording over informatieveiligheid. Concrete voorbeelden hiervan zijn 'Lektober' (2011) en de daaruit voortvloeiende DigiD audits bij aangeslotenen.

Een ander voorbeeld was de Taskforce BID begin 2013. Deze Taskforce was een initiatief van BZK om de informatieveiligheid binnen de overheidsgeledingen te versterken. De taskforce heeft een belangrijke bijdrage geleverd om 'bestuurders te doordringen van het belang van digitale veiligheid' en 'hen te voorzien van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie'. Gebaseerd op dit onderzoek zijn er kamerbrieven over Informatieveiligheid opgesteld waarin één belangrijk beleidsuitgangspunt centraal stond: Iedere bestuurslaag is zelf verantwoordelijk voor het borgen van informatieveiligheid. Bestuursorganen dragen daaraan bij door 'verplichtende zelfregulering'.

Dankzij het programma Compacte Rijksdienst (2011-2012) hebben de Belastingdienst, DUO, SVB en UWV het Centrum Informatiebeveiliging en Privacybescherming (CIP) opgezet. Het CIP is een netwerkorganisatie waarin participanten van alle overheidslagen samenwerken. Het CIP beoogt een bijdrage te leveren aan de informatieveiligheid van de Nederlandse overheid en de ketens waarin de organisaties samenwerken.

Het Nationaal Cyber Security Centrum (NCSC) is op 1 januari 2012 opgericht. Het NCSC bestaat uit een samenwerking van publieke en private organisaties die zich richt op een integrale aanpak van cybersecurity waar informatieveiligheid een onderdeel van uitmaakt. Het Computer Emergency Response Team van de overheid (GovCert) maakt sinds 1 augustus 2011 onderdeel uit van het

Nationaal Cyber Security Centrum (NCSC). Binnen het NCSC worden tactische en operationele kennis en expertise uit de publieke en private sector bij elkaar gebracht.

Met de Wet revitalisering generiek toezicht is een weg ingezet om toezichtlasten omlaag te brengen door de specifieke toezichtarrangementen terug te dringen en deze te vervangen door vormen van generiek toezicht. Dit houdt in dat interbestuurlijk toezicht in beginsel generiek is en dat dit is belegd bij de hoger gelegen bestuurslaag, tenzij deze aanwijsbaar geen expertise heeft op het betreffend domein.

Met de ontwikkeling van eerst de Wet Generieke Digitale Infrastructuur en nu de Wet Digitale Overheid wordt de Europese eIDAS verordening in nationale wetgeving geïmplementeerd. Met de komst van eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken.

Het wetsvoorstel Digitale Overheid vormt een eerste tranche van regelgeving ten behoeve van toegang tot de digitale overheid .

Met de Wet beveiliging netwerk- en informatiesystemen (Wbni) wordt de Europese NIB-richtlijn omgezet naar Nederlands recht. Het doel is dat lidstaten hun digitale weerbaarheid verbeteren en beter met elkaar samenwerken, zodat Europa digitaal veiliger wordt.

5.3 Gemeenten

Tijdens de bijzondere Algemene Leden Vergadering van de VNG op 29 november 2013 hebben de gemeenten ingestemd met de resolutie dat informatieveiligheid onderdeel wordt van de collegeambities 2014-2018 en opgenomen wordt in de portefeuille van een van de leden van het college van B&W. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Het informeren van de gemeenteraad moet plaatsvinden via een aparte paragraaf informatieveiligheid in het jaarverslag.

Tijdens die bijzondere ALV van de VNG in 2013 hebben de gemeenten ook de Baseline Informatiebeveiliging Gemeenten (BIG) vastgesteld als hét gemeentelijke basisnormenkader voor informatieveiligheid. Samen met de VNG en de Informatie Beveiliging Dienst (IBD) hebben gemeenten gewerkt aan de realisatie van de aangenomen resolutie van de VNG. Eén van de punten van realisatie was de uitwerking van het toezicht op en de verantwoording over informatieveiligheid. Gemeenten maken de lokale invulling rondom het thema van informatieveiligheid transparant voor burgers, bedrijven en (keten)partners. Deze transparantie wordt onder meer bereikt door inzet van de VNG-website waarstaatjegemeente.nl. Deze openbare informatie op de site vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews). Daarnaast toetst een interbestuurlijke visitatiecommissie, tenminste eens in de vijf jaar, of het systeem van ‘verplichtende zelfregulering’ voldoende werkt.

Het werk van de Taskforce BID, de initiatieven van het IBD en de visitatiecommissie (met als eindrapport “Durven Leren”) hebben bijgedragen aan het creëren van bestuurlijk bewustzijn.

Daarnaast is door de ontwikkeling van ENSIA (Eenduidige Normatiek Single Information Audit) een bestuurlijk verantwoordingsproces opgesteld voor (en door) gemeenten om het toezicht op informatieveiligheid verder te professionaliseren en aan te sluiten op de gemeentelijke planning en control cyclus. Uitgangspunt van ENSIA is de single information audit. Dit betekent dat er één keer per jaar een zelfevaluatie op het brede gebied van informatieveiligheid wordt uitgevoerd. Die informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting departementen. Zo is het verticale toezicht op de naleving van zowel de Paspoortwet als de Wet BRP belegd bij de minister van BZK. Waar mogelijk baseert het verticale toezicht zich op de uitkomsten van het horizontale toezicht bij gemeenten. Daar waar de eerste stappen op dit gebied zijn gezet, zien de meeste gemeenten nog ruimte om hierin te leren en te groeien. Daarnaast bestaat er ook nog tussen de gemeenten veel verschillen in volwassenheid.

Eind 2018 is door de VNG het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020 uitgebracht. Dit dreigingsbeeld heeft als doel gemeenten weerbaarder te maken op het gebied van informatiebeveiliging door inzicht te geven in de belangrijkste risico’s voor de eigen organisatie. Hierin wordt bestuurders een handelingsperspectief geboden in de vorm van een bestuurlijke risicoanalyse en prioriteitstelling.

5.4 Provinciën

In 2010 is de Interprovinciale Baseline Informatieveiligheid (IBI) vastgesteld. De IBI beschrijft een standaard maatregelen set en een standaard Business Impact Analyse (BIA)-methodiek die moeten leiden tot een uniforme werkwijze voor alle provincies op het gebied van informatieveiligheid. Hierbij zijn afspraken gemaakt over de provinciale invulling van zelfregulering en vastgelegd in het convenant ‘Interprovinciale Regulering Informatieveiligheid’.

Het Interprovinciaal Overleg (IPO) is eigenaar van de IBI. Op IPO-niveau wordt gerapporteerd over de status van informatieveiligheid middels een monitor. Informatieveiligheid is voor de provinciën onderdeel van de bedrijfsvoering loopt daarmee mee in de planning en control-cyclus.

Onderdeel van het IPO is het CIBO, het Centraal Informatiebeveiligingsoverleg, waarin alle 12 provincies vertegenwoordigd zijn. Het CIBO is inhoudelijk verantwoordelijk voor de IBI en voor het actualiseren hiervan. Er loopt een verkenning op samenwerking met de gemeentelijke IBD en het Nationaal Respons Netwerk (NRN) van het NCSC, om de response bij dreigingen, incidenten en crisis beter te kunnen organiseren.

5.5 Waterschappen

In 2013 is het programmaplan ‘Informatieveiligheid voor de waterschappen’ gelanceerd. Middels het programmaplan zijn afspraken gemaakt over de kaders, ambitie en governance voor

'verplichtende zelfregulering' bij waterschappen. Dit programmaplan is bestuurlijk vastgesteld door de Unie van Waterschappen (UvW). Elk waterschap is verantwoordelijkheid om aantoonbaar aan informatieveiligheid te werken.

