Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Governance normenkader IBP FO

Definitief

Colofon

Titel	Governance Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs
Uitgebracht aan	De opdrachtgever, mr. drs. I.J. (Inge) Vossenaar MBA
Datum	11 april 2024
Kenmerk	2024-0000227132
Referentienummer	

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Centrale boodschap—5

1 Inleiding—10
1.1 Aanleiding onderzoek—10
1.2 Doelstelling en onderzoeksvragen—10
1.3 Afbakening—11
1.4 Leeswijzer—11

2 Context voor scholen in relatie tot governance inrichting op het Normenkader IBP voor het FO—12
2.1 Status Normenkader IBP voor het FO—12
2.2 Interne en externe governance inrichting IBP—12
2.2.1 Huidige stand implementatie interne Governance IBP bij scholen—13
2.3 Aandachtspunten van de scholen en andere stakeholders van het FO—14
2.3.1 Aandacht voor de 'basis op orde'—14
2.3.2 Aandacht voor kennis en ontwikkeling ICT en IBP—14
2.3.3 Verhogen (ICT-)organisatiegraad van het FO—14
2.3.4 Behoefte aan kostenoverzicht implementatie IBP voor het FO—15

3 Opties voor governance inrichting voor het Normenkader IBP voor het FO en bestaande governance inrichting bij het HO en de Zorg—16
3.1 Inrichting ontwikkeling en beheer governance IBP voor het FO—16
3.1.1 Ontwikkeling en beheer governance IBP voor het FO: input scholen—16
3.1.2 Ontwikkeling en beheer governance IBP voor het FO: input overige stakeholders—17
3.2 Inrichting toezicht en naleving governance IBP voor het FO—18
3.2.1 Toezicht en naleving governance IBP voor het FO: input scholen—19
3.2.2 Toezicht en naleving governance IBP voor het FO: input overige stakeholders—19
3.3 Inrichting beheer en ontwikkeling governance IBP bij het HO en bij de Zorg—22
3.3.1 Beheer en ontwikkeling governance IBP bij het HO—22
3.3.2 Beheer en ontwikkeling governance IBP bij de Zorg—23
3.4 Inrichting toezicht en naleving governance IBP bij het HO en bij de Zorg—24
3.4.1 Toezicht en naleving governance IBP bij het HO—24
3.4.2 Toezicht en naleving governance IBP bij de Zorg—25

4 Keuzemogelijkheden inrichting IBP voor het FO—26
4.1 Keuzemogelijkheid 1. Governance inrichting zoals bij het Hoger Onderwijs—26
4.2 Keuzemogelijkheid 2. Governance inrichting zoals bij de Zorg—29
4.3 Keuzemogelijkheid 3. Ontzorgen door Maatwerk—31
4.4 Keuzemogelijkheid 4. Ontzorgen door Centrale aanpak—32
4.5 Keuzemogelijkheid 5. Toezichthoudende rol binnen Governance inrichting—33
4.6 Keuzemogelijkheid 6. Normenkader IBP voor het FO omzetten in Wetgeving—35

5 Verantwoording onderzoek—37
5.1 Werkzaamheden en afbakening—37
5.2 Gehanteerde standaard en kwaliteitsborging—37
5.3 Verspreiding rapport—38

6 Ondertekening—39

Managementreactie—40

Bijlage (1) Wat is Governance?—42

Bijlage (2) Nadere informatie Nulmeting—44

Bijlage (3) Interne Governance bij FO—46

Bijlage (4) Geïnterviewde stakeholders—50

Bijlage (5) Overeenkomsten en verschillen tussen de Zorg, het HO en het FO—53

Bijlage (6) Visiebrief Minister OCW aan Tweede Kamer—54

Centrale boodschap

In het kader van de informatiebeveiliging op scholen heeft OCW het Normenkader Informatiebeveiliging en Privacy (IBP) voor het Funderend Onderwijs (FO)[1] ontwikkeld. Scholen moeten dit kader implementeren en er in 2027 aan voldoen. De governance[2] op het Normenkader moet nog worden ingericht. Wij zijn gevraagd om in beeld te brengen welke rollen daarbij nodig zijn en hoe de rolinvulling eruit zou kunnen zien volgens verschillende stakeholders, rekening houdend met de doelen van het Normenkader IBP[3].

De centrale onderzoeksvraag van dit inventariserend onderzoek luidt:
Welke keuzemogelijkheden zijn er voor de inrichting van de governance van het Normenkader en welke opties liggen er vervolgens voor welke partijen voor de rolinvulling die past bij de inrichting van de governance?

De mogelijke rollen, rolverdeling en keuzemogelijkheden zijn gebaseerd op een inventarisatie van suggesties bij zestien stakeholders[4], waaronder drie scholen. Ook hebben wij gekeken naar de governance inrichting op vergelijkbare Normenkaders IB bij het Hoger Onderwijs (HO) en bij de Zorg en de voor- en nadelen[5] volgens stakeholders geïnventariseerd.

Wij geven in dit onderzoek geen richting of advies over de uiteindelijk te kiezen rollen en rolinvulling: die keuze is aan de opdrachtgever OCW. Wij raden OCW aan om de stakeholders mee te nemen zodat de uitkomsten van dit onderzoek in gezamenlijkheid kunnen worden vertaald naar beleid. Dit mede in het kader van het creëren van draagvlak en betrokkenheid.

Opties voor rollen en rolinvulling zoals onderscheiden door de stakeholders

Deelvraag 1 richt zich op een mogelijke rolindeling/rolinvulling voor de governance inrichting in het FO zoals gesuggereerd door de stakeholders. Een nadere onderbouwing hiervan is te vinden in 3.1 en 3.2.

FUNDEREND ONDERWIJS	
ROLLEN	**ROLINVULLING**
Input scholen	
1. Beheerder	NEN, Edu-standaard, PO-en VO-Raad, SIVON en Kennisnet
2. Faciliterende rollen -Intermediairsrol -Katalysatorrol 3. Meldpunt 4. Helpdesk	 SIVON, Kennisnet SIVON, Kennisnet en ook de Leveranciers/ Technologie aanbieders CERT i.o.
5. Toetser -Zelfregulering 6. Externe toetsing Accreditatie, Auditing, Visitatie 7. Externe Toezichthouder	SIVON/Kennisnet Scholen Schoolbestuur primair verantwoordelijk Onafhankelijke bureaus: niet de accountant Niet de IvhO (tenzij thema-onderzoek)
Input Overige stakeholders	
1. Uitvoerder	Scholen
2. Eigenaar	OCW, (mede-eigenaar: PO en VO-raad)
3. Beheerder/Ontwikkelaar	Kennisnet (met expertise), SIVON
4. Leverancier informatie aan rol 3.	Scholen, PO en VO-Raad, Netwerk IBP en IvhO en AP (AVG-gerelateerd)

[1] Funderend Onderwijs bestaat uit het Primair Onderwijs en het Voortgezet Onderwijs.
[2] Zie Bijlage 1.
[3] Het normenkader heeft als doel om schoolbesturen te verduidelijken wat de minimale set aan eisen is op het gebied van IBP, bij te dragen aan bewustwording op scholen en schoolbesturen te stimuleren om te benchmarken en te verbeteren.
[4] Zie Bijlage 4.
[5] Voor- en nadelen kunnen ook worden gelezen als 'voor- en tegenargumenten'.

5. Adviseur voor PO en VO Raad	Adviesgroep Regie op ICT
6. Relatiemanager	PO en VO Raad en Kennisnet
7. Facilitator 8. Helpdesk voor scholen	SIVON
9. Meldpunt 10. Toetser: -Monitoring/Advisering -Self-assessments -Certificering -Deep dives -Productontwikkeling 11. Externe toetsing 12. Externe Toezichthouder	CERT i.o. Diensten via Kennisnet en PO en VO-Raad Scholen (eventueel aangevuld met toezicht) In te regelen dienst via SIVON en Edu-V SIVON Kennisnet en SIVON Accountant onder voorwaarden, met voor- en tegenstanders en optie alternatieve aanpak IvhO onder voorwaarden, met voor- en tegenstanders en optie alternatieve aanpak AP is bestaande toezichthouder (AVG)

Keuzemogelijkheden gerelateerd aan de governance inrichting bij het HO en de Zorg

In het HO en de Zorg is ervaring opgedaan met de governance op een Normenkader IB, daarom hebben we gekeken naar hoe deze sectoren de governance hebben ingericht en welke voor- en nadelen betrokken stakeholders daarbij zien. (Deelvraag 2 en 3). Parallelle opties voor het FO hebben wij aangegeven. Nadere uitwerking is te vinden in 3.3, 3.4, 4.1 en 4.2

1. Governance inrichting zoals bij het Hoger Onderwijs

Het HO werkt met het Normenkader IB Hoger Onderwijs 2015, het betreft een sectorale afspraak, alle HO-instellingen moeten aan de normen voldoen. Er zijn geen formele afspraken over de governance op het Normenkader. SURF vervult bij de governance op het Normenkader IB voor het HO diverse rollen, er is sprake van een gecentraliseerde aanpak. Dit ligt voor het FO lastiger omdat de organisatiegraad daar lager is. OCW ontwikkelt een plan om de organisatiegraad van het FO te verhogen.

De governance inrichting voor het HO kent de volgende rollen en rolinvulling:
Eigenaar is het HO. Het HO is snel overgegaan tot verplichting van het Normenkader, dit kwam vanuit de sector zelf en het HO werkt vanuit de community-gedachte met uitgangspunten van gedeeld eigenaarschap. Relevant is dat het FO voldoende kennis en kunde over ICT/IBP verkrijgt om optioneel volwaardig eigenaarschap te kunnen invullen.

Ontwikkelaar is het HO. Kennisnet heeft voor het FO momenteel de rol om dienstverlening te ontwikkelen en te beheren. Het FO zou volgens ons met Kennisnet (en wellicht SIVON, Edu-V, CERT i.o.) kunnen optrekken om ontwikkeling van het Normenkader vorm te geven. Via het IBP-Netwerk bestaat een soortgelijke situatie. Voor *Innovatie* zou FO volgens ons aansluiting kunnen zoeken bij SURF gezien het volwassenheidsniveau bij het FO. Leden van de IBP-netwerken, de Regiegroep ICT en FG's en CISO's met eventueel een vertegenwoordiging van Kennisnet, SIVON, Edu-V en CERT i.o. kunnen hier een rol in hebben.

Beheerder, Facilitator en CERT zijn rollen van SURF. Het *beheer* van het Normenkader IB is bij SURF belegd bij een maturity-werkgroep binnen SURFibo. SURF beschikt over experts, daardoor hoeven HO-instellingen niet zelf het wiel uit te vinden. Bij het FO zijn experts binnen verschillende organisaties vertegenwoordigd. Het FO kan aansluiting zoeken bij de Maturity-werkgroep en de stuurgroep van het HO om te leren zelf gremia in te richten dan wel te komen tot een samenwerkingsverband FO – HO of anderszins het beheer van het Normenkader voor het FO te beleggen. Voor het FO kan gedacht worden aan leden van IBP-netwerken, de Regiegroep ICT en FG's en CISO's. Een CIO-beraad, ICT-directeuren en IT-

managers zoals bij het HO zijn bij het FO vaak niet aanwezig. SURF huisvest het Platform Integrale Veiligheid HO voor de thema's Privacy, Cybersecurity en het Normenkader IB HO. Overwogen kan worden of SIVON, Kennisnet (met CERT i.o.) en Edu-V gezamenlijk voor het FO een vergelijkbaar platform kunnen inrichten. SURF faciliteert diensten voor de uitvoering van audits, in het kader van contract-management en leveranciers compliancy. Bij het FO kunnen audits via SIVON/ Kennisnet worden ingeregeld en de andere twee diensten zouden tussen SIVON, Kennisnet (met CERT i.o.) en Edu-V kunnen worden opgepakt met gebruikmaking van de leerpunten van SURF. SURF geeft interne toezichthouders bij HO-instellingen cursussen over IB. SURF werkt met *SURFcert*. Voor het FO is er CERT i.o. (bij Kennisnet).

Intern toezicht bij HO-instellingen: over de auditfrequentie en -aanpak zijn per sector tussen de koepels en OCW, afspraken gemaakt. Resultaten van audits sturen HO-instellingen naar SURF die vervolgens een 'cyber-dreigingsbeeld' opstelt.
Bij HO-instellingen komt Cybersecurity voor in jaarverslagen, dit is niet verplicht voorgeschreven in het accountantsprotocol. HO-instellingen werken vaak met grotere accountantskantoren waar de accountant vraagt naar IB.

Extern toezicht bij HO-Instellingen: er is geen externe toezichthouder voor het Normenkader IB HO, er wordt gewerkt met zelfregulering. De IvhO verricht geen vierjaarlijkse kwaliteitsonderzoeken in het HO (bekostigd of onbekostigd), dit doet de Nederlands-Vlaamse Accreditatieorganisatie (NVAO), IB is daarbij geen thema.

SURF ziet aan een governance inrichting als bij het HO voor- en nadelen:

Voordelen

- Doordat er experts verbonden zijn aan SURF, hoeven HO-instellingen niet ieder het wiel zelf uit te vinden.
- SURF krijgt steeds meer inzicht in de situatie en de kwetsbaarheden bij de sector.
- Contactpersonen van de SURF-leden wisselen onderling kennis en ervaringen uit.
- Het HO heeft zichzelf ontwikkeld op het gebied van IBP, kan impact van wijzigingen inschatten en voert wijzigingen (na pilots etc.) beheerst door.
- Het lerend vermogen is bij het HO goed ontwikkeld en er wordt gewerkt met best practices.

Nadelen

- Niet-bekostigde HO-en MBO-instellingen maken geen onderdeel uit van SURF. Hun informatiepositie is een andere: zij zijn momenteel niet aange-sloten op landelijke dreigingsinformatie via de CERTS of informatiepunten.

2. Governance inrichting zoals bij de Zorg

Binnen de Zorg is werken volgens de NEN 7510 wettelijk verplicht gesteld. Er zijn geen formele afspraken over de governance op het Normenkader Zorg.
De governance inrichting voor de Zorg kent de volgende rollen en rolinvulling:
Eigenaar van het Normenkader NEN 7510 is de Zorg. De overheid heeft hierin een beperkte rol, het is aan instellingen zelf om dit te regelen. Opties voor het FO zijn vergelijkbaar met die zijn genoemd bij het HO voor de rol van eigenaar.

Beheerder is NEN[6].NEN beheert de normen en stelt ze vast. NEN nodigt belanghebbenden uit deel te nemen. Afspraken komen op basis van consensus tot stand.

[6] NEN staat voor Nederlandse Norm EN voor Europese Norm. Het betrokken Nederlands Normalisatie-Instituut (NEN), valt onder verantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat. (Stichting Koninklijk Nederlands Normalisatie Instituut).

De bezetting met betrokken functionarissen van het FO zou overeenkomen met die zoals beschreven bij de rol van beheerder bij het HO. Ook bij een keuze voor NEN als beheerder zal sprake moeten zijn van voldoende kennis en capaciteit van IT/IBP bij verschillende gremia in het FO om deze rol goed invulling te geven. Experts zijn in het FO aanwezig bij Kennisnet, SIVON, CERT i.o. en Edu-V. Hun rol bij de invulling van de rol van beheerder NEN zou nader afgewogen moeten worden.

Ontwikkelaar is de Zorg zelf. De Zorg is medeontwikkelaar van de normen. Actualisatie vindt iedere vijf jaar plaats. NEN nodigt de werkgroep met stakeholders uit, die aangeeft wat er in de praktijk is gewijzigd m.b.t. IB/ISO-normen. Het FO zou met vertegenwoordiging van Kennisnet (en wellicht SIVON, Edu-V, CERT i.o, de Regiegroep ICT en IBP-netwerken) als stakeholder kunnen optrekken voor de ontwikkeling van het NEN-Normenkader. VWS meldt dat het Nationaal Instituut ICT in de Zorg (NICTIZ) vergelijkbaar is met Kennisnet binnen het onderwijsveld en dat VWS, NICTIZ een publieke rol wil gaan geven (bouwen van een bibliotheek met verschillende informatie-standaarden).