In samenwerking met Het Waterschapshuis zijn alle waterschappen in 2013 gestart met de implementatie van de BIWA. De BIWA bevat een aantal minimale beveiligingsniveaus waaraan een waterschap moet willen voldoen. Ten aanzien van de risico's die niet door de BIWA zijn afgedekt, moet het management van het waterschap aanvullende maatregelen vaststellen. Allen hebben daartoe besloten informatieveiligheid op te nemen in hun reguliere planning en control-cyclus. Daarnaast loopt er vanuit Het Waterschapshuis een Programma Informatieveiligheid om producten te ontwikkelen en kennis te delen rondom het thema. In 2017 heeft hebben de waterschappen zich extern te laten auditen op de BIWA en hebben het voornemen dit jaarlijks te herhalen, met als doel toe te groeien naar een hoger volwassenheidsniveau van informatieveiligheid. De waterschappen willen als het gaat om informatieveiligheid transparant zijn om het vertrouwen in de sector te vergroten.

5.6 Gemeenschappelijke regelingen

Op dit moment zijn de gemeenschappelijke regelingen nog een 'witte vlek' als het gaat om verantwoording en toezicht op het gebied van informatieveiligheid. Noch uit het documentenonderzoek, noch uit de interviews is een eenduidig beeld naar voren gekomen m.b.t. de huidige status of een toekomstvisie ten aanzien van informatieveiligheid en verantwoording binnen de gemeenschappelijke regelingen.

De gemeenschappelijke regeling is een instrument om vraagstukken die grensoverschrijdend zijn voor bestuursorganen en -lagen op te lossen en daarmee een belangrijk vehikel voor de dienstverlening naar de burgers en ondernemers toe en een belangrijk. Toch worden deze regelingen nog niet (h)erkend in de meeste beleidstukken of staat informatieveiligheid nog niet op de agenda. Bij de introductie van ENSIA is dit vraagstuk duidelijk naar voren gekomen.

Een uitzondering hierop vormen de veiligheidsregio's. Het Veiligheidsberaad heeft een programma Informatievoorziening veiligheidsregio's 2015-2020 vastgesteld. Daarin is informatieveiligheid als één van de zes prioriteiten opgenomen. Om de regio's te ondersteunen bij de realisatie van informatieveiligheid is door de vakgroep Informatieveiligheid een traject van collegiale toetsing opgezet.

6 WET REVITALISERING GENERIEK TOEZICHT, WET DIGITALE OVERHEID EN WET BEVEILIGING NETWERK- EN INFORMATIESYSTEMEN

6.1 Inleiding

Voor dit onderzoek zijn bovengenoemde drie (voorstellen van) wetten relevant. Deze wetten doen uitspraken over de wijze waarop verantwoording en (interbestuurlijk) toezicht op onder meer informatieveiligheid georganiseerd dient te zijn. Dit zijn wetten met een generieke strekking. In specifieke sectorale wetgeving zijn ook toezichtparagrafen opgenomen. Deze blijven buiten de scope van dit onderzoek. In dit onderzoek is nagegaan welke uitspraken deze wetten doen over interbestuurlijk toezicht en toezicht op informatieveiligheid.

6.2 Wet revitalisering generiek toezicht

Teneinde de vereenvoudiging van het interbestuurlijke toezicht is de Wet Revitalisering Generiek Toezicht (wet RGT) ingevoerd. Daar waar er in het verleden veel instrumenten voor interbestuurlijk toezicht waren die het een complex en bureaucratisch geheel maakten, is sinds 1 oktober 2012 de wet RGT ingevoerd die een eind maakte aan veel specifieke toezichtsbepalingen om het proces van toezicht eenvoudiger en transparanter te maken. Deze lijn geldt als uitgangspunt bij nieuw beleid. Dit houdt in dat eventueel toezicht in beginsel generiek is en dat het is belegd bij de naast hoger gelegen bestuurslaag, tenzij deze aanwijsbaar geen expertise heeft op het betreffend domein.

Het uitgangspunt van de wet is vertrouwen: "*Het vertrouwen dat een bestuurslaag zijn taken goed uitoefent. En dat de horizontale verantwoording - van gemeentebestuur aan gemeenteraad en van Gedeputeerde Staten aan Provinciale Staten - op orde is. Verder geldt het uitgangspunt 'eenmalige uitvraag, meervoudig gebruik': gemeenten en provincies hoeven voortaan hun verantwoordingsinformatie dus nog maar 1 keer aan te leveren*"[3].

Gemeenten hebben een toezichthouder per beleidsdomein. De Provincie is conform de wet RGT de toezichthouder voor ruimtelijke ordening, bouwen, milieu, huisvesting, monumenten, archieven (overheidsinformatie) en constructieve veiligheid van bouwwerken. Het Rijk is toezichthouder op die terreinen waar provincies geen taak of expertise hebben (bijvoorbeeld onderwijswetten en sociale zaken). Het Rijk is toezichthouder op provincies, als het gaat om provinciale medebewindstaken.

Door deze wet is het specifieke toezicht afgeschaft, maar wel met uitzondering als er sprake is van uitvoeringsvervlechting of functioneel bestuur. Uitvoeringsvervlechting houdt in dat de toezichthouder een wettelijke operationele verantwoordelijkheid heeft, waarbij deze voor de uitvoering volledig afhankelijk is decentrale overheden, zoals bij de Veiligheidsregio's. Functioneel

[3] Rijksoverheid, 2018, https://www.rijksoverheid.nl/onderwerpen/provincies/interbestuurlijk-toezicht

bestuur houdt in dat de provincie de taakvervulling van waterschappen (functioneel bestuur) moet inpassen in haar algemeen beleid. Daarom blijft het specifieke toezicht op waterschappen bestaan.

6.3 Wet Digitale Overheid

In het wetsvoorstel Digitale Overheid (WDO) wordt de wettelijke basis gelegd voor de gehele generieke digitale infrastructuur (GDI). Onderdeel hiervan zijn regels over informatieveiligheid en privacy. Het wetsvoorstel biedt daarmee de grondslag om overheidsinstanties te verplichten open standaarden te gebruiken. Ook toezicht en handhaving krijgt hiermee een wettelijke basis.

De basis van dit wetsvoorstel is gegrond op het principe dat alle bestuursorganen van de verschillende bestuurslagen voldoen aan bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten op verschillende betrouwbaarheidsniveaus. Bestuursorganen zijn daarbij verantwoordelijk voor de naleving van de wet en dat de taken op het niveau waarop deze zijn belegd toereikend worden opgepakt[4].

6.3.1 Horizontale verantwoording en interbestuurlijk toezicht

De controle op de juiste en toereikende naleving van de wet ligt bij de horizontale verantwoording binnen een bestuurslaag. In de tweede plaats komt het interbestuurlijk toezicht op de decentrale overheden, conform het beginsel dat slechts één bestuurslaag – de naast hoger gelegen bestuurslaag – toezicht houdt. Deze wet is in lijn met de uitgangspunten van de Wet revitalisering generiek toezicht, dat interbestuurlijk toezicht sober en terughoudend is. Uit de memorie van toelichting: "*In lijn met dit beginsel houdt de Minister toezicht op overheidsorganen op het niveau van de provincies en houden provincies toezicht op overheidsorganen op het niveau van gemeenten. Dit wetsvoorstel verplicht het provincies om de Minister te informeren over de (mate van) naleving door overheidsorganen op het niveau van gemeenten. Het interbestuurlijk toezicht biedt de naast hoger gelegen bestuurslaag (uitsluitend) de mogelijkheden tot repressief ingrijpen, te weten schorsing en vernietiging bij handelen in strijd met het recht of het algemeen belang (door de Kroon) en in uiterste gevallen indeplaatsstelling (bij taakverwaarlozing)[5]".*

Hierbij wordt een grote verantwoordelijkheid voor toezicht op gemeenten op het gebied van informatieveiligheid neergelegd bij de provincie. Dit is voor de provincie een geheel nieuwe taak, waarbij tegelijkertijd de provincie ook zelf een bestuursorgaan is dat dient te voldoen aan de informatieveiligheidseisen van de wet. Zoals beschreven vereist het toezicht op informatieveiligheid specifieke expertise die in de huidige praktijk vooral aanwezig is op rijksniveau**.** Indien het gewenst is dat in lijn met deze wet het primaat van interbestuurlijk toezicht op informatieveiligheid wordt gelegd bij de naast hoger gelegen bestuurslaag dat moet nagegaan worden welke gevolgen dit heeft voor de ontwikkeling van kennis en expertise voor deze taakuitvoering bij de provincie. Indien het gewenst is het primaat van het interbestuurlijk toezicht

[4] Wet Digitale Overheid, Vergaderjaar 2017–2018, artikel 4, lid 1

[5] Memorie van toelichting, Vergaderjaar 2017–2018, p.33

op informatieveiligheid op gemeenten, provincies en waterschappen te beleggen op rijksniveau dient nagegaan welke gevolgen dit heeft voor het huidige wetsvoorstel.

6.3.2 Verantwoording en auditing

De wet kent in artikel 4, lid 2 een aanvullende verplichting tot auditing. *"Bestuursorganen en aangewezen organisaties overleggen aan Onze Minister een verklaring van een auditor waaruit blijkt of zij voldoen aan de in het eerste lid bedoelde regels."* De Memorie van Toelichting (MvT) bij de wet geeft aan dat het bestuursorgaan of de aangewezen organisatie in aanvulling op het generiek toezicht regulier een verklaring van een auditor aan de Minister moet overleggen. De auditor toetst daarbij of de dienstverlener aan de eisen voldoet. Bij gemeenten wordt momenteel de ENSIA systematiek gehanteerd, waarbij het college een verklaring opstelt voor de raad over de naleving van de beveiligingsnormen. De auditor voegt daar een auditverklaring bij. De Collegeverklaring en de auditverklaring worden gezonden aan het ministerie van BZK.

De wet geeft de Minister de mogelijkheid om bij een ernstige storing of aantasting dan wel misbruik of ongeoorloofd gebruik van de toegang tot elektronische dienstverlening of als ook na aanmaningen de benodigde verbeteringen niet worden aangebracht als uiterste middel de bevoegdheid de toegang tot elektronische dienstverlening van een bestuursorgaan of een aangewezen organisatie te (doen) onderbreken.

Artikel 4 lid 3 van de wet geeft aan dat de Minister bij of krachtens algemene maatregel van bestuur regels stelt over de wijze waarop bestuursorganen en aangewezen organisaties aantonen dat zij aan de regels, bedoeld in het eerste lid, voldoen.

In versie 21 augustus 2018 van het concept 'Besluit houdende wijziging van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking' wordt een kader geboden voor de dienstverleners in de relevante beleidsdomeinen. Daarbij is het streven dat er materieel niet of nauwelijks nieuwe verplichtingen zullen gelden. De verwachting wordt uitgesproken dat de administratieve lasten en kosten (regeldruk) voor dienstverleners beperkt blijven.

Feitelijk betreft dit een uitwerking van de wijze waarop bestuursorganen en aangewezen organisaties informatieveiligheid plannen, organiseren, uitvoeren en monitoren, alsmede de wijze waarop daar audits op werden uitgevoerd. Het concept besluit verwijst naar ISO/NEN 27001 – 27002 als norm waaraan bestuursorganen en aangewezen organisaties dien te voldoen. Inmiddels is besloten dat voor de gehele overheid de Baseline Informatiebeveiliging Overheid (BIO) wordt gehanteerd.

In dit concept worden in paragraaf 5.3 Monitoring en verantwoording in de artikelen 22 t/m 24 regels gesteld voor Aansluiting, Logging en Audit. In deze paragraaf wordt niet aangegeven op welke wijze het bestuursorgaan zich dient te verantwoorden over het gevoerde beheer.

In de internationale corporate governance praktijk (COSO) is de verantwoording door een organisatie over het gevoerde beheer het meest cruciale moment in de planning en control-cyclus. In de verantwoording geeft de organisatie aan op welke wijze het beleid is gerealiseerd, welke afwijkingen er zijn en welke verbeteringen worden doorgevoerd. Dit naar analogie met de financiële verantwoording/jaarrekening. Met ENSIA is bij gemeenten de weg ingeslagen dat het college zich aan de raad verantwoordt over het gevoerde informatieveiligheid beleid. Ook waterschappen hanteren voor informatieveiligheid de verantwoording van het Dagelijks Bestuur (DB) aan het Algemeen Bestuur (AB) als het centrale moment in de planning en control-cyclus.

De internationale audit en assurance praktijk sluit aan op de internationale corporate governance praktijk. De auditor geeft een verklaring van getrouwheid bij de verantwoording door de organisatie over het gevoerde beheer. Gezien de potentieel bredere reikwijdte van de Wet Digitale Overheid dan alleen toegang tot de digitale overheid kan de verantwoording gaan over het bredere beheer van de generieke digitale infrastructuur zoals genoemd in Artikel 5; verantwoordelijkheid voor het beheer van de generieke digitale infrastructuur: *“Onze Minister draagt zorg voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur, waaronder infrastructuur.”*

De auditor kan zelfstandig een assurance rapport opstellen over de het gevoerde beheer gericht op informatieveiligheid. Auditors noemen dit 'direct reporting'; de auditor doet direct verslag van zijn waarnemingen. De beroepsorganisatie NOREA heeft geen voorkeur voor ‘direct reporting’. De (ook internationaal) gewenste assurance benadering is is 'assertion based', waarbij de auditor zijn rapport (verklaring van getrouwheid) voegt bij een 'management assertion' (de verantwoording) door een organisatie aan de betrokken stakeholders. Daarmee wordt meer de centrale rol van het bestuursorgaan benadrukt om verantwoording te nemen en verantwoording af te leggen aan de stakeholders/toezichthouders over het gevoerde beheer.

Overwogen kan worden de ‘assertion based’ assurance benadering op te nemen in het besluit. Daarmee sluit het beter aan bij de algemeen geaccepteerde governance en assurance praktijk en ook de weg die met ENSIA is ingeslagen.

6.4 Wet BNI en verhouding tot BZK

De Europese NIB-richtlijn[6] is door de Nederlandse overheid in de nationale wetgeving geïmplementeerd. Vanwege de inhoudelijke samenhang en overlap met de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) zijn de NIB-richtlijn en de Wgmc samengegaan in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

In de Wbni en het onderliggende Besluit beveiliging netwerk- en informatiesystemen (Bbni) worden vitale aanbieders aangewezen. De wet spreekt van een aanbieder als een

[6] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, (PbEU 2016, L 194).

overheidsorganisatie of privaatrechtelijke rechtspersoon een dienst exploiteert, beheert of beschikbaar stelt. In de wet is de definitie van een vitale aanbieder tweeledig, hierdoor ontstaan twee soorten vitale aanbieders:

1. Aanbieder van een essentiële dienst (*AED*) (artikel 2 Bbni) of;
2. Aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving (*zogenaamde andere vitale aanbieders*) (artikel 3 Bbni).