Facilitator is VWS. De stelseleigenaar (VWS) heeft een faciliterende rol en ontvangt signalen over IB in de Zorg via Z-CERT, NEN, de Inspectie Gezondheidszorg en Jeugd (IGJ) en de Zorg, creëert meer bewustwording bij partijen en beoogt naleving makkelijker te maken. Bij het HO heeft SURF de rol van facilitator. OCW zou kunnen overwegen zelf deze rol in te vullen.
Z-CERT vervult de rol in de Zorg. Het FO kent CERT i.o.

Intern toezicht bij de Zorg: een (C)ISO helpt organisaties om aan de normen te voldoen. Zelfevaluaties kunnen mogelijk worden aangeboden met Z-CERT of ICTU, de verantwoordelijkheid ligt bij besturen zelf. Zorgaanbieders moeten verplicht en aantoonbaar voldoen aan de NEN; de wet zegt echter niet *hoe* dit moet worden aangetoond maar dit kan b.v. via een certificaat of middels een audit.

Extern toezicht bij de Zorg: de Inspectie Gezondheidszorg en Jeugd (IGJ) werkt met toetsingskader 'E-Health', met daarin eisen op basis van NEN 7510.

VWS ziet aan een governance inrichting als bij de Zorg voor- en nadelen:

Voordelen

- NEN is beheerder van het Normenkader en zorgt voor verbinding van partijen in de werkgroep.
- Er worden afspraken gemaakt waar je, indien nodig, aan kunt refereren.
- Er is sprake van een autonoom aanpassingsproces.

Nadelen

- Het NEN-proces kost tijd.
- VWS heeft als één van de partijen beperkte mogelijkheden om op inhoud van de normen te sturen. Als de norm zou gaan afwijken van de wensen van VWS, moet VWS de wet aanpassen.

Keuzemogelijkheden op basis van dit onderzoek en de ontwikkelkoers OCW

Dit onderzoek geeft mede inzicht in de volwassenheid van de scholen op het gebied van de interne governance, en op het gebied van begrip en de kennis van de materie uit het Normenkader IBP (zie Bijlagen 2 en 3). Scholen zijn nog niet altijd in staat om het Normenkader zelfstandig toe te passen. We hebben de uit dit onderzoek verkregen informatie gehouden tegen de Visiebrief van 6 juli 2023 van de Minister van OCW aan de Tweede Kamer (zie Bijlage 6) om deze aan te laten sluiten op de gewenste ontwikkelkoers van OCW.
Meer informatie over deze keuzemogelijkheden is te vinden in 4.3 tot en met 4.6.

3. Ontzorgen door maatwerk

Stakeholders benoemen rollen voor de governance inrichting waaruit blijkt dat (extra) hulp nodig is. Scholen kennen ieder hun eigen 'vertrekpunt' en eigen hulpvraag voor het zetten van een volgende ontwikkelstap om te (gaan) voldoen aan het Normenkader. 'Hulp op maat' is nodig met respect voor de autonomie van scholen en om in hun specifieke behoefte te voorzien. Met de inzet van Kennisnet (en IBP-netwerk) en SIVON zou dit kunnen volgens scholen. Nu scholen het Normenkader al enige tijd in volle omvang kennen (april 2023) lijkt het ons goed om de specifieke behoefte aan maatwerk/expliciete hulpvraag bij scholen te inventariseren.

4. Ontzorgen door centrale aanpak

Inventarisatie van de specifieke behoefte bij scholen kan ook leiden tot de overweging tot een (gedeeltelijke) Centrale aanpak. Stakeholders noemen diverse argumenten en thema's die pleiten voor een centrale aanpak zoals een gezamenlijk gebruik van dezelfde IT-informatiestructuur, IT-systemen en leveranciers.

5. Toezichthoudende rol binnen governance inrichting

In 2027 vindt er Toezicht en Handhaving plaats en scholen zijn vanaf het jaarverslag over 2024 verplicht om aandacht te besteden aan IBP. Extern toezicht is nu nog niet ingeregeld en verantwoording over IBP gebeurt willekeurig. Intern toezicht (FG, CISO en RvT)[7] en extern toezicht (accountant, IvhO, AP)[8] vraagt om een zekere wederzijdse balans en onder meer tools om het toezicht vorm te geven. Als de basis op orde is, intern toezicht bij het FO een meer volwassen vorm heeft, kan effectief extern toezicht plaatsvinden. Daarnaast zien we samenhang met het nog te completeren Normenkader zelf en het verder ontwikkelen van kennis bij optionele betrokkenen en de beschikbaarheid van voldoende capaciteit bij die betrokkenen.

6. Normenkader IBP voor het FO omzetten in wetgeving

In de huidige situatie is er geen sprake van wetgeving: het Normenkader IBP is nog niet compleet, het is een levend document. Ontwikkelingen ten aanzien van ICT/IBP (AI gerelateerde kwesties met ChatGPT), wetgeving (NIS2)[9] en verbeteringen die scholen aanreiken op basis van ervaringen in de praktijk, kunnen aanleiding geven tot verdere aanpassing van het kader. Een stakeholder spreekt in dit kader van een groeimodel: als partijen nog niet zover zijn, is het verplichten van het hoogste niveau niet reëel en na een groeiperiode kan worden overwogen om het Normenkader meer juridisch te maken. Wetgeving maakt (extern) toezicht mogelijk door bijvoorbeeld de accountant als toetser aan te wijzen en de IvhO als toezichthoudend orgaan. Beiden zien opties voor toezicht nu wetgeving nog niet aan de orde is.

[7] Functionaris Gegevensbescherming (FG), Chief Information Security Officer (CISO), Raad van Toezicht (RvT).
[8] Inspectie van het Onderwijs (IvhO), Autoriteit Persoonsgegevens (AP).
[9] In een tijd van groeiende digitale afhankelijkheid en toenemende cyberdreigingen heeft de Europese Unie de **N**etwork and **I**nformation **S**ecurity Directive herzien, resulterend in NIS2. Deze richtlijn, van kracht sinds januari 2023, versterkt de digitale weerbaarheid van de lidstaten. Organisaties moeten zich voorbereiden op de eisen die in januari 2025 van kracht worden.

1 Inleiding

Het ministerie van OCW heeft samen met SIVON, Kennisnet, de PO Raad (voor Primair Onderwijs) en de VO Raad (voor Voortgezet Onderwijs) het Programmaplan Digitaal Veilig Onderwijs (DVO) opgesteld (versie 1.0 maart 2023). Dit kent naast strategische doelen en programmalijnen tevens operationele doelen die meetbaar zijn en in een Normenkader Informatiebeveiliging en Privacy (IBP) voor het Funderend Onderwijs (FO)[10] staan. De governance op het Normenkader moet nog ingericht worden (zie Bijlage 1).

1.1 Aanleiding onderzoek

De digitalisering in het onderwijs houdt – naast veel voordelen – het risico in dat scholen doelwit kunnen worden van cyberaanvallen[11]. Het gevolg van dit soort aanvallen is dat IT-systemen niet meer benaderbaar zijn waardoor de continuïteit van het onderwijs in gevaar komt, of gevoelige gegevens van leerlingen op straat komen te liggen. Specifiek voor kinderen geldt dat zij volgens de Algemene verordening gegevensbescherming (AVG) en het Verdrag inzake de rechten van het kind recht hebben op specifieke bescherming[12]. De minister van Onderwijs wil daarom de digitale veiligheid in het primair en het voortgezet onderwijs verhogen. Hij investeert daartoe €6 miljoen in het programma Digitaal Veilig Funderend Onderwijs (DVFO)[13]. Eén van de speerpunten van het programma DVFO is het ontwikkelen van een Normenkader IBP in het primair en voortgezet onderwijs.
De stichting Kennisnet ontwikkelt het Normenkader. Het kader is bijna gereed. Het Normenkader heeft als doel om voor schoolbesturen te verduidelijken wat de minimale set aan eisen is op het gebied van IBP, bij te dragen aan bewustwording op scholen en schoolbesturen te stimuleren om te benchmarken en te verbeteren[14]. Om deze doelen te kunnen verwezenlijken, is meer nodig dan sec het Normenkader. Minimaal moet er een eigenaar van het kader zijn, een partij die het kader actueel houdt en ontwikkelt en een toezichthouder voor de naleving van het Normenkader. Kortom, de *governance* van het Normenkader moet ingericht worden.

1.2 Doelstelling en onderzoeksvragen

De directeur-generaal Primair en Voortgezet Onderwijs heeft de Auditdienst Rijk (ADR) gevraagd om te inventariseren welke rollen er nodig zijn voor de governance rondom het Normenkader IBP en welke partijen deze rollen zouden kunnen invullen om het Normenkader IBP passend in te kunnen richten. Passend wil zeggen dat de governance bijdraagt aan de doelen van het Normenkader IBP volgens het ministerie van OCW[15].

De hoofdvraag die voortkomt uit de doelstelling van het onderzoek luidt:

[10] Het primair en voortgezet onderwijs worden gezamenlijk geduid als Funderend Onderwijs
[11] Zie bijvoorbeeld op: Cyberaanvallen op onderwijsinstellingen sterk gestegen (kpn.com)
[12] Zie kamerbrief: digitalisering-in-het-funderend-onderwijs.pdf (overheid.nl)
4 Zie kamerbrief: verhogen-digitale-veiligheid-onderwijs-en-onderzoek.pdf (overheid.nl)
[14] Bron: *Nadere offerteaanvraag ten behoeve van Onderzoek naar Governance IBP Normenkader FO.* Ministerie van OCW, 2022
[15] Met een Normenkader wordt volgens het ministerie van OCW beoogd om voor schoolbesturen te verduidelijken wat de minimale set aan eisen is op het gebied van IBP, bij te dragen aan bewustwording op scholen, en schoolbesturen te stimuleren om te benchmarken en te verbeteren.

Welke keuzemogelijkheden zijn er voor de inrichting van de governance van het Normenkader en welke opties liggen er vervolgens voor welke partijen voor de rolinvulling die past bij de inrichting van de governance?

De hoofdvraag wordt beantwoord in de vorm van mogelijke keuzes en bestaat uit de volgende deelvragen:

1. Welke suggesties, belangen en randvoorwaarden onderkennen stakeholders in het FO bij de rolindeling en -invulling voor de governance?

2. Welke governance-inrichting bestaat er in de Zorg en het Hoger Onderwijs op normenkaders voor IBP en welke organisaties vullen deze rollen in?

3. Waarom is in de Zorg en het Hoger Onderwijs voor de huidige governance-inrichting gekozen en welke voor- en nadelen zijn daaraan verbonden?

De opdrachtgever, mr. drs. I.J. (Inge) Vossenaar MBA, is eigenaar van de rapportage. De doelstelling van het onderzoek en de onderzoeksvragen zijn met de opdrachtgever afgestemd en vastgelegd in een getekende opdrachtbevestiging van 29 maart 2023 (2023-0000087059).

1.3 Afbakening

Het onderzoek bestaat uit een inventarisatie van de inrichting van de governance op een Normenkader IBP voor het FO. Daarbij is gekeken naar de sectoren Hoger Onderwijs (HO) en de Zorg. Deze twee sectoren zijn gekozen door de opdrachtgever, omdat daar al sprake is van een ingericht systeem van governance op een vergelijkbaar Normenkader. De sectoren hebben bovendien raakvlakken met het veld van het FO. Beide sectoren zijn net als het FO decentraal georganiseerd met veel kleine, zelfstandige organisaties die aan een centraal opgelegde norm moeten voldoen. Het betrokken ministerie heeft hierdoor een minder directe lijn met deze organisaties.

Het onderzoek heeft verschillende keuzemogelijkheden opgeleverd met voor- en nadelen, maar het geeft geen richting of advies over de uiteindelijk te kiezen rollen en rolverdeling van de governance. Deze afweging is aan de opdrachtgever.

1.4 Leeswijzer

Hoofdstuk 2 geeft de huidige context voor het FO in relatie tot de in te richten externe governance IBP voor het FO. Hoofdstuk 3 biedt inzicht in de potentiële inrichting van governance IBP voor het FO (deelvraag 1) en de feitelijke inrichting bij het HO en in de Zorg (deelvragen 2 en 3). Hoofdstuk 4 geeft op basis van de onderzoek informatie zes keuzemogelijkheden en vermeldt daarbij ook de voor- en nadelen (voor- en tegenargumenten) als antwoord op deelvraag 3.

Dit is een inventariserend onderzoek. De inhoud is vormgegeven door inbreng van betrokken stakeholders bij het onderzoek (zie Bijlage 4). Daar waar de ADR zelf bevindingen weergeeft omschrijven we dit door gebruik van ‘wij’ en ‘ons’.

2 Context voor scholen in relatie tot governance inrichting op het Normenkader IBP voor het FO

In dit hoofdstuk schetsen we de huidige context voor de scholen in relatie tot de in te richten externe governance op het Normenkader IBP voor het FO.

2.1 Status Normenkader IBP voor het FO

De scholen dienen het Normenkader te implementeren. Dit Normenkader is 19 april 2023 gepubliceerd en kent nog een aantal elementen die in ontwikkeling zijn:

- Normen voor Privacy: in de onderwijssector bestaat nog geen leidend kader voor privacy-normen, publicatie volgt naar verwachting in het eerste kwartaal 2024.
- Ondersteunende documentatie (zoals format en handreikingen) is deels nog in ontwikkeling.
- Het Groeipad: dit beschrijft op welk moment aan welke normen moet worden voldaan en welke veranderingen in de schoolorganisatie op welk moment moeten worden doorgevoerd, want niet alles hoeft in één keer. Tijdens ons onderzoek is er nog geen realistisch groeipad voor het FO. De vormgeving ervan is evenmin helder bij de scholen.

Het Normenkader bevat een Toetsingskader bij elke norm, dat het minimumniveau beschrijft waar de sector naar toe wil werken. Voor alle normen is het advies van experts om volwassenheidsniveau 3 van het NBA-model te hanteren.
Het Normenkader is, als aangegeven, een levend document dat steeds is gebaseerd op de nieuwste kennis en ontwikkelingen waarbij ook suggesties van scholen worden gevraagd.

Stakeholders (zie Bijlage 4) onderkennen dat het voor schoolbesturen een flinke klus is om aan het Normenkader te voldoen voor eind 2027. Specifiek voor kleine schoolbesturen lijken de niveaus en maatregelen soms ver van de praktijk te staan. De vraag is of het voor alle scholen realistisch is. De PO- en VO-Raad vraagt zich af hoe zij in die ontwikkeling kunnen helpen. Bewustwording, draagvlak en urgentie-besef spelen volgens stakeholders een rol. Ook wordt weerstand tegen het Normen-kader ervaren, die volgens een stakeholder voornamelijk ten grondslag ligt aan het gebrek aan mensen en middelen. De scholen die we hebben gesproken vinden het Normenkader overwegend goed en hebben tegelijkertijd nog vragen, behoefte aan (veel) hulp, kennen tekorten en ervaren onduidelijkheden bij de toepassing ervan in hun praktijk. Aandacht moet volgens stakeholders vooral gaan naar de z.g. ‘eenpitters’: de kleinere scholen, waar geschetste tekorten het grootst zijn, zie 2.3.

2.2 Interne en externe governance inrichting IBP

Het Normenkader heeft als doel schoolbesturen te verduidelijken wat de minimale set aan eisen is op het gebied van IBP, bij te dragen aan bewustwording op scholen èn schoolbesturen te stimuleren om te benchmarken en te verbeteren.
Deze doelstelling veronderstelt volgens ons onder meer begrip van het Normen-kader zelf bij de scholen, kennis van IBP/ICT en daarmee een zekere volwassenheid van de organisatie om uitvoering te kunnen geven aan het Normenkader. Dit maakt volgens ons duidelijk, dat governance op twee niveaus wenselijk is om de effectiviteit van het Normenkader IBP optimaal te faciliteren:

- Interne Governance: binnen de school om de eisen uit het Normenkader te kunnen inregelen, uitvoeren, te toetsen en te verbeteren.
- Externe Governance: op veldniveau om het Normenkader zelf actueel en relevant te houden, naleving te faciliteren en te toetsen.