AED's zijn op basis van sectoren door Europa in de NIB-richtlijn aangewezen.[7] Het andere type vitale aanbieder komt voort uit de voormalige Wgmc en wordt door de vakdepartementen zelf geïdentificeerd en aangewezen als een vitale aanbieder.[8]

6.4.1 Meldplichten onder de Wbni

Voor beiden type vitale aanbieders is een zogenaamde meldplicht bij het NCSC opgenomen. Een melding moet worden gedaan op het moment dat inbreuk of een incident aanzienlijke gevolgen heeft voor de continuïteit van de verleende dienstverlening. Het NCSC kan dan zorgen voor informatie, bijstand en advies.

Een andersoortige meldplicht is die aan de bevoegde autoriteiten / toezichthouders.[9] De bevoegde autoriteiten hebben voor wat betreft AED's de taak om zorg te dragen voor de bestuursrechtelijke handhaving ten aanzien van de verplichtingen uit de Wbni. Dit betekent dat de andere vitale aanbieders, niet zijnde AED's geen meldplicht aan een bevoegde autoriteit hebben en dus op basis van de Wbni niet onder toezicht staan.

6.4.2 Rol van de Minister van BZK in de Wbni

Op dit moment zijn door de Minister van BZK geen vitale aanbieders in de Wbni aangewezen, waardoor op basis van de wet geen toezichthoudende rol is weggelegd voor de minister.

In de Nota van Toelichting van het Bbni[10] wordt wel vooruitgelopen op de sector digitale overheid. In deze sector bevinden zich de aanbieders van datasystemen waarvan meerdere overheidsorganisaties afhankelijk zijn. In deze toelichting geeft de Minister van Justitie en

[7] Energie, Vervoer, Bankwezen, Infrastructuur voor de financiële markt, Drinkwater en Digitale infrastructuur. In de Wbni is daarnaast nog een privaatrechtelijke groep aangewezen namelijk de Digital Service Providers (DSP's) maar deze zijn niet als vitaal aangewezen.

[8] Op dit moment de sectoren: Nucleair, Keren en Beheren, Financieel, Elektronische communicatienetwerken en -diensten/ICT (zijnde de diensten die telefoon-, sms- of internettoegangsdienst verlenen).

[9] Het betreft hier de: 1. De Minister van Economische Zaken voor de sectoren energie en digitale infrastructuur; 2. De Nederlandsche Bank N.V. voor de sectoren bankwezen en infrastructuur voor de financiële markt; 3. De Minister van Infrastructuur en Waterstaat voor de sectoren vervoer en levering en distributie van drinkwater; 4. De minister voor Medische Zorg gezondheidszorg (*red. vooralsnog geen sectoren aangewezen als AED*). Deze toezichthouders kunnen het toezicht naar eigen inzicht vormgeven.

[10] Staatsblad 8 november 2018, nr. 388.

Veiligheid aan dat de sector: *"naar verwachting bij de eerstvolgende wijziging van het Bbni aan artikel 3 worden toegevoegd".*

Op het moment dat de sector digitale overheid aan artikel 3 Bbni wordt toegevoegd, impliceert dit een kwalificatie als een "andere vitale aanbieder" niet zijnde een AED. De vitale aanbieders in de sector digitale overheid zullen op dat moment alleen moeten voldoen aan de meldplicht bij het NCSC.

6.4.3 Toekomstige rol BZK in de Wbni

Zonder de Wbni en het onderliggende besluit aan te passen is de minister van BZK alleen in staat om vitale aanbieders in deze sector aan te wijzen. Het is daarbij niet mogelijk om de sector als AED aan te wijzen omdat in de huidige Wbni AED's worden gekoppeld aan de sectoren uit artikel 4 van de NIB-richtlijn. In de NIB-richtlijn is de sector digitale overheid niet opgenomen.

De Minister van BZK zal op basis van de huidige Wbni daarom niet geëquipeerd zijn om toezicht te houden op de sector digitale overheid. Indien de Minister van BZK wel via de Wbni wettelijk toezicht wenst te verkrijgen moet het wetsvoorstel door de Minister van Veiligheid en Justitie worden aangepast. Zo kan in een aanpassing van de wet de bestuursrechtelijke handhaving op AED's ook van toepassing worden verklaard op het andere type vitale aanbieder.

7 TOEZICHTSVARIANTEN

7.1 Beleidsuitgangspunten over toezicht op informatieveiligheid

Uit de interviews en documentstudie zijn meerdere standpunten over interbestuurlijk toezicht op informatieveiligheid naar voren gekomen. Deze standpunten kunnen richting geven aan de keuzes die gemaakt moeten worden voor het in te richten interbestuurlijk toezicht op informatieveiligheid.

Het overkoepelende kader voor toezicht is verwoord op pagina 33 van de Memorie van Toelichting bij de WDO: "*In lijn met de Wet revitalisering generiek toezicht is het toezicht van de hogere overheid op de naleving van het wetsvoorstel door de lagere overheid (interbestuurlijk toezicht) sober en terughoudend. Decentrale overheden zijn zelf verantwoordelijk voor de naleving van de wet en er wordt op vertrouwd dat de taken op het niveau waarop deze zijn belegd toereikend worden opgepakt. Het primaat voor de controle op de naleving ligt bij de horizontale verantwoording binnen een bestuurslaag."* Dit kader is het uitgangspunt bij de vorming van nieuw beleid en houdt in dat eventueel verticaal toezicht in beginsel generiek is en dat het is belegd bij de naast hoger gelegen bestuurslaag, tenzij deze aanwijsbaar geen expertise heeft op het betreffend domein.

Op basis van de eerdergenoemde documentstudie, de interviews en de kaders van wet- en regelgeving is onderstaand overzicht opgesteld met beleidsuitgangspunten. Dit overzicht geeft een beeld van de meest maatgevende uitgangspunten voor toezicht op informatieveiligheid.

1. Horizontaal toezicht door het bestuursorgaan, inclusief externe auditing is de basis voor de inrichting van verantwoording en toezicht voor alle bestuurslagen.

2. Iedere bestuursorgaan opereert in de keten van de generieke digitale infrastructuur. Er moet transparantie zijn en toezicht in de keten bestaan over de informatieveiligheid van deze infrastructuur.

3. De verantwoording- en auditlast moet beperkt blijven door gebruik van standaarden en hergebruik van beschikbare verantwoordingsinformatie.

4. Specifieke toezichtarrangementen worden teruggedrongen en zoveel mogelijk vervangen door vormen van generiek toezicht.

5. Naast wettelijke kaders kunnen ook (niet-wettelijke) kwaliteitsinstrumenten bijdragen aan informatieveiligheid. Voorbeeld van instrumenten zijn:
    a. Visitatie
    b. Benchmarking
    c. Praktijktraining
    d. Leren en groeien in volwassenheid

7.2 Toezichtvarianten

Verschillende vormen van toezicht zijn mogelijk. Onderstaand beschrijven wij vier varianten voor toezicht, variërend van zelfregulering/horizontaal toezicht per bestuurslaag tot verticaal toezicht op de naleving van de voorwaarden voor generieke digitale infrastructuur voorzieningen. In alle gevallen is de basis voor het toezicht een constructieve dialoog over onderwerpen die de uitvoering en sturing raken met als doel te werken aan continue verbetering en toegevoegde waarde. Dit om te voorkomen dat pas achteraf wordt bijgestuurd. Het vereist dat er veel geïnvesteerd wordt in een goede open relatie. Interesse en betrokkenheid in de organisatie en de bereidheid ontwikkelingen en onderwerpen buiten de planning en control-cyclus om met elkaar te delen.

De varianten worden beschreven aan de hand van een aantal onderscheidende criteria voor verantwoording en toezicht:

1. De verantwoording van het bestuursorgaan
2. De wijze van toezicht
3. De rol van audits
4. De verantwoordingsinformatie

1. ALLEEN HORIZONTAAL TOEZICHT

Deze variant gaat ervan uit dat het bestuursorgaan zelf binnen de reguliere planning en control-cyclus verantwoordelijk is voor de planning, uitvoering, controle en verantwoording over informatieveiligheid. De BIO vormt daarbij de basis. Het toezicht is uitsluitend horizontaal en vindt plaats door de gekozen vertegenwoordiging. De auditor geeft een verklaring van getrouwheid bij de verantwoording over informatieveiligheid. Kwaliteitsinstrumenten als intercollegiale reviews, benchmarking en praktijkoefeningen dragen bij aan transparantie en het lerend vermogen op het gebied van informatieveiligheid. Het toezicht van het rijk beperkt zich tot het verzamelen van de informatie voor het uitvoeren van beleidsmatige risicoanalyses en op te stellen benchmarks en is niet gericht op het toetsen van de naleving en het eventueel nemen van (interbestuurlijke) maatregelen bij niet-naleving.

2. HORIZONTAAL TOEZICHT EN VERTICALE INFORMATIEVOORZIENING

In deze variant stelt het bestuursorgaan op basis van de BIO een horizontale verantwoording op over de informatieveiligheid en de auditor geeft een verklaring van getrouwheid. Kwaliteitsinstrumenten als intercollegiale reviews, benchmarking en praktijkoefeningen dragen bij aan transparantie en het lerend vermogen op het gebied van informatieveiligheid. Het rijk maakt daarbij afspraken met de bestuursorganen over de gewenste verticale informatievoorziening over informatieveiligheid en sluit daarbij zoveel mogelijk aan bij de generieke basis van de BIO. Specifieke informatiebehoeften worden vanuit een specifiek toezichtbeleid gemotiveerd. Het toezicht van het rijk beperkt zich tot het verzamelen van de informatie voor het uitvoeren van beleidsmatige risicoanalyses en het opstellen van rapportages en is niet gericht op het toetsen van de naleving en het eventueel nemen van (interbestuurlijke) maatregelen bij niet-naleving.

3. HORIZONTAAL TOEZICHT EN GENERIEK VERTICAAL TOEZICHT

In deze variant stelt het bestuursorgaan op basis van de BIO een horizontale verantwoording op over de informatieveiligheid en de auditor geeft een verklaring van getrouwheid. Kwaliteitsinstrumenten als intercollegiale reviews, benchmarking en praktijkoefeningen dragen bij aan transparantie en het lerend vermogen op het gebied van informatieveiligheid. Het rijk maakt afspraken met de bestuursorganen over de gewenste verticale informatievoorziening over informatieveiligheid en sluit daarbij zoveel mogelijk aan bij de generieke basis van de BIO. Specifieke informatiebehoeften worden vanuit een specifiek toezichtbeleid en risicoanalyse gemotiveerd. Het rijk voert op basis van de verantwoording generiek toezicht uit op de naleving van de voorwaarden voor het gebruik van de generieke digitale infrastructuur. Bij niet-naleving kan het rijk (interbestuurlijke) maatregelen nemen.

Deze situatie komt grotendeels overeen met de huidige praktijk van ENSIA. Daarbij stelt het college van BenW van een gemeente op basis van de BIG (de BIG gaat over in de BIO) en de normen voor DigiD een verantwoording op over informatieveiligheid aan de gemeenteraad. De auditor geeft daar een verklaring bij. De uitkomsten voor het naleven van de SUWInet en DigiD normen worden getoetst door het rijk.

4. SPECIFIEK VERTICAAL TOEZICHT

In deze variant stelt het rijk op basis van haar eindverantwoordelijkheid voor de informatieveiligheid van de generieke digitale infrastructuur en het uitgewerkt toezichtbeleid specifieke eisen aan de verantwoording en verticale informatievoorziening van bestuursorganen die deze voorzieningen gebruiken. Bij de verantwoording dient een verklaring van getrouwheid van de auditor gevoegd te zijn. Het rijk toetst de verantwoording op de naleving van de voorwaarden voor het gebruik van de generieke digitale infrastructuur en kan bij niet-naleving (interbestuurlijke) maatregelen nemen.

Deze situatie komt grotendeels overeen met de huidige praktijk bij DigiD audits. Daar brengt het bestuursorgaan niet zelf een verantwoording uit, maar stelt de auditor rechtstreeks een assurancerapport op over de naleving van de specifieke DigiD normen.

7.3 Scores toezichtvarianten

In onderstaande tabel zijn de verschillende varianten gescoord op de beleidsuitgangspunten over toezicht op informatieveiligheid. De scores zijn gebaseerd op eigen inzichten van de onderzoekers en niet gevalideerd bij de geïnterviewden of bij de opdrachtgever.

Uitgangspunt	Variant	1. Alleen horizontaal toezicht	2. Horizontaal toezicht en verticale informatie	3. Horizontaal toezicht en verticaal generiek toezicht	4. Specifiek verticaal toezicht
1.	Zelfregulering	++	+	+	0
2.	Transparantie in de keten	-	0	++	++
3.	Beperken auditlast	+	+	0	-
4.	Terugdringen specifiek toezicht	++	+	0	--
5.	Inzet kwaliteitsinstrumenten	++	+	+	0

De toezichtvarianten 1. en 4. laten hierbij een wisselende positieve/negatieve score zien op de uitgangspunten en de toezichtvarianten 2. en 3. meer gemiddeld positief scoren.

Toezicht variant 1. scoort hoog op de uitgangspunten die samenhangen met horizontaal toezicht, maar minder op het uitgangspunt transparantie in de keten.

Toezichtvariant 4. scoort hoog op transparantie in de keten, maar minder op terugdringen auditlast en laag op terugdringen specifiek toezicht.

De varianten 2. en 3. Scoren neutraal/positief op de geformuleerde beleidsuitgangspunten. Deze bespreken wij in de volgende paragraaf meer in detail.

7.4 Analyse Toezichtvarianten 2. en 3.

In toezichtvariant 2. ‘Horizontaal toezicht en verticale informatie’ ligt de nadruk op de eigen verantwoordelijkheid van het bestuursorgaan voor de borging van de informatieveiligheid. Informatieveiligheid maakt integraal onderdeel uit van de planning en control-cyclus van het bestuursorgaan. Bestuursorganen zetten tevens kwaliteitsinstrumenten in om transparantie te geven over de informatieveiligheid.

Het toezicht door het rijk wordt ingevuld met bestuurlijke afspraken over de verticale verantwoordingsinformatie over de informatieveiligheid. Het rijk kan op basis van eigen analyses een risicorapportage opstellen en deze publiekelijk delen met de betrokken partijen. Het is vervolgens aan de bestuursorganen om navolging te geven aan de signalen. Dit wordt niet afgedwongen door interbestuurlijke maatregelen.

In deze toezichtvariant wordt sterk gesteund op de kracht van transparante informatievoorziening en het versterken van de betrokkenheid van burgers, instellingen en bedrijven bij de prestaties van het bestuursorgaan op het gebied van informatieveiligheid. Deze variant geeft beperkte mogelijkheden om interbestuurlijke maatregelen te treffen bij het niet naleven van de eisen van informatieveiligheid. Natuurlijk biedt het generieke toezichtinstrumentarium uit de Wet revitalisering generiek toezicht mogelijkheden tot interventie, maar deze moet gezien worden als een ultimum remedium.