Bij ontwikkeling van externe governance is een zeker evenwicht met de ontwikkeling van de interne governance aan de orde evenals het meebewegen van betrokken partijen. Wij geven eerst een beeld van de interne governance bij drie scholen.

2.2.1 Huidige stand implementatie interne Governance IBP bij scholen

Bij de publicatie van het Normenkader (april 2023) is aangegeven dat zolang het groeipad nog niet bestaat, schoolbesturen kunnen beginnen met het nemen van maatregelen voor 'de basis op orde' met referentie aan de normen 1.1 (Strategie en Visie op Informatie- en Cybersecurity) en 1.2. ((Informatie-) beveiligingsbeleid). Tegelijkertijd staat op pag. 94 van het Normenkader een andere duiding van 'de basis op orde'. Daar worden naast bovenstaande normen 1.1, 1.2 de volgende normen en thema's genoemd:

Norm	Thema
2.1	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid
6.1	Incidentmanagement
6.2	Incident-escalatie
6.4	Problem management
7.1	Change management
7.2	Impact assessment, prioriteren en autoriseren
7.3	Noodwijzigingen
9.1	Data- en systeemeigenaarschap
9.2	Classificatie
9.3	Beveiligingseisen voor datamanagement
12.1	Fysieke beveiligingsmaatregelen
14.1	Bedrijfscontinuïteitsplanning
14.5	Crisismanagement

November 2023 is een nieuwe set basismaatregelen geïntroduceerd, op basis van de adviezen voor het MKB van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)[16].

Uit een Nulmeting (zie Bijlage 2) blijkt - uit een steekproef van 15 schoolbesturen - dat geen enkel schoolbestuur aan het gewenste volwassenheidsniveau 3 voldoet voor de getoetste onderdelen uit het Normenkader[17]. Het rapport onderscheidt vier archetypes voor de scholen: alleen Koplopers (~10%) beschikken over beleid en praktijk. Overige scholen beschikken of alleen over beleid, of alleen over praktijk of kennen noch beleid noch praktijk.
Wij hebben in het kader van dit onderzoek met drie scholen gesproken: een grote school (21.000 leerlingen) een middelgrote school (4.500 leerlingen) en een kleine school (520 leerlingen). Wij hebben hierdoor onder meer een beeld gekregen van de interne governance op IBP bij deze scholen, die elementen uit norm 2.1 kent (zie Bijlage 3). Deze situatie kan volgens ons, aanleiding geven om de externe governance op het Normenkader IBP bijvoorbeeld via een groeimodel vorm te geven en/of rollen benodigd voor de externe governance gedurende een periode intensiever in te zetten om zodoende mee te bewegen met de ontwikkelingen in het FO. Bij de keuzemogelijkheden in hoofdstuk 4 komen we hierop terug.

[16] Het gaat om De 11 basismaatregelen om je informatiebeveiliging te verhogen (kennisnet.nl)
[17] Nulmeting IBP-Normenkader voor het Funderend Onderwijs door Dialogic juni 2022/2023 (?)

2.3 Aandachtspunten van de scholen en andere stakeholders van het FO

2.3.1 Aandacht voor de 'basis op orde'

Ons is duidelijk dat scholen tijd, geld, kennis, capaciteit (specifieke IT-expertise), ondersteuning, rust en ruimte nodig hebben om de eisen van het Normenkader IBP te kunnen implementeren, deze na te leven en om te kunnen groeien in kennis en volwassenheid. Scholen ervaren op die thema's overwegend tekorten. Het zijn meerjarige projecten en werving binnen de ICT-markt is lastig. Volgens een school kent het FO zo'n 800-900 kleine instellingen die geen ruimte hebben om specialisten in huis te halen.
De doelstelling van het Normenkader veronderstelt bij de scholen volgens ons, begrip van de inhoud van het Normenkader zelf. Kennis van IBP/ICT is nodig om de verantwoordelijkheid van de implementatie van het Normenkader te kunnen nemen en dragen: het vormgeven aan de sturing, inrichting, uitvoering en het (intern) toezicht op het Normenkader IBP door de scholen.

2.3.2 Aandacht voor kennis en ontwikkeling ICT en IBP

Stakeholders vragen aandacht voor het kennisniveau voor ICT en IBP bij de scholen en geven aan dat bij het schoolbestuur (RvB) het kennisniveau vaak onder de maat is. Volgens hen komt dit mede door gebrek aan een bedrijfskundige achtergrond. RvB leden hebben veelal een achtergrond in het onderwijs. De toezichthouders (RvT) kennen voor het thema IBP/ICT overwegend geen portefeuillehouder, risico's voor IBP worden soms ingeschat op basis van perceptie en het opleidingsaanbod voor toezichthouders geeft geen informatie over IBP. Interne toezichthouders op scholen, zoals de RvT, dienen zich bewust te zijn van IBP, urgentie te voelen over het thema en hierover voldoende kennis te hebben om bestuurders de juiste kritische vragen te kunnen stellen en ze verder te helpen. Scholen zouden geholpen moeten worden met goede interne tegenspraak. VTOI-NVTK vertegenwoordigt interne toezichthouders uit de kinderopvang en het onderwijs. Volgens ons zou OCW zich met VTOI-NVTK kunnen richten op verbetering.

Leraren krijgen in hun opleiding volgens de scholen geen informatie over bewustwording en kennis gericht op ICT/IBP. De minister van OCW schrijft in zijn brief van 06 juli 2023 (hierna: 'de Visiebrief' en zie Bijlage 6) dat hij werkt aan een kader voor de digitale en didactische vaardigheden van leraren: de generieke kennisbases worden herijkt[18]. De nadruk ligt op implementatie van belangrijke maatschappelijke thema's, waaronder digitale geletterdheid. Kennis over digitale geletterdheid, het gebruik van digitale leermiddelen en de digitale vaardigheid van de leerkracht zelf komen hier aan bod. In het studiejaar 2025-2026 zullen de herijkte kennisbases naar verwachting in werking treden. Ook is belangrijk, dat er meer aandacht en passend aanbod komt voor de bij- en nascholing van leraren op het gebied van digitale geletterdheid. Leraren zullen beter opgeleid worden in hun bekwaamheid in dit vakgebied, aldus de Visiebrief. Wij merken op dat niet expliciet is gemaakt of kennis over IBP hierin specifiek een plaats krijgt.

2.3.3 Verhogen (ICT-)organisatiegraad van het FO

Bij de huidige organisatie IBP voor het FO, geven stakeholders het volgende aan: een hogere organisatiegraad is nodig om het naleven van de eisen van het Normenkader IBP überhaupt mogelijk te maken en meer awareness en urgentiegevoel te creëren.

[18] Visiebrief Digitalisering in het funderend onderwijs van de minister van OCW aan de Tweede Kamer op 6 juli 2023.

SIVON is de ICT-coöperatie van en voor het FO en beschikt medio 2023 over 34 medewerkers. De organisatiegraad van het FO is momenteel beperkt op IBP-gebied, kijkend naar het lidmaatschap van SIVON. 70% van de besturen van VO-scholen zijn lid van SIVON, 23% van de besturen van PO-scholen zijn lid van SIVON. Omdat niet alle scholen in het FO lid zijn van SIVON is een combinatie van de vijf partijen (de PO- en VO-Raad, Kennisnet, SIVON en OCW) nodig om iedereen te bereiken. Met name Kennisnet en SIVON hebben veel technische kennis binnen het FO, zij worden echter niet altijd gevonden door het FO, in ieder geval niet zo goed als dat SURF wordt gevonden door het HO. SURF ontwikkelt ICT-dienstverlening voor (Hoger) Onderwijs en Onderzoek en beschikt in 2022 over 386 medewerkers. Ter vergelijking: in het Hoger Onderwijs (HO) zijn alle bekostigde hogescholen, universiteiten en MBO-instellingen lid van SURF.

De Regiegroep ICT bestaat uit 7-8 bestuurders uit het FO en houdt zich bezig met onder meer de verantwoordelijkheid voor ICT van een schoolbestuur en hoe daar invulling aan te geven. De Regiegroep ICT adviseert bij de activiteiten van de PO-Raad en de VO-Raad.

Het Netwerk IBP wordt beheerd door Kennisnet met mensen die zich op school bezighouden met (het Normenkader) IBP. Hierop zijn niet alle scholen aangesloten. Momenteel telt het Netwerk IBP 867 leden die onder 465 schoolbesturen vallen (van de in totaliteit ongeveer 1.200 besturen). Ook bij de PO-Raad en VO-Raad kun je stellen dat de organisatiegraad in het FO beter kan:

- Bij PO-Raad is 89% van de schoolbesturen van een PO-instelling lid.
- Bij VO-Raad is 98% van de schoolbesturen van een VO-instelling lid.

Ter vergelijking: in het HO zijn alle bekostigde Hogescholen en Universiteiten aangesloten bij de Vereniging van Hogescholen en Universiteiten Nederland.
In eerste instantie lijkt stelseleigenaar OCW aan zet om ervoor te zorgen dat onderwijsinstellingen zich zoveel mogelijk aansluiten bij SIVON, netwerk IBP en de PO- en VO-raad. In zijn Visiebrief schrijft de minister dat hij het waardeert dat steeds meer schoolbesturen de meerwaarde zien, zich solidair tonen en hun verantwoordelijkheid nemen door lid te zijn van SIVON. De Kamer heeft de minister verzocht om een plan te maken zodat zoveel mogelijk schoolbesturen aansluiten bij SIVON. OCW is met SIVON en de sector in gesprek over een stabiele en krachtige positie van SIVON. Voor de zomer van 2024 wordt de Kamer verder geïnformeerd.

2.3.4 Behoefte aan kostenoverzicht implementatie IBP voor het FO

Scholen geven aan behoefte te hebben aan beter inzicht in kosten die implementatie met zich meebrengt. Volgens hen zou een Project-/Implementatieplan hierbij kunnen helpen. Een school geeft aan dat in diens situatie ongeveer twee miljoen euro nodig is om in twee jaar tijd op volwassenheidsniveau 3 te komen: middelen komen uit het eigen vermogen. Jaarlijkse exploitatiekosten stijgen ook. De school veronderstelt dat het voor een kleinere school om eenzelfde soort bedrag gaat en vindt dat de basis-bekostiging niet gebaseerd is op dit soort IT-ontwikkelingen. Bij het voortgezet onderwijs (VO) is 150 of 200 euro per leerling voor ICT gereserveerd. Een school geeft aan dat het bekostigingsstelsel anders ingericht moet worden.[19] Een heel klein deel van de lumpsum is momenteel gereserveerd voor ICT: inhuur is dan geen optie[20].

[19] Een onderbouwing van door scholen genoemde bedragen in 2.3.4 hebben wij niet gevraagd of ontvangen. Bedragen zijn dus niet door ons geverifieerd: dat valt buiten de scope van dit onderzoek.
[20] Elke school krijgt een vast bedrag per leerling. Hiervan betaalt de school personeel, materialen, en onderhoud van het schoolgebouw. Eén keer per jaar wordt dit bedrag in zijn geheel uitgekeerd aan het schoolbestuur. Dit bedrag heet de lumpsum. De school beslist vervolgens hoe het geld wordt verdeeld. Bron: https://oudersenonderwijs.nl/kennisbank/schooloverkoepelend/bekostiging/lumpsum/

3 Opties voor governance inrichting voor het Normenkader IBP voor het FO en bestaande governance inrichting bij het HO en de Zorg

In dit hoofdstuk gaan wij in op de mogelijkheden voor een rolindeling en rolinvulling ten aanzien van de governance op het Normenkader IBP. Wij zijn hiertoe gekomen door het voeren van zestien gesprekken met stakeholders uit het FO waaronder drie scholen (zie Bijlage 4).

Paragraaf 3.1 gaat in op de suggesties, belangen en randvoorwaarden die door stakeholders in het FO worden onderkend bij de rolinvulling voor de governance IBP gericht op ontwikkeling en beheer. Paragraaf 3.2 gaat in op de suggesties, belangen en randvoorwaarden die door stakeholders in het FO worden onderkend bij de rolinvulling voor de governance IBP gericht op toezicht en naleving. Hierbij wordt gerefereerd aan ontwikkelingen die hierop van invloed zijn. Paragraaf 3.3 biedt inzicht in de governance inrichting in het HO en de Zorg op Normenkaders voor IBP en de organisaties die deze rollen invullen. Ook hier is de indeling ontwikkeling en beheer enerzijds en toezicht en naleving anderzijds gehanteerd.

3.1 Inrichting ontwikkeling en beheer governance IBP voor het FO

In deze paragraaf gaan wij dieper in op de rollen en invulling ervan als aangegeven door scholen en overige stakeholders op het gebied van ontwikkeling en beheer rond het Normenkader governance IBP voor het FO. Samen met paragraaf 3.2 geven wij hiermee antwoord op deelvraag 1.

3.1.1 Ontwikkeling en beheer governance IBP voor het FO: input scholen

Uit ons onderzoek blijkt dat scholen behoefte hebben aan faciliterende, ondersteunende rollen bij het inrichten van de IT- en informatiestructuur.
Rollen die in dit verband genoemd worden zijn een *intermediairsrol,* om voor hen de vertaalslag te maken tussen het Normenkader en de situatie van de school en een *katalysator-rol* om ook echt stappen te kunnen zetten. Voor een verdere invulling van deze rollen wordt gedacht aan SIVON, Kennisnet en ook de Leveranciers/ Technologie aanbieders als het gaat om de katalyserende rol.

Een (technisch) beheerdersrol vraagt om specialisten en zou onafhankelijk moeten worden belegd, waarbij gedacht wordt aan NEN of Edu-standaard[21]. Beheer van een Normenkader is iets anders dan het ondersteunen bij implementatie en het ontwikkelen van advisering aan scholen, daarom wordt door een stakeholder opgemerkt om de taak niet bij Kennisnet of SIVON te beleggen.
Anderen noemen de PO-en VO-Raad, SIVON en Kennisnet voor het vervullen van de rol van beheerder. Kennisnet wordt door stakeholders gezien als het meest visie- en toekomstgericht.

[21] Edu-Standaard is de Standaardisatieraad voor het onderwijsdomein, die scholen ontzorgt met standaarden voor informatie-uitwisseling tussen onderwijsinstellingen, DUO, OCW en leveranciers. Edu-Standaard is aangesloten op de Informatiekamer van OCW en in die zin afgestemd op de wet- en regelgeving van de overheid. NEN staat voor Nederlandse Norm EN voor Europese Norm. Het betrokken Nederlands Normalisatie-Instituut (NEN), valt onder verantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat.

Daarnaast kan gedacht worden aan een meldpunt of helpdesk bij (dreigende) cyberincidenten, een cybercentre zoals bijvoorbeeld CERT.

3.1.2 Ontwikkeling en beheer governance IBP voor het FO: input overige stakeholders

Andere stakeholders dan scholen benoemen expliciet de rol van uitvoerder voor scholen. SIVON en Kennisnet zouden een hulpstructuur kunnen bieden.

OCW krijgt de rol van eigenaar (Stelselverantwoordelijke, Vaststellend gremium, Regieverantwoordelijke en Penvoerder) aan wie taken zoals het bepalen van het niveau waaraan moet worden voldaan, het vaststellen van het Normenkader en het bepalen of het kader blijft of wettelijk voorschrift wordt, zijn toebedeeld.
Een nieuwe versie van het Normenkader wordt idealiter niet in de Algemene Ledenvergadering van de Raden vastgesteld vanwege de vereiste (technische) expertise en het risico op vertraging in het proces. De voorkeur gaat uit naar een organisatie waarin schoolbesturen onderdeel zijn van de governance voor de vaststelling van het Normenkader. Eigenaarschap vanuit de sector zou draagvlak voor het Normenkader kunnen creëren.
Een stakeholder waarschuwt voor het belang van schoolbesturen om de norm niet te hoog te stellen en stelt zich de vraag wie er bij het vaststellen wel zal gaan pleiten voor een hoog niveau. Een andere stakeholder vindt het relevant dat scholen weten waar ze wel en geen invloed op hebben: scholen zijn aan zet voor het toetsen op bruikbaarheid en uitvoerbaarheid en niet voor de inhoud op de normen en het minimumniveau. Maar er is ook een stakeholder die aangeeft dat de PO- en VO-Raad mede-eigenaar zou moeten zijn, om vanuit ervaringen bij de scholen het kader te kunnen bijstellen en vanwege inspraak gezien de vrijheid van onderwijs. Ook een rol als adviseur naar de PO- en VO-Raad is genoemd. De Adviesgroep Regie op ICT heeft reeds veel draagvlak en zou deze rol daarom op zich kunnen nemen.