Toezichtvariant 3. 'Horizontaal toezicht en verticaal generiek toezicht' combineert het horizontale toezicht van het bestuursorgaan met generiek toezicht door het rijk op de naleving van voorwaarden voor het gebruik van de generieke digitale infrastructuur, waarvoor het rijk de eindverantwoordelijkheid draagt. Voor veel generieke digitale voorzieningen gelden dezelfde generieke beveiligingseisen, zoals deze opgenomen in de BIO. Op basis van een risicoafweging kunnen aanvullende specifieke eisen gelden, die veelal een nadere uitwerking zijn van de generieke beveiligingseisen. Het toezicht door het rijk wordt in de variant ingevuld door een toezichtarrangement dat bestaat uit de volgende onderdelen:

1. Een informatieprotocol, waarin (jaarlijks) afspraken worden opgenomen over de wederzijdse informatieverplichtingen tussen toezichthouder en bestuursorgaan.
2. Een controleprotocol, waarin (jaarlijks) afspraken worden gemaakt over de externe audit op de verantwoording over informatieveiligheid.
3. Een risicoanalyse, waarmee inzicht wordt verkregen in de (voor zover het de ministeriële verantwoordelijkheid raakt) meest risicovolle onderwerpen. Het toezicht kan zich vervolgens op deze onderwerpen toespitsen.
4. Het reviewbeleid, waarmee afspraken worden gemaakt over het verrichten van reviews op de verantwoording en de externe audit op de verantwoording.
5. De bevoegdheden waarover de minister beschikt bij het nemen van interbestuurlijke maatregelen bij geconstateerde niet-naleving, waarbij de zwaarte van de maatregelen in overeenstemming moet zijn met de ernst van niet-naleving.
6. De overlegvormen op de verschillende niveaus.

Uit het geformuleerde toezichtbeleid moet blijken hoe ver de ministeriële verantwoordelijkheid zich uitstrekt. Alleen bij uitzondering en gemotiveerd op basis van een risicoanalyse worden specifieke informatie-eisen worden geformuleerd.

De beschreven toezichtvarianten vereisen van zowel het bestuursorgaan als de toezichthouder een hoge mate van volwassenheid, zowel op bestuurlijk vlak als op het vlak van inhoudelijke kennis van informatieveiligheid. Zoals eerder aangegeven bestaan er verschillen in volwassenheid bij bestuursorganen en bestuurslagen. Om te kunnen voldoen aan de criteria, zoals beschreven in de toezichtvarianten, zal een forse inspanning geleverd moeten worden op alle bestuurlijke niveaus. Naar analogie van de Deense programmatisch aanpak voor cyber- en informatiebeveiligingsstrategie zal naar verwachting een interbestuurlijk meerjarig programma voor informatieveiligheid nodig zijn waarin doelstellingen, leer- en groeipaden, projecten,

stimuleringsbudgetten en in te zetten expertisecapaciteit zijn opgenomen. Het ministerie van BZK kan hierbij vanuit haar stelselverantwoordelijkheid een coördinerende rol vervullen.

8 CONCLUSIES EN AANBEVELINGEN

Uit bovenstaande beschrijvingen van de huidige inrichting van de verantwoording en het toezicht op informatieveiligheid, de wettelijke kaders en mogelijke varianten van toezicht is een aantal conclusies te trekken die mede antwoord geven op de geformuleerde vragen voor dit onderzoek. Daar waar relevant geven we tevens *in cursief tevens* onze aanbevelingen daarbij.

8.1 Ontwikkelingen bij de bestuurslagen

1. Op alle bestuurslagen is het bewustzijn over informatieveiligheid toegenomen en zijn initiatieven genomen om informatieveiligheid een onderdeel uit te laten maken van de reguliere planning en control-cyclus. Tussen bestuurslagen en tussen bestuursorganen bestaan nog flinke verschillen in de mate van volwassenheid.

   Om informatieveiligheid een integraal onderdeel te laten zijn van de planning en control-cyclus zullen de meeste bestuursorganen op alle bestuurslagen nog aanzienlijke moeten groeien in volwassenheid.

2. Bij gemeenschappelijke regelingen is de besturing van informatieveiligheid minder ontwikkeld. Een uitzondering hierop vormen de veiligheidsregio's waar informatieveiligheid als één van de prioriteiten is bepaald.

   Bij gemeenschappelijke regelingen zal een forse inspanningen geleverd moeten worden om informatieveiligheid zowel bestuurlijk als inhoudelijk op een hoger volwassenheidsniveau te brengen.

8.2 Ontwikkelingen in het buitenland

1. Van de vier onderzochte landen is de situatie in Nederland het best vergelijkbaar met die van België en Oostenrijk. Ook deze landen zetten in op de organisatie en inrichting van governance van informatieveiligheid. Een duidelijke keuze voor horizontaal of verticaal toezicht is daarbij nog niet gemaakt.
2. In NRW en op bondsniveau in Duitsland is sprake van een sterkere top-down sturing op informatieveiligheid dan in Nederland. De federale wetgeving op het gebied van informatieveiligheid en de sterke positie van het federale BSI spelen daarbij een belangrijke rol.
3. De programmatische aanpak in Denemarken, waarbij tussen de bestuurslagen onder leiding van een coördinerend minister meerjarenafspraken zijn gemaakt over de sturing op informatieveiligheid, kan als voorbeeld dienen voor de Nederlandse situatie.
4. Alle landen geven wel aan dat forse investeringen nodig zijn in de benodigde kennis en kunde op het gebied van informatieveiligheid.

   Het is zinvol de ontwikkelingen in de onderzochte landen te blijven volgen en wederzijds ervaringen uit te wisselen. Daarbij verdient de toepasbaarheid van de programmatische

aanpak van Denemarken in de Nederlandse situatie bijzondere aandacht. Gedacht kan worden aan een meerjaren informatie beveiligingsplan overheid, waarin het ministerie van BZK, de VNG, de UvW en het IPO afspraken maken over de doelen en in te zetten middelen voor interbestuurlijke beleidsprogramma's en projecten om de informatieveiligheid te verbeteren.

8.3 Ontwikkelingen op het gebied van wet- en regelgeving

1. De wet- en regelgeving die relevant is voor de inrichting van verantwoording en toezicht op het gebied van informatieveiligheid legt het primaat bij het horizontaal toezicht binnen een bestuurslaag. Het interbestuurlijk verticaal toezicht op de decentrale overheden kan hier op aansluiten.
2. Het wetsontwerp Digitale Overheid (WDO) gaat ervan uit dat de provincies toezicht houden op gemeenten. Dit is voor de provincie een geheel nieuwe taak, waarbij een geheel nieuw expertisegebied opgebouwd moet worden. In de huidige praktijk is deze expertise vooral aanwezig op rijkniveau**.**

   Ga na op welk bestuurlijk niveau het beste het interbestuurlijk toezicht op informatieveiligheid neergelegd kan worden. Indien het primaat voor interbestuurlijk toezicht op provinciaal niveau dient te liggen, ga dan na welke gevolgen dit heeft voor de kennisontwikkeling op dit bestuurlijke niveau. Indien het primaat van het interbestuurlijk toezicht op informatieveiligheid op rijksniveau dient te liggen, ga dan na welke mogelijkheden hiervoor binnen de verdere ontwikkeling van de WDO en de Wet revitalisering generiek toezicht bestaan.

3. In het concept van het 'Besluit houdende wijziging van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking' bij de WBO worden wel eisen gesteld aan de wijze van auditing van informatieveiligheid, maar niet aan de wijze waarop een bestuursorgaan zich moet verantwoorden over de naleving van informatieveiligheid bij toegang tot de digitale overheid.

   Geef, in navolging van de internationale corporate governance praktijk, de verantwoording van een bestuursorgaan een meer centrale rol in het toezicht op informatieveiligheid. De auditor kan vervolgens een verklaring van getrouwheid geven bij de verantwoording.

4. In de huidige Wbni zijn nog geen vitale aanbieders aangewezen door de Minister van BZK. De aanwijzing van de sector "digitale overheid" wordt wel verwacht in de tweede tranche van de Wbni. Deze aanwijzing wordt aangekondigd in de nota van toelichting van het

onderliggende besluit Bni.[11] Op basis van de huidige vorm van de Wbni zal echter geen toezichthoudende rol weggelegd zijn voor de minister van BZK. Dit heeft te maken met de keuzes en formuleringen bij de implementatie van de wet waardoor twee soorten vitale aanbieders zijn ontstaan. Enerzijds aanbieders van essentiële diensten (AED's) waarvoor wettelijk toezicht is opgenomen en anderzijds de groep andere vitale aanbieders waarvoor geen toezicht is opgenomen (dit zijn de voormalige Wgmc aanbieders). De Minister van BZK zal op basis van de huidige Wbni daarom niet geëquipeerd zijn om toezicht te houden op de sector digitale overheid. Dit komt omdat de Minister de sector digitale overheid niet als AED kan aanmerken. AED sectoren komen namelijk uit de Europese NIB-richtlijn, de sector digitale overheid is daar niet als AED opgenomen. Zonder de Wbni en het onderliggende besluit aan te passen is de minister van BZK alleen in staat om vitale aanbieders (niet zijnde AED's) in deze sector aan te wijzen. Hierdoor ontbreekt het wettelijk toezicht op basis van de Wbni.

Ga na of de Minister van BZK via de Wbni specifiek wettelijk toezicht wenst te verkrijgen op de toekomstige sector digitale overheid. Dit vergt overleg en afstemming met de andere departementen en een aanpassing van het wetsvoorstel.

8.4 Vormgeving horizontaal en verticaal toezicht

1. Varianten voor verantwoording en toezicht op informatieveiligheid, kunnen variëren van zelfregulering/horizontaal toezicht per bestuurslaag tot verticaal toezicht op de naleving van specifieke regelingen. In dit onderzoek is een viertal toezichtvarianten getoetst aan enkele uitgangspunten voor verantwoording en toezicht op informatieveiligheid. De toezichtvariant die horizontaal toezicht van het bestuursorgaan combineert met generiek toezicht door het rijk op de naleving van het gebruik van de generieke digitale infrastructuur scoort daarbij gemiddeld tot hoog op de genoemde uitgangspunten en met name op de gewenste transparantie in het naleven van de afspraken in de keten van de generieke digitale infrastructuur.

   Overweeg de variant die horizontaal toezicht van het bestuursorgaan combineert met generiek toezicht door het rijk als basis te nemen voor het de inrichting van het interbestuurlijk toezicht op informatieveiligheid.

2. Alle varianten van toezicht op informatieveiligheid gaan uit van een volwassenheidsniveau ('stip op de horizon') van de planning en control-cyclus op het gebied van informatieveiligheid waar veel bestuursorganen nog naar toe moeten groeien.

[11] Nota van toelichting op de Bbni: *"Vitale aanbieders binnen de sector digitale overheid (aanbieders van datasystemen waarvan meerdere overheidsorganisaties afhankelijk zijn) zullen naar verwachting bij de eerstvolgende wijziging van het Bbni aan artikel 3 worden toegevoegd."*

Bij de implementatie van een toezichtvariant dient rekening gehouden te worden met een minimaal volwassenheidsniveau bij de bestuursorganen.

Om het gewenste volwassenheidsniveau te bereiken zal naar verwachting een meerjarige interbestuurlijke programmatische inspanning noodzakelijk zijn. Hiervoor kan lering getrokken worden uit de Deense programmatische aanpak voor informatieveiligheid.

8.5 Kennisniveau en waarborgen/instrumenten

Op operationeel en tactisch niveau is een belangrijke sprong voorwaarts gemaakt binnen alle bestuurslagen en -organen om kennis en inzicht in technische en organisatorische informatieveiligheid te vergroten. De bestuurlijke aandacht voor informatieveiligheid blijft daarbij achter. Meerdere initiatieven zijn genomen om het bestuurlijk bewustzijn te vergroten. Als volgende stap in dit proces willen betrokkenen werken aan het 'bestuurlijk handelingsperspectief', zodat de bestuurder richting kan geven aan informatieveiligheid.

Zoek voor het versterken van het bestuurlijk handelingsperspectief op het gebied van informatieveiligheid naar een taal en naar instrumenten die aansluiten bij de praktijk van overheidsbestuurders, zoals collegiale visitatie, benchmarking, praktijkoefeningen en leren en groeien in volwassenheid. Een goed voorbeeld is het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten dat tweejaarlijks wordt uitgebracht door de VNG. Dit beeld geeft zicht op de belangrijkste bestuurlijke risico's en prioriteiten bij het vergroten van de digitale weerbaarheid van gemeenten.

A Bijlage: Bronnenlijst

Onderstaand een kort overzicht van de uitgangspunten van relevante documenten die een rol hebben gespeeld in dit onderzoek.

EINDRAPPORT TASKFORCE BID

De inzet van Taskforce BID was om de verplichtende zelfregulering gedurende de looptijd van de Taskforce BID tot stand te brengen door een iteratief proces van 'leren' en 'het verankeren' op het niveau van de organisatie en de overheidslaag, met als doel om een zichtbare en meetbare verandering te realiseren bij bestuur en topmanagement binnen de overheidslagen op het vlak van informatieveiligheidsbewustzijn en risicobewust handelen. In het eindrapport van Taskforce BID worden de aanpak, resultaten en bevindingen besproken van de daaraan voorafgaande jaren met betrekking tot de realisatie en verankering van verplichtende zelfregulering per overheidslaag.

WETSVOORSTEL DIGITALE OVERHEID

In het wetsvoorstel Digitale Overheid wordt de wettelijke basis gelegd voor de gehele basisinfrastructuur (GDI). Onderdeel hiervan zijn regels over informatieveiligheid en privacy. Het wetsvoorstel biedt daarmee de grondslag om overheidsinstanties te verplichten open standaarden te gebruiken. Ook toezicht en handhaving krijgt hiermee een wettelijke basis. Hiermee geven we invulling aan de één-overheids-gedachte, in het belang van de burger en ondernemer.

NL DIGIBETER: AGENDA DIGITALE OVERHEID

De Nederlandse Digitaliseringsstrategie, Nederland Digitaal, is een kabinetsbrede strategie over álles wat met digitalisering te maken heeft. De Agenda Digitale Overheid richt zich op de overheid en het contact met burgers en ondernemers. Deze Agenda Digitale Overheid is een agenda van alle overheden gezamenlijk en legt de verbinding met belangrijke publieke en private partners. Op basis van 5 "thema's" worden initiatieven genomen, kansen ontdekt en plannen gemaakt om de strategie concreet te maken.

KADERS VOOR TOEZICHT EN VERANTWOORDING

Dit rapport is een uitwerking van uitgangspunten, redeneerlijnen en handreikingen van de Algemene Rekenkamer als het gaat om toezicht en verantwoording. Het is een uitbreiding van eerder onderzoek van de Algemene Rekenkamer, maar met een verbreding in scope. De kaders voor toezicht en verantwoording die in dit rapport centraal staan zijn niet alleen bruikbaar vanuit het perspectief van de rwt's, maar zijn bruikbaar voor alle inastellingen op afstand van het rijk. Het rapport gaat onder andere in op de mix aan checks and balances, verticaal toezicht en verticale verantwoording, intern toezicht, meervoudige publieke verantwoording en de verschillende kwaliteitsinstrumenten.