De rol van Relatiemanager wordt onderkend bij het verkrijgen van draagvlak in het FO met de vijf partijen (Kennisnet, OCW, PO- en VO-raad en SIVON) en het informeren van bestuurders. De PO en VO-Raden communiceren naar de achterban en zorgen voor draagvlak. Relatiemanagers van Kennisnet informeren de bestuurders.

Kennisnet zou een rol als Beheerder en Ontwikkelaar kunnen vervullen waarbij externe experts kunnen worden geraadpleegd. Kennisnet heeft echter zeggenschap van schoolbesturen niet in het organisatiemodel opgenomen. SIVON heeft dit als vereniging wel en zou ook een rol als Beheerder en Ontwikkelaar in kunnen vullen. Nog niet alle schoolbesturen zijn lid.

Naast rollen als Beheerder en Ontwikkelaar, wordt ook gedacht aan rollen ter ondersteuning ervan zoals bijvoorbeeld Leverancier (van informatie) en Adviseur. Scholen leveren input voor de ontwikkeling van het Normenkader en worden geholpen door PO- en VO-Raad, Kennisnet en SIVON. Kennisnet begeleidt het proces met een werkgroep van scholen uit het Netwerk IBP. Scholen hebben vraagstukken en agenderen deze in het Netwerk, deelnemers zelf hebben de regie. Het changeproces kan op soortgelijke wijze verlopen: wijzigingen worden besproken met de doelgroep, Sectorraden en SIVON. Ter vaststelling gaan uitkomsten met advies naar OCW. Bij het verzamelen en doorgeven van signalen (vanuit de doelgroep en vanuit leveranciersmanagement) voor de doorontwikkeling van het kader ziet SIVON voor zichzelf een rol weggelegd. Scholen zouden bruikbaarheid en uitvoerbaarheid moeten kunnen toetsen. De Inspectie van het Onderwijs (IvhO) kan uit de praktijk een signaalfunctie hebben en suggesties doen. Als aandachtspunt meldt een stakeholder, dat eenduidigheid van communicatie en mediagebruik bij de informatie-uitwisseling over beheer en ontwikkeling nodig is.

Daarnaast is nog de rol van Facilitator genoemd, voor het bieden van hulp bij de praktische toepassing van het Normenkader. Zo hebben de scholen allemaal een eigen vertrekpunt en dus behoefte aan ondersteuning die daarbij aansluit. Zoals een bron het formuleerde: *'De eerste stap is in deze fase de faciliterende kant, de kenniskant ter ondersteuning van de implementatie. Het is voor veel mensen al een 'eng' gebied'.* De rol van Facilitator wordt ook benoemd bij het voorzien in disciplines voor intern tweedelijns toezicht zoals een FG en een CISO. SIVON kent de faciliteit CISO-as-a-service voor de scholen en heeft in het verleden invulling gegeven aan de FG-as-a-service faciliteit.

Een landelijke Helpdesk biedt ondersteuning en expertise aan scholen en leveranciers. Ook Kennisnet heeft expertise nodig voor vragen over toepassing van het Normenkader. (Sleutel-)partijen moeten in positie worden gebracht voor ondersteuning bij informatiebeveiliging, daar waar scholen te klein zijn om het zelf te regelen. SIVON wil scholen centraal stellen en hen een hulpstructuur bieden om te voorzien in hun behoeften voor doorontwikkeling en ziet voor zichzelf daarbij een ondersteunende rol. Het gemeenschappelijk gebruik van de diensten van financieel functionarissen, ondersteuningsaanbod etc. vanuit het Programma DVFO kan decentraal nog verder invulling krijgen. Een stakeholder noemt een commercieel adviesbureau: een organisatie die alle organisaties in het onderwijs wil ondersteunen (advies en onderzoek) bij Privacy en Informatiebeveiligingsvraagstukken.

De inhoud van de normen en het minimumniveau zou door experts beoordeeld moeten worden. De Autoriteit Persoonsgegevens (AP) ziet voor zichzelf een adviserende rol bij het opstellen/bijstellen van guidance en/of Normenkaders en de vraag of het Normenkader eventueel geschikt is voor een AVG-gedragscode (en bij indiening: goedkeuring daarvan). De adviesrol richt zich voornamelijk op de inhoudelijke kennis van de AP.

Tenslotte wordt het verplicht melden van een hack/cyberincident of een acute dreiging (zoals de situatie rond log4J[22], eind 2021) bij een meldpunt genoemd. Bij voorkeur bij een organisatie waar scholen worden geholpen met het oplossen en afhandelen van een dergelijk incident. Als voorlichtingsmateriaal kan informatie worden gedeeld met de sector. Besturen kunnen dan nagaan of zij zelf ook kwetsbaar zijn en eventueel tijdig maatregelen nemen. CERT wordt vanuit Kennisnet vormgegeven en ziet het als een van zijn taken om het eerste aanspreekpunt te zijn en een coördinerende rol te hebben bij een gemelde kwetsbaarheid op school. Daarnaast wordt via CISO-netwerken al veel informatie uitgewisseld en wordt wederzijds hulpverleend.

Het werken met Ethical Hackers wordt voorgesteld. Universiteiten werken hier al mee. Het implementeren van een 'responsible disclosure' is wellicht een optie.[23]

3.2 Inrichting toezicht en naleving governance IBP voor het FO

In deze paragraaf volgt nadere beantwoording van deelvraag één in aanvulling op de informatie in paragraaf 3.1. We schetsen eerst een aantal ontwikkelingen die op toezicht en naleving van invloed zijn.

In de Visiebrief meldt de Minister dat er in 2027 Toezicht en Handhaving zal plaatsvinden en dat scholen vanaf het jaarverslag over 2024 verplicht zijn aandacht te besteden aan IBP.

[22] Log4J staat voor Log for Java en is de benaming van een logboekprogramma dat gebruikt wordt in Java-applicaties. Het registreert input van gebruikers en is aanwezig in een groot aantal webapplicaties. In een aantal versie is het mogelijk voor kwaadwillenden om codes toe te voegen aan Log4J en dit geeft de mogelijkheid om onder andere aanvallen op te zetten op schoolnetwerken of bij andere educatieve dienstverleners.
[23] De vinder van een kwetsbaarheid stelt eerst de eigenaar van het kwetsbare systeem op een verantwoorde manier op de hoogte voorafgaand aan het publiekelijk delen.

Eerder in 2023 stond op de website van de PO-Raad het volgende:

*Vanaf schooljaar **2023-2024** wordt het voor schoolbesturen verplicht om in hun jaarverslag aandacht te besteden aan informatiebeveiliging en privacy (IBP).*[24]

Volgens de NBA is hierbij een formeel proces van toepassing:
Vanuit het Verslaggevingskader - de Regeling Jaarverantwoording Onderwijs (RJO) – dient de wijziging te worden gecommuniceerd en daarna kan dit in het Onderwijs accountantsprotocol (OAP) een plaats krijgen: de verplichting voor IBP in het jaarverslag moet daarin worden opgenomen.

De huidige inrichting van intern toezicht en toetsing bij de scholen ziet er als volgt uit: de grote en middelgrote school die we hebben gesproken beschikken over IBP-ers, een Functionaris voor de Gegevensbescherming (FG) en een Privacy Officer (PO). De kleine school spreekt over een 'ICT-clubje van leerkrachten'. Functie- en Rollenscheiding zijn vaak aandachtspunten (zie Bijlage 3). De grote school voert self-assessments uit, de andere twee scholen werken nog niet met self-assessments.
Alleen bij de grote school kijkt de accountant naar IBP, bij de andere twee scholen is dit niet het geval. Een externe toezichthouder is (nog) niet van toepassing.

Volgens VTOI-NVTK zou de RvT een eigen Toezicht visie, met een Toetsingskader en bijbehorende criteria moeten hebben. Dit is echter nog lang niet bij iedere RvT het geval. VTOI-NVTK wil dat IBP daarin een vast thema wordt en draagt dit ook uit.

3.2.1 Toezicht en naleving governance IBP voor het FO: input scholen

De scholen hebben behoefte aan een toetsende rol waarbij zelfregulering wordt genoemd, een jaarlijkse toets door SIVON of Kennisnet of audits in de vorm van accreditatie, auditing of visitatie door onafhankelijke bureaus. Deze rol willen scholen bij voorkeur niet bij de accountant beleggen omdat het niet tot de kern van de accountantsrol behoort volgens de scholen en het tot hogere kosten gaat leiden. Zelfregulering is in deze fase passend omdat scholen nog niet voldoende volwassen zijn op het gebied van IBP. Het lerende aspect is belangrijk en kan beter gefaciliteerd worden in het zelfreinigend vermogen van de sector zelf. "Je moet 'je eigen blinde vlekken' blijven zien": onafhankelijke bureaus/auditors worden als criticasters door schoolbesturen ingeschakeld. De rol van Toezichthouder wordt door de scholen in verband gebracht met de IvhO, tegelijkertijd geven zij niet de voorkeur aan de IvhO als toezichthouder omdat scholen menen dat het niet behoort tot de kerntaak van de IvhO, die de wet controleert (het Normenkader is niet in wet omgezet). Op het gebied van themaonderzoek zijn wellicht mogelijkheden voor de IvhO volgens de scholen. Op het gebied van Toezicht en Handhaving is volgens scholen het schoolbestuur zelf verantwoordelijk en daardoor aanspreekbaar op IBP. Als het thema IBP in het jaarverslag komt, worden maatregelen voor het bestuur zichtbaar b.v. bij school- of organisatie specifieke punten uit het kader. De IvhO kan vervolgens controleren op uitvoering daarvan onder het thema '(digitale) veiligheid'.

3.2.2 Toezicht en naleving governance IBP voor het FO: input overige stakeholders

Interne toetsing wordt aan de hand van diverse methodes gesuggereerd, zoals Monitoring en Advisering, Zelfregulering en Certificering. De dienst Monitoring en Advisering bieden Kennisnet met de PO- en VO-Raad samen aan, aan de scholen om elkaar scherp te houden.
Zelfregulering komt naar voren als goede rolinvulling als het wordt ondersteund en gestimuleerd door toezicht. De sector kan zichzelf reguleren en toetsen door het

[24] https://www.poraad.nl/schoolontwikkeling/digitalisering/structureel-6-miljoen-voor-digitale-veiligheid-in-het-funderend

uitvoeren van monitoring/benchmarking, self-assessments en onafhankelijke audits (in lijn met de werkwijze bij het MBO en het HO/WO). Self-assessments kunnen ook helpen meer zicht te krijgen op naleving van IBP. Inzicht in waar de school nu staat en hoe de school door kan groeien, kan verkregen worden door de uitvoering van 'deep dives'[25] die SIVON uitvoert. Kennisnet en SIVON ontwikkelen producten en diensten.
Instellen van 'Certificering' is een optie wanneer ICT van scholen is uitbesteed aan leveranciers. Edu-V helpt scholen met een certificaat. Auditing helpt. Als SIVON de certificeringseis van leveranciers meeneemt in de aanbestedingseisen, dan vallen leveranciers buiten de boot als ze er niet aan voldoen.
Bij Certificering noemt een stakeholder als aandachtspunt: *"in het kader van goed leveranciersmanagement (Norm 15.1) is het certificeringsschema ROSA essentieel voor het behalen van de doelen van het Normenkader en is het belangrijk om vervolgens de governance rond dit schema te verbinden aan het Normenkader".*

Volgens een stakeholder zijn er eisen gesteld aan wat een RvT minimaal moet vermelden in het jaarverslag van de RvT maar zijn er geen eisen gesteld aan hoe uitgebreid het zou moeten zijn of welke kwaliteit het jaarverslag zou moeten hebben. ICT/IBP is nog geen verplicht onderdeel in dit jaarverslag. Daarnaast wordt aandacht gevraagd voor een Educatie Rol voor het ontwikkelen van IT/IBP-kennis voor onder meer leden van de RvT's. Hiertoe volgen suggesties:
-Een handleiding IBP door SIVON en Kennisnet.
-VTOI/NVTK kent training in digitalisering voor RvT's en zou hen kunnen ondersteunen met een handleiding of beeldmateriaal over het Normenkader.
-Tools voor RvT's voor het stellen van kritische vragen aan de RvB over IBP en ook voor het specifiek en separaat opnemen van IBP in hun toezichtvisie.
-Webinars organiseren voor meer bewustwording bij de RvT's en de scholen.

De rol van de Accountant als Toetser kan pas invulling krijgen na aanpassing van de Regeling Jaarverantwoording Onderwijs en van het Onderwijs Accountantsprotocol (OAP) door opname van het Normenkader.
De accountant kijkt nu niet naar IBP. In de huidige situatie worden echter door de accountant wel opties voor werkzaamheden van de accountant gegeven:
- kijk naar IBP vanuit de thema's 'Continuïteit' en de 'Risicoanalyse', of
- benader IBP op dezelfde wijze als de accountant kijkt naar 'Duurzaamheid' vanuit het OAP[26].
- mogelijk kan de accountant ook van betekenis zijn als het thema IBP net als b.v. Integriteit wordt opgenomen in de Governance Codes van de scholen. Er zijn ontwikkelingen gaande voor aanpassing van de Corporate Governance Code.
-de accountant zou een toets op aanwezigheid van het thema in het bestuurverslag kunnen doen: controle op juistheid van die informatie verricht de accountant niet.
Als niets expliciet wordt geregeld voor IBP is het een generiek risico. De accountant kijkt dan alleen naar de risicoanalyse en maatregelen (impliciete werkzaamheden).
Over de potentiële rol van de accountant, wordt door overige stakeholders het volgende genoemd*:*
-het accountantsprotocol is geen goed medium, het richt zich op het jaarverslag, de financiën etc. Opnemen van het thema IBP zou kunnen tenderen naar 'geen goedkeurende verklaring'. Bovendien: een thema benoemen in het jaarverslag om de goedkeurende verklaring te krijgen en er inhoudelijk weinig tot niets mee doen is niet wenselijk.
- het ligt niet voor de hand om de accountant eigen onderzoek te laten doen wegens hoge kosten, benodigde capaciteit en specifieke expertise voor het Normenkader.

Naast de rol van Toetser is ook de rol van Toezichthouder verkend.

[25] Deep dive js een methode waarbij een persoon of team een intense, diepgaande analyse uitvoert van een bepaald probleem of onderwerp.
[26] Duurzaamheid en accountancy (nba.nl)

De IvhO kijkt nu niet naar IBP omdat het Normenkader niet in de wet is verankerd. Stakeholders spreken over een toezichthoudende rol voor de IvhO vergelijkbaar met die van de Inspectie Gezondheidszorg en Jeugd (IGJ): het woord van een Inspectie heeft gewicht. Als je het kader langdurig wilt hanteren en bijvoorbeeld door de IvhO wilt laten handhaven, dan zou je dat meer moeten formaliseren.
VWS stelt dat IGJ toe zag op IB vanuit de kwaliteit van zorg waardoor IGJ alleen handhavend kon optreden als de kwaliteit van zorg in gevaar was. Dit is nu niet meer voldoende; VWS expliciteert dat momenteel in de wet.