HANDBOEK WET REVITALISERING GENERIEK TOEZICHT

Interbestuurlijk toezicht als instrument. Kenmerken van deze vorm van toezicht zijn nabijheid, enkelvoudigheid, samenwerking, selectiviteit en terughoudendheid, en proportionaliteit. Generieke instrumenten zijn indeplaatsstelling, schorsing en vernietiging,

TOEZICHT BIJ BZK, VERANTWOORDE UITVOERING

In dit document zijn de kaders opgenomen die in de komende jaren richting kunnen geven aan de dagelijkse contacten tussen het departement en de organisaties op afstand.

1. BZK werkt vanuit de ministeriële verantwoordelijkheid bij alles wat we doen. Het ministerie heeft bij organisaties op afstand de taakuitvoering (met eventuele bijbehorende bevoegdheden) aan de organisaties overgelaten en is die verantwoordelijkheid beperkter. Niettemin zorgen ook die organisaties ervoor dat de minister zich altijd kan verantwoorden over de uitvoering van hun taken.
2. BZK en de uitvoeringsorganisaties dragen zorg voor externe transparantie. Dit vraagt heldere taken, bevoegdheden en verantwoordelijkheden plus duidelijke interne en externe rapportagemomenten.
3. BZK richt toezicht in op basis van de volgende kenmerken opgenomen in de KVoT: risicogericht en selectief, slagvaardig, samenwerkend, onafhankelijk, transparant en professioneel.
4. BZK en de uitvoeringsorganisaties dienen het algemeen belang en de beleidsdoelstellingen van BZ Kin het bijzonder.
5. Alles wat BZK en de uitvoeringsorganisaties doen is rechtmatig en doelmatig. We zijn integer, sober en tonen voorbeeldgedrag.
6. BZK en de uitvoeringsorganisaties uniformeren waar het kan en individualiseren waar nodig.

DURVEN LEREN

Het rapport ‘Durven leren’ is het eindverslag visitatiecommissie Informatieveiligheid. Deze visitatiecommissie heeft in twee jaar met bestuurders en onder andere CISO’s van 120 gemeenten gesproken over informatieveiligheid en getracht een impuls te geven om het thema beter te verankeren op bestuurlijk, operationeel en tactisch niveau. De commissie heeft in haar rapport meerdere belangrijke boodschappen geformuleerd die het handelingsbewustzijn van bestuurders moet kunnen vergroten.

MAAK VERSCHIL

Dit rapport is het resultaat van de studiegroep Openbaar Bestuur, waarin commissie van Zwol heeft onderzocht of Nederland economische groei laat liggen omdat de inrichting en werkwijze van het openbaar bestuur niet optimaal georganiseerd is. In de analyse wordt onderscheid gemaakt tussen drie trends:

- Verschuiving belang naar regionaal niveau
- Meer adaptief vermogen van het bestuur noodzakelijk
- Verwevenheid belang tussen domeinen, tussen regionaal en internationaal niveau en tussen bestuurslagen

De aanbevelingen in het rapport richten zich op de versterking van het bestuurlijk vermogen in regionaal verband.

MAAK WAAR

Adviesrapport over de digitale transformatie van de overheid. Het gaat daarbij specifiek om 'de doorontwikkeling, de financiering en de governance van de generieke digitale voorzieningen' en 'de doorontwikkeling en de benodigde kennis en kunde voor het leveren van digitale overheidsdiensten voor burgers en bedrijven'. Fundament van het rapport is dat de digitalisering door alle overheidslagen heen gaat, er is één overheid, er is een interbestuurlijke verantwoordelijkheid en de GDI zijn bestempeld als vitale infrastructuur voor Nederland. "*In deze langere termijnvisie op de ontwikkeling van de digitale basisinfrastructuur is toezicht van groot publiek belang. Het is bij uitstek een overheidsverantwoordelijkheid om dat toezicht in te richten. Het lijkt voor de hand liggend dit toezicht meer integraal van karakter te laten zijn dan tot nu toe*[12]".

EN NU VERDER!

Dit rapport van de Raad van State is een periodieke beschouwing over interbestuurlijke verhoudingen na de decentralisaties in het sociale en fysieke domein. Dit rapport is gemaakt omdat er een verheveling heeft plaats gevonden van een substantieel aantal taken en verantwoordelijkheden van het rijk naar de medeoverheden, die aan de betekenis van hun onderlinge verhoudingen een nieuwe impuls gegeven. Thema's die hierbij aan de orde komen zijn regiovorming, stelselverantwoordelijkheid, democratische legitimatie van overheidsbeslissingen, rechtsbescherming en herijking van het toezicht.

DREIGINGSBEELD INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN 2019/2020

Het dreigingsbeeld is opgesteld door de IBD en biedt een handvat om informatiebeveiliging verder te verbeteren en daarmee de digitale weerbaarheid van een gemeente verhogen. Het geeft inzicht in de grootste bedreigingen en ontwikkelingen en adviseert over prioriteiten voor de komende jaren. De prioriteiten die de gemeenten conform dit onderzoek de komende jaren zouden moeten stellen zijn:

1. Zet informatiebeveiliging op de agenda van het college en zorg dat lintmanagers verantwoordelijkheid kunnen nemen. De top van de organisatie moet doordrongen zijn van het belang van informatiebeveiliging en een voorbeeldfunctie innemen.
2. Breng de basis op orde, want de basale beveiligingsprocessen en maatregelen zijn belangrijk om de digitale weerbaarheid van de gemeente te verhogen.
3. Versterk de menselijke schakel, want technologie alleen is niet de oplossing. Informatiebeveiliging begint bij de bewuste medewerker.
4. Versterk de positie van de CISO. Een CISO moet de ruimte en de middelen krijgen en investeren in kennis en kunde om de gemeente weerbaarder te maken tegen huidige en toekomstige digitale dreigingen.
5. Verbeter het inzicht in de risico's van nieuwe technologieën: Maak de juiste mensen verantwoordelijk voor deze ontwikkelingen en betrek vanaf het beginstadium de CISO en de verantwoordelijke lijnmanagers.

[12] Maak Waar, 2016, p.31

B Bijlage: Lijst geïnterviewden

Expertisegebied	Geïnterviewde(n)
Voorzitter van de VNG-commissie Dienstverlening en Informatiebeleid Lid college van Dienstverleningszaken	Franc Weerwind, Burgemeester Almere Frans Backhuijs, Burgemeester Nieuwegein
Vertegenwoordiging VNG	Nathan Ducastel Peter van Dijk
Programmamanager Informatiebeveiliging Waterschappen en bestuurder waterschap	Marianne Krug Piet Sennema
Programmamanager Informatiebeveiliging provincies	Arianne de Man
Autoriteit Telecom	Jasper Nagtegaal
Toezicht cybersecurity J&V	John Stienen
NCTV	Martine DeKoninck
BZK Wetgeving WDO	Barbera Veltkamp
Logius	Mark Janssen Jorik van ’t Hof
RvIG	Frans Venus David de Boer
BZK Toezicht BRP PUN	Aart Verloop
Bureau Forum Standaardisatie	Maarten van der Veen

Expertisegebied	Geïnterviewde(n)
	Ludwig Oberendorff
Rekenkamer Rotterdam	Rolf Willemse
NOREA	Wilfried Olthof Peter Verstege Winfried Nanninga Ronald van Langen

C Bijlage: Leden begeleidingscommissie BZK

Organisatie	Naam
Directie Informatiesamenleving en Overheid	Dirk Maats
Directie Constitutionele Zaken en Wetgeving	Barbara Veldkamp
Programma- en projectmanager toezicht BAG, BGT	Alex van de Ven
Directie Informatiesamenleving en Overheid	Meryem Çimen