Diepgaande gesprekken over IT/IBP kunnen de meeste inspecteurs bij IvhO nog niet voeren, maar IvhO ontwikkelt hiervoor een groeipad voor de komende jaren. De IvhO ziet opties voor het uitvoeren van IBP-werkzaamheden gegeven de huidige situatie, zoals:
-Kijken naar IBP vanuit de thema's 'Continuïteit van het onderwijs'. Mogelijk geldt hetzelfde voor de 'Deugdelijkheidseis'.
-Kijken naar het systeem van 'Risicobeheersing'. De IvhO kijkt iedere vier jaar naar risicobeheersing en bekijkt hoe de IvhO besturen kan wijzen op het belang van deze risico's via gesprekken of in de jaarverslagen.
-Kijken naar IBP vanuit het thema 'De Code Goed Bestuur'. De IvhO toetst of scholen zich aan deze code houden en als zij hier (deels) niet aan voldoen, moeten zij dit in het jaarverslag melden.
-Kijken naar IBP vanuit de Verantwoording; hierbij kan de IvhO kijken naar b.v. uitgevoerde self-assessments en collegiale visitaties.
-Besturen erop aanspreken of ze (indien vereist) 'Certificering' op orde hebben.
-IvhO kan erop toezien dat scholen zich verantwoorden over IBP en hen eventueel een herstelopdracht geven.
-IBP maakt nu geen deel uit van het toezichtkader van IvhO, daar zou het wel in opgenomen kunnen worden. Een nieuwe toezicht structuur zou moeilijk zijn voor de scholen.
-De IvhO heeft een wettelijke basis nodig om de toezicht functie te kunnen vervullen en zou de RvT's moeten aanspreken op het onderwerp digitalisering: hoe gaat de RvT hiermee om en hoe weet de RvT dat dit goed gaat?

Andere stakeholders dan de IvhO melden bij de suggestie voor Toezicht door IvhO:
-Het Normenkader IBP biedt 'guidance' wat 'hard toezicht' niet noodzakelijk maakt.
-Het huidige inspectiekader biedt al aanknopingspunten om met schoolbesturen in gesprek te gaan of onderzoek te doen op basis van incidenten, vanwege de verantwoordelijkheid voor continuïteit van het onderwijs en financiële verantwoording. Verantwoordelijkheden zouden aangrijpingspunt moeten zijn, in plaats van digitalisering an sich.
-Als de IvhO extra bevoegdheden krijgt, is het de vraag welke invloed dat heeft op het huidige systeem van toezicht met interne en externe toezichthouders.
-Voorkeur is om aan te sluiten bij de huidige structuur voor toezicht: intern gaat dit om de RvT en de FG, extern wordt verantwoording afgelegd aan de IvhO. De Autoriteit Persoonsgegevens (AP) houdt toezicht op basis van de AVG.
-De IvhO is niet de geschikte partij om te handhaven op het thema IBP: het is voor hen erg specifiek en staat ver af van de kern van hun taak (kwaliteit onderwijs).
-Toezichthouden is niet gewenst door een externe specifiek op IBP gerichte partij.

De AP kan op eigen initiatief onderzoek doen in het onderwijsveld, maar moet keuzes maken wegens beperkte capaciteit en veel signalen, meldingen en klachten. Een datalek of bijvoorbeeld een bericht in de media kan voor de AP, aanleiding vormen voor onderzoek en bezoek aan scholen.

Het Normenkader IBP staat wat de AP betreft naast de AVG. De AP heeft verkend of het Normenkader kan worden ondergebracht in een AVG-gedragscode: daarvoor lijkt het niet geschikt. De AP en de IvhO kennen een Samenwerkingsconvenant wat

zich richt op het hoe te handelen daar waar overlap ligt in het toezicht en het uitwisselen van signalen en persoonsgegevens voor het toezicht. De IvhO geeft signalen aan de AP om deze te verkennen. Uitwisseling van kennis/informatie over cybersecurity is nog niet geregeld. Regulier overleg tussen de AP en de IvhO is gericht op cyber security en op signalen/klachten die de IvhO ontvangt met betrekking tot privacy.

De rol van Handhaver is ook genoemd, waarbij enerzijds het argument is genoemd dat handhaving als 'stimulerend' moet worden ervaren omdat er al genoeg regels zijn, anderzijds is het argument dat er duidelijkheid moet komen over wie scholen gaat aanspreken als ze niet voldoen aan het Normenkader en wie hen controleert. Edu-V zou een rol kunnen gaan spelen in het kader van het Privacy convenant dat samen met leveranciers is opgesteld. Edu-V geeft zelf aan dat toezicht op naleving van het Privacy-convenant nog niet is ingeregeld.

3.3 Inrichting beheer en ontwikkeling governance IBP bij het HO en bij de Zorg

Deze paragaaf biedt inzicht in de huidige governance inrichting bij het Hoger Onderwijs (HO) en bij de Zorg op Normenkaders voor IBP gericht op beheer en ontwikkeling en de organisaties die deze rollen invullen. In deze paragraaf wordt antwoord gegeven op de deelvragen twee en drie van het onderzoek. Binnen 4.1 en 4.2 worden de voor- en nadelen (voor-/tegenargumenten) genoemd (gericht op deelvraag 3) en de parallelle situatie voor het FO geschetst.

Bijlage 5 biedt inzicht in overeenkomsten en verschillen tussen de Zorg, het HO en het FO met betrekking tot de governance rollen en rolinvulling.

3.3.1 Beheer en ontwikkeling governance IBP bij het HO

Stakeholders hebben hierover het volgende weergegeven:
Het HO werkt met het Normenkader Informatiebeveiliging Hoger Onderwijs 2015 gebaseerd op het informatiebeveiligingskader van de NBA en NOREA (niveau 3). Het is een sectorale afspraak: alle HO-instellingen moeten aan de normen voldoen. Formele afspraken over de governance op het Normenkader HO zijn er niet, maar er zijn sectorale plannen (WO, HBO, MBO) waarvan het Normenkader de basis is.

Het HO-veld bepaalt als eigenaar en ontwikkelaar de inhoud van het Normenkader IBP, gefaciliteerd door SURF[27]. Elke instelling die lid is van SURF heeft een vertegen-woordiger bij SURF, aangesteld door het bestuur van de betrokken instelling. Werken vanuit de community-gedachte en principes van gedeeld eigenaarschap zijn relevant. Groepen van contactpersonen uit het HO werken aan ontwikkeling vanuit thema's integrale veiligheid en onderwijskwaliteit. SURF werkt samen met leden aan de verhoging van de kwaliteit van onderwijs en onderzoek door ICT-innovatie in negen innovatiezones, waaronder Cyberveiligheid. Regievoering op de innovatie-zone gebeurt door CISO's, IT-directeuren van de instellingen en andere IBP-experts.

SURF vervult voor het HO de volgende rollen: Facilitator, Beheerder en CERT[28]

SURF als Facilitator:
-SURF huisvest een Platform, waar Privacy, Cybersecurity en het Normenkader IB HO, thema's zijn en HO instellingen samenwerken aan het verbeteren van de integrale veiligheid in het HO. Betrokkenen zijn: het FG-overleg, het CISO-overleg en de SURFcommunity voor IBP (SCIPR).

[27] Het HO veld omvat WO-, HBO- en MBO-instellingen (in dit geval, die zijn aangesloten bij SURF).
[28] CERT wordt ook wel digitale brandweer genoemd. CERT staat voor Computer Emergency Response Team.

-SURFaudit is een dienst die SURF aanbiedt: hiermee kunnen instellingen een self-assessment doen, of een audit laten doen (SURF verricht zelf geen audits). Daarnaast biedt SURF benchmarks aan en een cyberdreigingsbeeld.
-Contractmanagement: SURF is ISO-gecertificeerd, wil dit ook bij de eigen leveranciers terugzien en stelt IBP-eisen aan de leverancier bij Europese aanbestedingen.
-Leveranciers compliancy: de Innovatiezone van SURF ontwikkelt een leveranciers-compliancy-dienstverlening: alle leveranciers moeten gaan voldoen aan IBP-eisen.
-SURF ondersteunt instellingen bij het uitvoeren van DPIA's en DTIA's, eventueel met aanvullende externe juridische expertise[29]. Bevindingen pakken instellingen op met de leveranciers.
-SURF coördineert onderzoek naar de impact van Europese wet- en regelgeving zoals NIS2 op Onderzoek en Onderwijs in samenwerking met de koepels en OCW.

SURF als Beheerder kent een interne governance inrichting met beheer van het Normenkader IB bij de maturity-werkgroep binnen SURFibo. De stuurgroep daarvan bewaakt evaluatie en herziening, na behandeling in de stuurgroep gaat het naar het CIO-beraad, de ICT-directeuren van de universiteiten en de groep van IT-managers van HO-instellingen voor accordering.

CERT is SURFcert.

3.3.2 Beheer en ontwikkeling governance IBP bij de Zorg

Stakeholders hebben hierover het volgende weergegeven:
Voor Zorginstellingen geldt sinds 2008 een Normenkader voor informatiebeveiliging: de NEN 7510[30]. De Zorg heeft het initiatief genomen om deze norm te ontwikkelen en in 2008 is werken volgens de NEN 7510 wettelijk verplicht gesteld.
Formele afspraken zijn niet gemaakt over de governance op het Normenkader Zorg, wel zijn er (onderliggende) afspraken.

De Zorg vervult de rol van eigenaar van het Normenkader IBP Zorg en de rol van (mede-)ontwikkelaar ervan[31]. De Zorg heeft initiatief genomen voor de normen en daarmee is een grotere kans op implementatie door betrokkenheid en eigenaarschap. Draagvlak voor de normen en consensus over afspraken zijn relevant.

Actualisatie van de normen vindt iedere vijf jaar plaats of zo nodig eerder. NEN schakelt de werkgroep met stakeholders uit het Zorgveld proactief in en de werkgroep vermeldt wat er in de praktijk is gewijzigd op het gebied van IB en/of in ISO-normen. Na aanpassing en vaststelling van het kader, publiceert VWS dit in de Staatscourant: de zorgsector moet voldoen aan de geactualiseerde NEN 7510.

NEN vervult de rol van beheerder, zij beheert en stelt de normen vast. NEN nodigt alle belanghebbenden uit om deel te nemen. Afspraken komen op basis van consensus tot stand en worden vastgelegd.

VWS vervult als stelseleigenaar de rol van facilitator en ontvangt signalen over IB in de zorg via Z-CERT, NEN, de IGJ en de Zorg, creëert meer bewustwording bij partijen en wil naleving makkelijker maken. VWS biedt handreikingen en een analysetool aan, geeft randvoorwaarden, kent een Actieplan Informatieveilig gedrag, faciliteert workshops, masterclasses en kijkt met Z-CERT naar afspraken met leveranciers.
VWS wil het NICTIZ een publieke rol gaan geven (met wetgeving) om een bibliotheek op te bouwen met verschillende informatiestandaarden en om stelselbeheer

[29] DPIA: Data Protection Impact Assessment en DTIA: Data Transfer Impact Assessment.
[30] NEN staat voor Nederlandse Norm EN voor Europese Norm. Het betrokken Nederlands Normalisatie-Instituut (NEN), valt onder verantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat.
[31] Het Zorgveld bestaat uit de zorginstellingen. De overheid heeft een beperkte rol in het Zorgveld: het hele Zorgveld is privaat behalve de Academische Ziekenhuizen. Het is daarom in eerste instantie aan instellingen om het zelf te regelen.

op te bouwen.[32] Hoe invulling van de relatie tussen VWS (stelselhouder/regisseur) en NICTIZ (stelselbeheerder) en eventuele anderen vorm krijgt is de vraag.

Z-CERT, is vraagbaak en adviseert leden bij het oplossen van een IT-beveiligings-incident en kan helpen bij forensisch onderzoek.
Z-CERT deelt informatie over dreigingen met leden, geeft training met ethical hacks.

3.4 Inrichting toezicht en naleving governance IBP bij het HO en bij de Zorg

Deze paragaaf biedt inzicht in de huidige governance inrichting in het Hoger Onderwijs en de Zorg op Normenkaders voor IBP gericht op toezicht en naleving en de organisaties die deze rollen invullen. In deze paragraaf wordt antwoord gegeven op de deelvragen twee en drie van het onderzoek. Binnen 4.1 en 4.2 worden de voor- en nadelen (voor-/tegenargumenten) genoemd (gericht op deelvraag 3) en de parallelle situatie voor het FO geschetst.

3.4.1 Toezicht en naleving governance IBP bij het HO

Volgens de stakeholders zijn interne toezichthouders bij de instellingen belangrijk: SURF geeft cursussen over IB en attentiepunten om goed toezicht te houden. SURFaudit verricht zelf geen audits maar faciliteert een dienst waarmee instellingen self-assessments kunnen doen, of een audit kunnen laten uitvoeren. Auditfrequentie en aanpak zijn per sector tussen de koepels[33] en OCW afgesproken.
Resultaten van de self-assessments en audits sturen instellingen naar SURF, die vervolgens een tweejaarlijks sector breed 'cyber-dreigingsbeeld' opstelt. SURF deelt bevindingen met de koepels, die vervolgens verantwoording afleggen aan OCW met verbeterplannen.
Relevant is volgens een stakeholder, functiescheiding in betrokken rollen: SURFaudit verricht geen audits. Behalve waar het gaat om DPIA's/DTIA's[34] in relatie tot leveranciers, die SURF als coöperatie verricht en waar nodig ondersteund wordt door aanvullende externe juridische expertise. Uitkomsten worden zowel met de leden als publiek gedeeld, tenzij het gevoelige bevindingen betreft. SIVON en SURF hebben samengewerkt aan het uitvoeren van DPIA's op producten die gebruikt worden in het FO. Dit blijkt uit de Visiebrief. Het collectief uitvoeren van DPIA's neemt individuele scholen veel werk uit handen. DPIA's leiden tot goede privacyafspraken met leveranciers.

Volgens een stakeholder hebben instellingen binnen het HO een hoge mate van autonomie. De verantwoordingslijnen rond het Normenkader IB zijn als volgt:
-OCW vraagt de koepels naar de stand van zaken van bijvoorbeeld gedane beloftes.
-SURF levert de koepels hierover informatie aan op sectorniveau.
-De koepels leggen vervolgens verantwoording af aan OCW.
-De minister van OCW informeert de Tweede Kamer. Instellingen hebben een eigen verantwoordelijkheid: in de wet is niets vastgelegd.
Momenteel worden alternatieve vormen van verantwoording afleggen besproken:
-Via de individuele lijnen van de instellingen: via jaarverslagen etc. Deze publieke informatie zou kwaadwillenden juist kunnen voeden;
-Verantwoording via de koepels;
-Verantwoording via SURF door middel van het sectoraal cyberdreigingsbeeld en middels de benchmark resultaten.
Bij de laatste optie werd SURF gevraagd om te gaan rapporteren over de instellingen en dit zou potentieel kunnen conflicteren met de andere rollen die SURF als coöperatie heeft ten aanzien van haar leden.

[32] NICTIZ is Nationaal Instituut ICT in de Zorg
[33] Een koepel is een vertegenwoordigende groep HO instellingen
[34] Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat organisaties maatregelen kunnen nemen om risico's te verkleinen. Data Transfer Impact Assessment (DTIA) is een instrument om vooraf de privacyrisico's in kaart te brengen bij doorgifte van persoonsgegevens naar een land buiten de Europese Economische Ruimte (EER) en vervolgens maatregelen te nemen.

Bij het HO komt Cybersecurity vaak voor in jaarverslagen, dit is echter niet verplicht voorgeschreven in het accountantsprotocol. Het Normenkader Informatiebeveiliging Hoger Onderwijs 2015 is een sectorale afspraak, geen wetgeving. Alle HO-instellingen moeten voldoen.

HO instellingen werken vaak met grotere accountantskantoren waar de accountant vraagt naar IB. Bij iedere instelling wordt in het kader van de jaarrekeningcontrole door de accountant ook een aantal administratieve systemen beoordeeld. Incidenteel laat een instelling, op eigen initiatief, een externe audit verrichten soms naar aanleiding van incidenten en meestal op specifieke informatiesystemen zoals het studentinformatiesysteem. Peer reviews vormen een externe controle.

Er is geen externe toezichthouder voor het Normenkader IB HO. Binnen het HO wordt gewerkt met Zelfregulering. De IvhO verricht geen vierjaarlijkse kwaliteits-onderzoeken in het HO (bekostigd of onbekostigd), dit doet de Nederlands-Vlaamse Accreditatieorganisatie (NVAO). Echter IB is in hun beoordelingskader geen thema.

3.4.2 Toezicht en naleving governance IBP bij de Zorg

Op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (WABVPZ) moeten zorgaanbieders verplicht en aantoonbaar voldoen aan de NEN 7510 (en verdere specificering).

VWS geeft aan dat een CISO of ISO in dienst een organisatie helpt aan de normen te voldoen. Zorginstellingen zouden een zelfevaluatie uit moeten voeren. VWS bekijkt momenteel of ze dat met Z-CERT of ICTU kunnen gaan aanbieden. De uiteindelijke verantwoordelijkheid ligt bij besturen zelf. Op grond van wetgeving moeten zorgaanbieders verplicht en aantoonbaar voldoen aan de NEN 7510, 7512 en 7513. De wet zegt niet *hoe* zorgverleners moeten aantonen dat ze voldoen: het kan met een certificaat vanuit een certificerende instelling of door een audit maar dat wordt niet voorgeschreven. Zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie kunnen zich certificeren tegen NEN 7510. Het certificatie-proces staat onder toezicht van de Raad voor Accreditatie (RvA), die zowel eisen stelt aan het certificatieproces als aan de certificerende organisatie. De AP heeft met de richtsnoeren voor de beveiliging van persoonsgegevens een nadere uitwerking gegeven van art. 13 Wbp en art. 32 AVG.

De Toezichthouder is de Inspectie Gezondheidszorg en Jeugd (IGJ), deze werkt bij het toezichthouden met een toetsingskader 'E-Health', wat een aantal eisen bevat op basis van NEN 7510 waaraan Zorgaanbieders moeten voldoen. Dit toetst de IGJ steekproefsgewijs. Factsheets over E-Health staan op de site van IGJ. IGJ reflecteert daarbij op de naleving.

Aandachtspunten van VWS voor het FO:

- Voldoende kennis en capaciteit zijn relevant, de IGJ heeft onvoldoende capaciteit om alle zorgaanbieders te onderzoeken op de naleving van het Normenkader en waar nodig te beboeten.
- Daarnaast is het goed om de Toezichtsbevoegdheid op IB wettelijk goed geregeld te hebben. IGJ zag toe op IB vanuit de kwaliteit van zorg waardoor IGJ alleen handhavend kon optreden als de kwaliteit van zorg in gevaar was. Dit is nu niet meer voldoende; VWS expliciteert dat momenteel in de wet.

4 Keuzemogelijkheden inrichting IBP voor het FO

Hieronder schetsen we zes keuzemogelijkheden. De eerste twee keuzemogelijkheden hebben wij geformuleerd aan de hand van inzicht verkregen bij de inrichting van de governance op de Normenkaders IB (1.) bij het Hoger Onderwijs en (2.) bij de Zorg zie 3.3 en 3.4. Hieruit gedestilleerde parallelle opties voor het FO hebben wij omkaderd. Deze twee keuzemogelijkheden liggen in het verlengde van de deelvragen 2 en 3 van dit onderzoek en zijn voorzien van voor- en tegenargumenten (ook wel voor- en nadelen) van SURF (voor het HO) en van VWS (voor de Zorg).

Dit onderzoek geeft mede inzicht in de volwassenheid van de scholen op het gebied van de interne governance, en op het gebied van begrip en de kennis van de materie uit het Normenkader IBP (zie Bijlagen 2 en 3). Scholen zijn nog niet altijd in staat om het Normenkader zelfstandig toe te passen. We hebben de uit dit onderzoek verkregen informatie gehouden tegen de Visiebrief van 6 juli 2023 van de Minister van OCW aan de Tweede Kamer (zie Bijlage 6) om deze aan te laten sluiten op de gewenste ontwikkelkoers van OCW.
Vervolgens hebben we nog vier keuzemogelijkheden geformuleerd. Deze zijn onder meer gericht op het ontzorgen van de scholen door (3.) Maatwerk en (4.) Centrale aanpak en de laatste twee zijn gericht op (5.) Toezichthouden en (6.) Wetgeving. Ook deze keuzeopties zijn voorzien van voor- en tegenargumenten. Wie de verstrekker is van die argumenten is afhankelijk van de tijdens dit onderzoek verkregen informatie.

4.1 Keuzemogelijkheid 1. Governance inrichting zoals bij het Hoger Onderwijs

SURF vervult bij de governance op het Normenkader IB voor het HO diverse rollen. Daarmee is naar aard ook een (min of meer) gecentraliseerde aanpak voor ICT/IBP van toepassing. In 3.3.1 en 3.4.1 hebben we de rollen van de governance inrichting bij het HO behandeld. Daarbij hebben we gezien dat SURF onder meer audittools en het eigenaarschap faciliteert voor het HO. Voor het FO is dit lastiger te realiseren omdat de organisatiegraad bij het FO anders is dan die bij het HO.
Uit de Visiebrief blijkt dat OCW een plan ontwikkelt om de organisatiegraad te verhogen. Na het bereiken van 'de basis op orde' zou de governance op het Normenkader IBP voor het FO, opties bieden om te groeien naar een constellatie vergelijkbaar met hoe het in het HO is geregeld.

De governance inrichting voor het HO kent de volgende rollen:

- *Eigenaar is het HO*

Het FO zou eveneens eigenaar kunnen zijn/worden van het Normenkader IBP.
Bij het HO is *snel overgegaan tot verplichting van het Normenkader*, dit kwam vanuit de sector zelf. Het zou goed zijn die volgorde ook te hanteren in het FO volgens een stakeholder.
Relevant is volgens ons om het FO in staat te stellen voldoende kennis en kunde over ICT/IBP te verkrijgen om *volwaardig eigenaarschap te kunnen invullen*.
Uitwisselen van kennis, kunde, lessen en ervaringen tussen het HO (SURF) en het FO (vertegenwoordigers) is belangrijk om uiteindelijk vooral het FO op een hoger niveau te krijgen, dit gebeurt nu al regelmatig tussen SURF, Kennisnet en SIVON.
Werkzaamheden verrichten vanuit de community-gedachte (ervaringen delen) met uitgangspunten van *gedeeld eigenaarschap* zijn relevant, volgens een stakeholder.

Het FO wordt momenteel (naast de PO- en VO-Raden) vertegenwoordigd door het *Netwerk IBP en de Regiegroepen ICT*.
Scholen dienen volgens ons te beschikken over *interne functionarissen (denk aan FG's en CISO's, PO's)* die de RvB van informatie kunnen voorzien en de RvB in staat stellen zich hierover te verantwoorden en bestaande vertegenwoordigers van het FO eventueel kunnen verrijken/aanvullen. Deze interne functionarissen kunnen centraal (wellicht via SIVON) worden geworven en mogelijk een aantal scholen bedienen, mede afhankelijk van het ontwikkelstadium van de scholen.

- *Ontwikkelaar is het HO*

-Kennisnet heeft binnen de voorlopige governance inrichting de rol om dienst-verlening te ontwikkelen en te beheren voor het hele FO.
Het *FO zou met Kennisnet (en wellicht SIVON, Edu-V, CERT io)* kunnen optrekken om ontwikkeling van het Normenkader vorm te geven. Via het IBP-Netwerk is nu een soortgelijke situatie ingeregeld.
-Met betrekking tot *Innovatie zou het FO, aansluiting kunnen zoeken bij de initiatieven van SURF.* Voor het FO is Innovatie gezien het volwassenheidsniveau van het FO wellicht nog wat lastiger dan bij het HO. Hierbij wordt de nodige expertise, kennis, kunde en achtergrond van ICT bekend verondersteld.
Gedacht kan worden aan de leden van de bestaande *IBP-netwerken, de Regiegroep ICT, FG's en CISO's met eventueel een vertegenwoordiging van Kennisnet, SIVON, Edu-V en CERT i.o.*

- *Beheerder, Facilitator en CERT zijn rollen van SURF*

SURF huisvest het Platform Integrale Veiligheid HO waar Privacy, Cybersecurity en het Normenkader IB HO, thema's zijn en HO instellingen samenwerken aan het verbeteren van de integrale veiligheid in het HO.

Voor het beheer van het Normenkader IB kent SURF een interne governance inrichting. Het beheer van het Normenkader IB is belegd bij de maturity-werkgroep binnen SURFibo.

- *Beheerder is SURF*

Overwogen kan worden of *SIVON, Kennisnet (met CERT io) en Edu-V gezamenlijk voor het FO een vergelijkbaar platform* kunnen gaan inrichten.
Aandachtspunt is dat het aantal leden van SIVON (FO) als 'counterpart' van SURF (HO) aanmerkelijk lager ligt dan het aantal leden van SURF bij het HO.
In de tijdelijke Governance op het Normenkader heeft het programma aangegeven dat Kennisnet de rol van beheerder vervult. Wellicht is *het voor het FO een optie om aansluiting te zoeken met de Maturity werkgroep en de stuurgroep van het HO voor de uitwisseling van informatie- en leerpunten om vervolgens zelf gremia in te richten dan wel te komen tot een samenwerkingsverband FO – HO of anderszins het beheer (van vergelijkbare thema's) van het Normenkader voor het FO te beleggen.*
Voor de vertegenwoordiging van het FO kan worden gedacht aan de leden van de bestaande IBP-netwerken, de Regiegroep ICT en de eerdergenoemde FG's, CISO's.
Een CIO-beraad, ICT-directeuren en IT-managers zijn bij het FO vaak (nog) niet aanwezig. Voldoende kennis van IT/IBP van leden van de RvB's met inrichting van specifiek portefeuillehouderschap voor ICT/IBP kan een bijdrage leveren aan het zijn van een adequate gesprekspartner in een vergelijkbaar gremium. FG's en CISO's, PO's kunnen een informatierol richting RvB innemen.
SURF beschikt over experts, daardoor hoeven HO-instellingen niet ieder het wiel zelf uit te vinden; deze experts zijn bij het FO nu binnen verschillende organisaties vertegenwoordigd zoals Kennisnet, SIVON, CERT i.o. en Edu-V.

- *Facilitator is SURF*

Faciliteren van diensten voor het doen van audits op het Toetsingskader zouden via *SIVON/Kennisnet* kunnen worden ingeregeld (of zijn reeds beschikbaar). SIVON/ Kennisnet en CERT i.o. zouden na het verkrijgen van betrokken self-assessments ook aan het opstellen van een *benchmark en een cyberdreigingsbeeld* kunnen werken.
Contractmanagement en Leveranciers compliancy zouden centraal en in gezamenlijkheid tussen *SIVON, Kennisnet (met CERT i.o.) en Edu-V* kunnen worden opgepakt met eventuele gebruikmaking van de *leerpunten van SURF*.

- *SURFcert*

Voor het FO bestaat een CERT in oprichting (bij Kennisnet).

SURF geeft aan een governance inrichting als bij het HO een aantal argumenten voor en argumenten tegen:

Argumenten voor

- Doordat er experts verbonden zijn aan SURF, hoeven HO-instellingen niet ieder het wiel zelf uit te vinden.
- SURF krijgt steeds meer inzicht in de situatie en de kwetsbaarheden bij de sector.
- Ook contactpersonen van de SURF-leden met hun onderlinge uitwisseling van kennis en ervaringen verrijkt het.
- Het HO heeft zichzelf ontwikkeld op het gebied van IBP, kan impact van wijzigingen inschatten en voert wijzigingen (na pilots etc.) beheerst door.
- Het lerend vermogen is bij het HO goed ontwikkeld en er wordt gewerkt met best practices.

Argumenten tegen

- Niet-bekostigde HO-en MBO-instellingen maken geen onderdeel uit van SURF. Hun informatiepositie is een andere: zij zijn momenteel niet aangesloten op landelijke dreigingsinformatie via de CERTS of informatiepunten.

Tenslotte geeft SURF een aantal aandachtspunten gericht op de huidige situatie bij het FO in vergelijking met het HO:

- SURF kent een ander ontwikkelingsniveau dan SIVON. SURF is door leden opgericht en bestaat ongeveer 36 jaar. SURF werkt met ongeveer 480 medewerkers en circa 200 externen. In het HO zijn minder instellingen en is er sprake van meer slagkracht dan in het FO.
- De organisatiegraad bij het HO is een succespunt: alle bekostigde instellingen zijn lid van SURF. De lagere organisatiegraad in het PO/VO is mogelijk een probleem, ondersteuning bij het verhogen hiervan kan helpen. Potentiële imago-schade bij het HO is een natuurlijke prikkel om de beveiliging op orde te hebben.
- In het HO zijn rollen toebedeeld en is functiescheiding aangebracht, dit kan professioneel vanwege de schaalgrootte. Binnen het FO kan dit niet altijd. Het is dan ook de vraag of je aan kleine FO-instellingen dezelfde mate van inspanning en eenzelfde rolverdeling kunt vragen als aan grote.
- Binnen het HO bestaan ook kleinere instellingen zoals de PABO-hogescholen. Zij moeten met minder capaciteit dezelfde maatregelen invoeren en naleven als grotere instellingen. Zij organiseren samen kennis over IT en security, zoals het CISO-as-a-Service-concept, wat wordt verkend. FO-instellingen hebben veelal geen eigen IT-organisatie waardoor er relatief weinig IT-kennis aanwezig is wat een probleem kan zijn bij het laten groeien op het maturity level bij deze instellingen. Als bekend is welke scholen bij het FO met dezelfde problemen zitten, kunnen vergelijkbare scholen aan elkaar

worden gekoppeld met eventueel een externe voor inhoudelijke kennis om hen verder te helpen. Voor het draagvlak is cruciaal dat je geen onrealistische verwachtingen hebt van onderwijsinstellingen: te snel en te veel opleggen helpt dan niet.
- OCW heeft een investeringspakket aan het MBO verstrekt. Het MBO besteedt dit centraal (in overleg met SURF) aan maatregelen voor verhoging van het maturity level. Groeifonds NPULS heeft geld beschikbaar gesteld om het hele HO in een gezamenlijke IT-infrastructuur te krijgen, dit om ook IBP goed in te richten. Risico zit in het feit dat 'alle kikkers in de wagen' blijven. Gebruik van gezamenlijke systemen en leveranciers moet geborgd worden. Leveranciersmanagement moet adequaat zijn ingericht.

4.2 Keuzemogelijkheid 2. Governance inrichting zoals bij de Zorg

De Zorg heeft het initiatief genomen om een Normenkader te ontwikkelen en in 2008 is werken volgens de NEN 7510 wettelijk verplicht gesteld. In 3.3.2 en 3.4.2 hebben we de rollen van de governance inrichting bij de Zorg behandeld.
Na het bereiken van 'de basis op orde' zou de governance op het Normenkader IBP voor het FO, opties bieden om te groeien naar een constellatie vergelijkbaar met hoe het in de Zorg is geregeld.

De governance inrichting voor de Zorg kent de volgende rollen:

- *Eigenaar is de Zorg*

De eigenaar van het Normenkader NEN 7510 is de Zorg. De overheid heeft een beperkte rol in de Zorg omdat het privaat is met uitzondering van Academische Ziekenhuizen. In eerste instantie is het aan instellingen om het zelf te regelen.

De opties voor het FO zijn daarom vergelijkbaar met die zijn genoemd bij de rol van Eigenaar van het HO-veld (4.5).

- *Beheerder is NEN*

Beheerder van het Normenkader is NEN: de Stichting Koninklijk Nederlands Normalisatie Instituut. NEN beheert de normen en stelt ze vast. NEN nodigt alle belanghebbenden uit om deel te nemen: breed draagvlak is randvoorwaarde. Afspraken komen op basis van consensus tot stand en worden vastgelegd: dit is meestal een norm.

De Zorg heeft het beheer van het Normenkader IB belegd bij een (extern) instituut dat buiten het primaire Zorgveld staat. Bij het HO wordt gewerkt met SURFibo (met een governance van een stuur- en werkgroep en afstemmingsgremia bij het HO zelf) als beheerder van het Normenkader. Bij beiden geldt verplichte naleving en bij de Zorg van een wettelijke verplichting. Het werken met NEN kent een aantal voor- en nadelen volgens VWS die aan het einde van deze paragraaf worden beschouwd. Wat betreft de procesgang voor het beheer zijn overeenkomsten zichtbaar.
Voor de vertegenwoordiging van het FO kan worden gedacht aan de leden van de bestaande *IBP-netwerken, de Regiegroep ICT en de FG's, CISO's bij de scholen.* Een CIO-beraad, ICT-directeuren en IT-managers zijn bij het FO vaak (nog) niet aanwezig. *Ook bij NEN zal sprake moeten zijn van voldoende kennis en capaciteit van IT/IBP bij verschillende gremia in het FO om deze rol goed invulling te geven.* Experts zijn in het FO aanwezig bij *Kennisnet, SIVON, CERT i.o. en Edu-V. Een afweging zou moeten worden gemaakt welke rol zij bij het beheer van het Normenkader door NEN zouden kunnen innemen.*

- *Ontwikkelaar is de Zorg*

De Zorg is medeontwikkelaar van de normen. Actualisatie vindt iedere vijf jaar of zo nodig eerder plaats. NEN schakelt de werkgroep met stakeholders uit de Zorg hierbij proactief in en de werkgroep geeft aan wat er in de praktijk is gewijzigd op het gebied van IB en/of in ISO-normen.

Net als bij het Normenkader voor het HO is ook bij het Normenkader voor de Zorg, het veld (mede-)ontwikkelaar (en eigenaar). Het FO zou *met vertegenwoordiging van Kennisnet (en wellicht SIVON, Edu-V, CERT i.o, de Regiegroep ICT en IBP-netwerken)* als stakeholders kunnen optrekken om ontwikkeling van het NEN-Normenkader vorm te geven. Bij het FO zelf wordt *de nodige kennis, kunde en achtergrond van ICT* aanwezig verondersteld om de rol van (mede-)ontwikkelaar volwassen vorm te geven, denk aan: *de FG's en CISO's en hun vertegenwoordigers* bij de rol.

- *Facilitator is VWS*

VWS vervult als stelseleigenaar de rol van facilitator. VWS ontvangt signalen over IB in de zorg via Z-CERT, NEN, de Inspectie Gezondheidszorg en Jeugd (IGJ) en de Zorg. VWS creëert meer bewustwording bij partijen en beoogt naleving makkelijker te maken.

Bij het Normenkader van het HO zien we voor SURF een rol als facilitator daar waar deze rol bij het Normenkader voor de Zorg door VWS ingevuld wordt. OCW zou kunnen overwegen of OCW zelf deze rol wil en kan gaan vervullen.

- *Z-CERT*

De Zorg werkt met Z-CERT. FO kent een CERT in oprichting.

Specialist voor ICT in de Zorg
VWS meldt dat het Nationaal Instituut ICT in de Zorg (NICTIZ) vergelijkbaar is met Kennisnet binnen het onderwijsveld. VWS is bezig om NICTIZ een publieke rol te geven (dat zal met wetgeving moeten) om een bibliotheek op te bouwen met de verschillende informatie-standaarden en om stelselbeheer op te bouwen: hier moeten nog voorstellen voor komen. Hoe de relatie tussen VWS (stelselhouder/ regisseur) en NICTIZ (stelselbeheerder) en eventuele anderen wordt ingevuld is nog de vraag. Er is een relatie met het proces in het FO. Wat is de rol van de overheid? Wie heeft stelselregie?

Edu-V lijkt vergelijkbare activiteiten te verrichten voor het FO als NICTIZ in de Zorg daar waar het gaat om standaarden. *Wellicht kan OCW met VWS in gesprek over de relatie die zij kennen als stelselhouder naar stelselbeheerder* (voor zover dit aan de orde is voor OCW).

VWS geeft aan deze governance inrichting voor het FO als bij de Zorg een aantal argumenten voor- en argumenten tegen:

Argumenten voor
- NEN is beheerder van het Normenkader en zorgt voor verbinding van partijen in de werkgroep.
- Afspraken worden gemaakt waaraan je kunt refereren indien nodig.
- Er is sprake van een autonoom aanpassingsproces.

Argumenten tegen

- Het NEN-proces kost tijd.
- VWS heeft als één van de partijen beperkte mogelijkheden om op inhoud van de normen te sturen. Dit gaat goed, echter als de norm zou gaan afwijken van de wensen van VWS, moet VWS de wet aanpassen.

Tenslotte geeft VWS een aantal aandachtspunten gericht op de huidige situatie bij het FO in vergelijking met de Zorg:

- Hanteer een groeimodel: verplichten om te voldoen aan het hoogste niveau is niet reëel als partijen nog niet zover zijn, of er geen middelen beschikbaar zijn. Werk dan eerst aan: 'het kunnen voldoen'.
- Zet onderwijs specifieke zaken in het Normenkader, ook die zaken die je niet in internationale vereisten ziet.
- Formuleer normen en beheersmaatregelen niet te gedetailleerd omdat het Normenkader dan mogelijk extra eisen stelt aan organisaties die b.v. al voldoen aan ISO (NEN 7510 is gebaseerd op ISO 27001). Voldoen aan de normen van het kader is lastig bij gebrek aan een (C)ISO.
- Aandacht voor het voorkomen van monopolie vorming bij leveranciers. VWS kijkt daarom met de Autoriteit Consument & Markt naar de leveranciers-markt.
- Houd de governance eenvoudig en beleg zo mogelijk bij bestaande partijen. Wees helder over rollen en rolverdeling en beleg het eigenaarschap goed.
- Zorg als stelselverantwoordelijke voor voldoende kennis en capaciteit om b.v. alle signalen te verwerken in beleid. Deze rol is faciliterend: handvatten en tools aanreiken, randvoorwaarden geven, bewustwording creëren (beleggen in het veld), duidelijkheid bieden over de rollen en rolverdeling. Het (Nederlandse en Europese) wettelijke kader moet niet verzanden in verschillende wetten/kaders/normen: wees alert.

4.3 Keuzemogelijkheid 3. Ontzorgen door Maatwerk

Scholen en andere stakeholders benoemen rollen voor de externe governance waaruit blijkt dat (extra) hulp nodig is. Een Helpdeskrol wordt ingericht maar ook dan zal het voor scholen zonder eigen IT-expertise erg lastig worden om zelfstandig invulling te geven aan hun verantwoordelijkheid. Praktische toepassing van het Normenkader moet (meer) aandacht krijgen vanuit zowel het perspectief van de scholen, als dat van de leveranciers volgens stakeholders. In de Visiebrief staat dat het voor schoolleiders en bestuurders vaak onduidelijk is wat ze moeten doen en hoe ze dat moeten doen. Het programma ondersteunt alle scholen met passende producten, diensten en communicatie zo stelt de minister in de brief.

Uit ons onderzoek blijkt dat scholen ieder hun eigen 'vertrekpunt' kennen en dat daarmee ieder een eigen hulpvraag heeft voor het zetten van een volgende ontwikkelstap om te (gaan) voldoen aan het Normenkader. 'Hulp op maat' is nodig met respect voor de autonomie van scholen en om in hun specifieke behoefte te kunnen voorzien. Met de inzet van Kennisnet (en IBP-netwerk) en SIVON zou dit kunnen volgens scholen.

Nu scholen het Normenkader al enige tijd in volle omvang kennen (april 2023) lijkt het goed om de specifieke behoefte aan maatwerk/de expliciete hulpvraag bij scholen te inventariseren.

Volgens ons kent de toepassing van maatwerk de volgende argumenten voor en argumenten tegen:

Argumenten voor

- Scholen worden gericht meegenomen vanuit hun eigen specifieke organisatie/perspectief in de ontwikkeling van kennis en kunde over de elementen uit het Normenkader IBP.

- Scholen worden gericht geholpen bij het zetten van hun eigen specifieke volgende stap en worden daarmee meer in hun kracht gezet.
- Uiteindelijk wordt een bijdrage geleverd aan het doelbereik van het Normenkader (en daarmee aan het Programma Digitaal Veilig Onderwijs).

Argumenten tegen

- Voor zowel de vragende partijen als de helpende partijen zal dit een arbeids- en tijdsintensief traject betekenen.
- Aanwezige en benodigde capaciteit bij de vragende en de helpende partijen zullen moeten worden geïnventariseerd en afgestemd op de aanpak.

4.4 Keuzemogelijkheid 4. Ontzorgen door Centrale aanpak

Uitkomsten van de geïnventariseerde specifieke behoefte bij scholen kan echter ook leiden tot de overweging tot (gedeeltelijke) Centrale aanpak. Stakeholders noemen diverse argumenten en thema's die pleiten voor centrale aanpak zoals gezamenlijk gebruik van dezelfde IT-informatiestructuur, IT-systemen en leveranciers.

In de Visiebrief is sprake van een landelijk dekkend landschap van organisaties, voorzieningen, afspraken en standaarden, nodig om het FO veilig, efficiënt en flexibel te faciliteren om het gebruik van digitale middelen op scholen te ondersteunen. Er wordt geïnvesteerd in een digitale (leermiddelen) infrastructuur voor het FO. SIVON helpt alle scholen door afspraken te maken met leveranciers over tijdige levering van goede en betaalbare leermiddelen. Ook bereidt SIVON, afspraken voor die de afhankelijkheid van scholen van grote internationale techbedrijven indamt en zorgt voor een goed en aantrekkelijk aanbod voor haar leden. Digitale veiligheid en continuïteit van het FO staan onder druk omdat cyber-criminelen ook het onderwijs in hun vizier hebben. Vraagstukken worden complexer en urgenter, aangezien de infrastructuur van devices en software onmisbaar zijn in de klas. Het FO worstelt met afhankelijkheid van grote techbedrijven. Doelstelling is om een publiek-privaat afsprakenstelsel te realiseren, aldus de Visiebrief.

Edu-V vindt het belangrijk dat het Normenkader IBP zodanig is dat scholen eraan willen meedoen, omdat ze daarmee makkelijker, goedkoper, beter en veiliger kunnen werken en veronderstelt dat Edu-V scholen kan helpen bij onderdelen uit het Normenkader. Afspraken hierover zijn volgens Edu-V nog niet gemaakt. Het programma Edu-V heeft als doelstelling om op één plek de regie en het toezicht op afspraken te regelen: governance en het afsprakenstelsels meer standaardiseren. Afsprakenstelsels maken het scholen makkelijker om te kiezen voor software. Een softwareleverancier moet aan eisen voldoen maar scholen weten niet altijd precies welke dit zijn. Thema's waar de scholen tegen aan lopen liggen voor 80% bij de leveranciers/oftewel het primaire proces. 80% van het primaire proces zit bij Edu-V, er is dan één aanspreekpunt. Edu-V controleert niet of scholen afspraken uit het Normenkader naleven. Het programma Edu-V kent vijf technisch-inhoudelijke werkgroepen waarin leveranciers, scholen, Kennisnet en SIVON participeren. Vooral brancheorganisaties, uitgevers, dienstverleners (voor digitaal onderwijs) en VO-/PO-/MBO-raad zitten in Edu-V.

Een Centrale aanpak kent volgens ons onder meer de volgende argumenten voor en argumenten tegen:

Argumenten voor

- Scholen worden structureel ontzorgd op thema's die voor hen te complex, te tijdrovend, te duur en te veel omvattend zijn om individueel en duurzaam op te pakken en houden regie op thema's die zij zelf kunnen/willen regelen.
- Scholen kunnen zich concentreren op school specifieke beheersmaatregelen in het kader van het Normenkader IBP: bewustwording, gedrag, ingerichte

applicaties adequaat gebruiken, toetsing van naleving en de RvB en de RvT in staat stellen om hun verantwoordelijkheid te nemen etc.
- Scholen kunnen zich zo beter concentreren op hun kernactiviteiten: goed onderwijs geven en de kwaliteit van het onderwijs borgen.
- Centrale aanpak geeft (op termijn) schaalvoordelen.

Argumenten tegen
- Scholen hebben mogelijk weerstand uit angst (een deel van) hun autonomie te moeten inleveren. Voorbeeld: een school geeft aan dat *'het onverstandig zou zijn om alles rond het Normenkader landelijk te regelen en het vervolgens schoolbesturen 'niet meer aangaat'. Het gaat ook over gedrag binnen de school en daarvoor moet een schoolbestuur verantwoordelijkheid voelen. De school geeft mee dat als slechts een paar programma's gebruikt mogen worden (dan is ook veel geregeld), de school voorziet dat mensen op hun eigen PC aan de slag gaan en dat dan het probleem voor de bühne maar niet in gedrag is opgelost. Scholen willen betrokken zijn en betrokken blijven'.*
- De huidige organisatiegraad in het PO/VO is mogelijk een probleem wanneer je zaken centraal zult moeten organiseren.
- Scholen vinden het mogelijk lastig om de consequenties van de verandering te overzien.
- Aandacht voor tegengestelde belangen van marktpartijen.
- Aandacht voor een mogelijke monopolie positie van een leverancier en (te) grote afhankelijkheid van de afnemer.
- Juiste taak- en rolverdeling tussen partijen zonder overlap van rollen/taken en het voorkomen van rol-, taak- en belangenvermenging, en/of -verstrengeling (functiescheiding) zijn relevant, anders kan dit nadelig uitpakken.

4.5 Keuzemogelijkheid 5. Toezichthoudende rol binnen Governance inrichting

Momenteel is toezicht nog niet ingeregeld en ontbreekt veelal ook de basis ervoor. Verantwoording over IBP is nog niet ingeregeld en dit gebeurt nu willekeurig zoals aan de hand van een samenvatting van een veiligheidsverslag, vermelding in een risicoparagraaf etc. Wanneer verantwoording structureel en op uniforme wijze plaatsvindt kan extern toezicht zich hierop richten.
In de Visiebrief meldt de Minister dat er in 2027 Toezicht en Handhaving zal plaatsvinden en dat scholen vanaf jaarverslag over 2024 verplicht zijn aandacht te besteden aan IBP.

Intern toezicht (FG, CISO en RvT) en extern toezicht (accountant, IvhO, AP) vraagt om een zekere wederzijdse balans. Als de basis op orde is, intern toezicht bij het FO een meer volwassen vorm heeft, kan effectief extern toezicht plaatsvinden, veronderstellen we. Samenhang bestaat met:
- De volwassenheid van het FO;
- Het Normenkader zelf: het Privacy-deel is nog niet ingevuld en guidance is nog niet volledig beschikbaar;
- Het nog te verschijnen Groeipad;
- De kennis en capaciteit van optionele betrokken partijen.

Om intern toezicht in eerste aanleg verder op orde te brengen vermelden we de volgende onderzoek informatie en suggesties van stakeholders:

Het kennisniveau van ICT/IBP bij de leden van de RvT (de RvB en bij leraren) op orde brengen: het is nu vaak onder de maat en opleidingen voorzien niet in thema's als IBP/ICT. VTOI-NVTK zou met OCW kunnen werken aan verbetering. Volgens VTOI/NVTK zou de RvT een eigen Toezicht visie, een Toetsingskader en bijbehorende criteria moeten hebben. Dit is echter nog lang niet bij iedere RvT het geval. VTOI-NVTK wil dat IBP daarin een vast thema wordt. Wellicht kunnen

SIVON/Kennisnet (in gezamenlijkheid met SURF b.v.) een cursus aanbieden aan leden van de RvT of aan andere interne toezichthouders van het FO.

-Als het Normenkader IBP voor het FO gecompleteerd is kunnen Informatiebeveiliging en Privacy in self-assessments worden uitgevraagd en kan periodiek een IBP-dreigingsbeeld volgen door b.v. CERT i.o. aan de hand van de uitkomsten daarvan.
-CERT i.o. kan deze bevindingen delen met de PO- en VO Raad, die zich hiermee verantwoorden aan OCW.
-Scholen hebben behoefte aan praktische en goed toepasbare tools: SURFaudit lijkt een goed voorbeeld om self-assessments/audits te kunnen uitvoeren.
-SIVON verricht 'deep dives' die mogelijk een vaste dienst kunnen worden.
-OCW kan als stelselverantwoordelijke met de PO/VO Raad voor het FO ook afspraken maken over auditfrequentie en aanpak voor de FO-sector conform het HO. In het verlengde hiervan: de Autoriteit Persoonsgegevens (AP) heeft behoefte aan een geaggregeerd beeld over de AVG-compliance in het FO aan de hand van verantwoording door een onafhankelijke partij.

Over de (on-)mogelijkheden tot het inrichten van extern toezicht staat in 3.2.2. een uiteenzetting aangaande de accountant, de IvhO en de AP. Stakeholders, betrokken bij dit onderzoek noemen zowel intern als extern toezicht en of ze daar voorstander van zijn of tegenstander:

Argumenten voor

- Intern toezicht:
    - Zelfregulering/Self-assessments zijn nu passend omdat het Normenkader en bijbehorende guidance nog niet compleet zijn. Scholen zijn nog niet voldoende volwassen op het inhoudelijke gebied van IBP: het lerende aspect is relevant en het maakt dat ontwikkelingen in het FO zijn te volgen.
    - Het FO moet zich eigenaar voelen van en draagvlak hebben voor het Normenkader, dit vraagt om een start bij het FO-veld zelf.
- Extern toezicht:
    - Een zekere autoriteit is nodig zoals IGJ in de Zorg, scholen moeten worden aangesproken als ze niet voldoen anders gaat het om een 'papieren tijger'. Het woord van een Inspectie heeft gewicht.
    - Capaciteit en kennis van de materie voor accountants: inzet van een IT-auditor is een mogelijkheid. Er is een voorkeur voor een separate toezichthouder ter voorkoming dat besturen toezicht houden op hun eigen werk.

Argumenten tegen

- Extern toezicht:
    - Dit is nog niet nodig omdat het Normenkader 'guidance' biedt en gezien de omstandigheden in het FO is extern toezicht niet gepast.
    - Toezicht (nu) kan het veld gaan afremmen in de ontwikkeling: te snel ingrijpen kan het succes van de veldnorm remmen.
    - Bij controles door de Accountant/IT auditor dient er een uitvoerbaar en controleerbaar Normenkader IBP voor het FO aan ten grondslag te liggen.
    - Er is een tekort aan accountants en hun werkzaamheden breiden zich uit. Het beleggen van toezicht op IBP bij de accountant wordt niet gewenst in verband met de kern van de accountantsrol en de verhoging van de accountantskosten door

meer taken, tenzij het Normenkader een wettelijke verplichting wordt en er een sanctionerende werking volgt.
- Het gesprek over IT met de IvhO gaat naar verwachting het gesprek over het inhoudelijk onderwijs vertroebelen. De IvhO gaat over de inhoud en kwaliteit van het onderwijs. Scholen ervaren dat de IvhO adviezen geeft en beperkt bevoegd is tot het opleggen van sancties en daarom is dit geen goede rol voor de IvhO.
- De IvhO vermoedt dat de beschikbare IT-kennis en -capaciteit in Nederland onvoldoende is om het hele kader te toetsen in het hele FO en noemt 'Certificering' als optie.
- Is toezicht houden eigenlijk wel nuttig en nodig vraagt een school: bestuurlijke verantwoordelijkheid en aanspreekbaarheid ligt bij de RvB en de RvB spreekt met de RvT. Dan is er geen 'extern toezicht' nodig. De school stelt voor om de volledige cyclus van de scholen in beeld te krijgen en stelt zelf aan de hand van een veiligheidsverslag het volwassenheidsniveau IBP vast.

4.6 Keuzemogelijkheid 6. Normenkader IBP voor het FO omzetten in Wetgeving

Wetgeving maakt extern toezicht mogelijk door bijvoorbeeld de IvhO. In de huidige situatie is er geen sprake van wetgeving, wel zijn er opties mogelijk om toezicht in te regelen, denk aan de accountant als toetser en IvhO als toezichthoudend orgaan. In 3.2.2. zijn deze opties vermeld.

Het Normenkader IBP is momenteel een levend document en nog in ontwikkeling. Ontwikkelingen in ICT/IBP (AI gerelateerde kwesties met ChatGPT) en wetgeving (denk aan NIS2[35]) en verbeteringen die scholen aanreiken op basis van ervaringen in de praktijk, leiden mogelijk tot verdere aanpassing van het kader.

Zoals een stakeholder het formuleerde:
"Hanteer een groeimodel. Als partijen nog niet zover zijn, of als er substantieel geen middelen beschikbaar zijn, dan is het verplichten van het hoogste niveau niet reëel. Dan moet je eerst werken aan: 'het kunnen voldoen'. Na een groeiperiode kan worden overwogen om het Normenkader meer juridisch te maken".

Stakeholders geven zowel argumenten voor als argumenten tegen het omzetten van het Normenkader IBP voor het FO in wetgeving:

Argumenten voor
- Wetgeving lijkt de enige mogelijkheid om naleving af te dwingen en geeft opties tot sanctioneren.
- De technologie ontwikkelt snel, daarom moet richting worden gegeven aan de gewenste ontwikkeling. Het FO heeft behoefte aan duidelijkheid en die kan er komen met wetgeving.
- Het wettelijk maken van het Normenkader IBP kan bijdragen aan AVG-compliance. De PO/VO Raad en de AP hebben verkend of het Normenkader IBP voor het FO in een AVG-gedragscode is te brengen, dit bleek niet mogelijk.

Argumenten tegen

[35] In een tijd van groeiende digitale afhankelijkheid en toenemende cyberdreigingen heeft de Europese Unie de **N**etwork and **I**nformation **S**ecurity Directive herzien, resulterend in NIS2. Deze richtlijn, van kracht sinds januari 2023, versterkt de digitale weerbaarheid van de lidstaten. Organisaties moeten zich voorbereiden op de eisen die in januari 2025 van kracht worden.

- Het in wetgeving vastleggen kan leiden tot verminderde 'wendbaarheid' en kan de uitvoering belemmeren. In het HO is het kader niet in wetgeving vastgelegd, daardoor gebeurt er veel en is er wendbaarheid.
- De Zorg werkt met NEN 7510 en is wettelijk verplicht. Dit NEN-proces kost echter tijd.
- VWS is één van de betrokken partijen bij NEN en heeft beperktere mogelijkheden om op inhoud van de normen te sturen. Als de norm zou gaan afwijken van de wensen van VWS, dan moet VWS de wet aanpassen.
- Er is juist minder regeldruk gewenst (bij de scholen), met wetgeving gaat dit juist eerder toenemen en een verplichting/wetgeving helpt niet altijd.
- De sector moet zich eigenaar voelen van het Normenkader: draagvlak is nodig. Na een groeiperiode zou je het voldoen aan het Normenkader meer juridisch kunnen maken.
- Bij te veel voorschrijven wordt de uitvoering belemmerd en aanpassing van wet- en regelgeving duurt lang. Een juridisch vastgesteld Normenkader zou een optie zijn.
- Wettelijke verankering op inhoud (dat is gerichter te handhaven) is relevanter dan wettelijke verankering van het specifieke Normenkader.
- Wetgeving lijkt de enige mogelijkheid om naleving af te dwingen. Hoe ga je om met eenpitters die moeite zullen hebben met naleven, functiescheiding, de regellast die erbij komt kijken? Hoe acceptabel is het als mensen hier niet aan kunnen voldoen?

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

Het onderzoek heeft in een aantal stappen plaatsgevonden volgens de beschrijving in de opdrachtbevestiging. Stap 0 bestond uit het vooronderzoek waarin de ADR op basis van documentonderzoek en in vijf gesprekken met ADR-collega's heeft verkend wat er (bij de ADR) bekend is over de governance van Normenkaders.

Stap 1 was een verkenning van suggesties, belangen en wensen binnen het veld van het funderend onderwijs die een rol spelen in de governance. Deze verkenning bestond uit dertien gesprekken met stakeholders (inclusief drie scholen). Op de gespreksverslagen is hoor-wederhoor toegepast. Daarnaast heeft de ADR relevante documenten bestudeerd. Stap 2 bestond uit het ophalen van ervaringen met bestaande governance-inrichtingen op Normenkaders binnen het veld van de Zorg en het Hoger Onderwijs. Hiervoor zijn drie gesprekken gevoerd. Op de gespreksverslagen is hoor-wederhoor toegepast. Daarnaast heeft de ADR relevante documenten bestudeerd. In stap 3 heeft de ADR de uitkomsten uit de eerdere stappen geanalyseerd om te komen tot het antwoord op de onderzoeksvragen.

Referentiekader
De ADR heeft – conform opdrachtbevestiging – als referentie meegenomen: de Normenkaders IBP van het FO en die van de twee te onderzoeken sectoren: de Zorg en het Hoger Onderwijs. Aanvullend heeft de ADR het Normenkader IBP voor het MBO bestudeerd. De reden hiervan is dat de Normenkaders (indirect) informatie kunnen bevatten over de governance van het Normenkader. Daarnaast heeft de ADR het Plan-Do-Check-Act-cyclus (PDCA) principe meegenomen als referentie, evenals de *Kaderstellende visie op toezicht 2005,* die kaders geeft voor de positionering en inrichting van het toezicht op rijksniveau. Gedurende het onderzoek heeft de ADR nog andere referenties gevonden waaronder de Visiebrief (zie Bijlagen 1 en 6).

Beperkingen van het onderzoek
Vanwege de verkennende aard van dit onderzoek, heeft de ADR gedurende de gesprekken regelmatig suggesties gekregen voor aanvullende gesprekken met andere stakeholders dan vooraf voorzien. In een aantal gevallen heeft de ADR deze aanvullende gesprekken gevoerd, maar niet altijd. Dat heeft te maken met de tijdsplanning van het onderzoek in combinatie met de afbakening en het feit dat het aantal gesprekspartners dat iets kan zeggen over governance in principe oneindig is. Om deze reden maakt de ADR het voorbehoud dat er mogelijk waardevolle invalshoeken of ideeën voor de governance-inrichting ontbreken in dit rapport.

Hoor-wederhoor op dit rapport
De inhoudelijke afstemming van dit rapport heeft plaatsgevonden met de opdrachtgever. In de bijgevoegde managementreactie heeft de opdrachtgever zijn visie op de onderzoeksresultaten verwoord.

5.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een

onderzoeksopdracht betreft voor inventarisatie en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zou de ADR wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd volgens de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

5.3 Verspreiding rapport

De opdrachtgever, mr. drs. I.J. (Inge) Vossenaar MBA, Directeur-generaal Primair en Voortgezet Onderwijs bij het Ministerie van OCW, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

6 Ondertekening

Den Haag, 11 april 2024

Persoonsgegeven

Managementreactie

Ministerie van Onderwijs, Cultuur en Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

Persoonsgegeven
Ministerie van Financiën, Auditdienst Rijk

Korte Voorhout 7
2511 CW DEN HAAG

Onderwijspersoneel en Primair Onderwijs
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Datum
21 maart 2024

Onze referentie
44551603

Datum 28 maart 2024
Betreft Managementreactie op het onderzoeksrapport: Governance op het Normenkader IBP voor het funderend onderwijs

Geachte *Persoonsgegeven*,

Het bevorderen van de digitale veiligheid en het borgen van de privacy van leerlingen en onderwijspersoneel staat hoog op de agenda van het ministerie van OCW en de onderwijssector. Daartoe is het programma Digitaal Veilig Onderwijs opgericht: een samenwerkingsverband tussen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad. Binnen het programma Digitaal Veilig Onderwijs is in 2023 het normenkader informatiebeveiliging en privacy gelanceerd. Het normenkader biedt scholen belangrijke handvatten voor de digitale veiligheid binnen het funderend onderwijs. We zien dat scholen en bedrijven volop aan de slag zijn met het normenkader. De volgende stap is het verstandig inrichten van het beheer en toezicht op naleving.

Met interesse heb ik kennis genomen van het onderzoeksrapport *Governance normenkader IBP FO*. De keuzemogelijkheden die de ADR geeft in haar rapport helpen het ministerie van OCW om afwegingen rond beheer en naleving goed in kaart te brengen. De ADR heeft gesproken met een breed scala aan stakeholders. Standpunten zijn op een inzichtelijke manier samengebracht. In het rapport legt de ADR nadruk op de grote opgaven waar de sector voor staat, gecombineerd met de beperkte capaciteit. In het rapport worden bruikbare opties geschetst voor de governance op het normenkader, voor toezicht en handhaving bij de scholen en voor een succesvolle aanpak. Bij deze drie onderwerpen wordt inzicht gegeven in mogelijke rollen en de invulling hiervan. Daarnaast worden inrichtingsopties uitgewerkt, met behulp van een vergelijking met de normenkaders in het hoger onderwijs en de zorg.

Mede op basis van de door de ADR geschetste keuzemogelijkheden zal het ministerie van OCW een besluit kunnen voorbereiden over de inrichting van de governance op het normenkader voor informatiebeveiliging en privacy. Hierbij worden tevens de juridische en financiële randvoorwaarden zorgvuldig meegewogen. Ook wordt zo veel mogelijk rekening gehouden met de specifieke kenmerken van het funderend onderwijs.

Zoals in het rapport is aangegeven, kent elke oplossingsrichting zowel voordelen als nadelen. Daarom zal het ministerie van OCW de stakeholders goed blijven betrekken bij de vervolgstappen.

Ik wil de onderzoekers van de ADR bedanken voor het werk dat zij verricht hebben om dit rapport tot stand te laten komen. Daarnaast wil ik de gesprekspartners bedanken voor hun tijd en bereidwilligheid om met de onderzoekers in gesprek te gaan.

de directeur-generaal Funderend Onderwijs,

Persoonsgegeven

Inge Vossenaar

Onderwijspersoneel en Primair Onderwijs
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Datum
21 maart 2024

Onze referentie
44551603

Bijlage (1) Wat is Governance?

Voordat we ingaan op eisen en wensen voor de governance op het Normenkader IBP vanuit het veld van FO, staan we stil bij de definitie van governance. Dit is het uitgangspunt geweest voor de gesprekken met interviewkandidaten. Daarnaast geeft de theorie een kader voor de benodigde rollen en mechanismen voor een goed werkende governance.

Volgens de Nederlandse Corporate Governance Code houdt governance het volgende in:

Governance gaat over besturen en beheersen, over verantwoordelijkheid en zeggenschap en over toezicht en verantwoording.[36]

Deze definitie geeft aan welke activiteiten (rollen) betrokken zijn in governance. Wat deze precies inhouden, blijkt echter niet uit te tekst.

Meer specifiek en gericht op publieke organisaties verwoordt De Toolbox Externe Governance (2006) wat de activiteiten en rollen in governance behelzen.

- **Sturen** is het richting geven aan een organisatie om de organisatiedoelstellingen te kunnen realiseren.
- **Beheersen** is met maatregelen zorgen dat de uitvoering volgens plan verloopt en zo nodig bijsturen.
- Het **toezicht** geeft een oordeel over de vraag of iets voldoet aan de gestelde eisen en zo niet, dan kan een interventie volgen.
- In de **verantwoording** geeft de organisatie belanghebbenden informatie over het behalen van de doelstellingen, de sturing en beheersing en het toezicht.

Het doel van sturing en beheersing is om als organisatie de eigen doelen te behalen. In het geval van scholen in het primair en voortgezet onderwijs, is er een wettelijk kader voor deze doelen: de Onderwijswet. Hier moeten alle scholen in het primair-en voortgezet onderwijs zich aan houden. Daar houdt een extern toezichthouder toezicht op (de Inspectie van het Onderwijs).

Volgens de Kaderstellende visie op toezicht (2005, p.3), heeft toezicht verschillende doelen:

Toezicht bevordert naleving van normen door regels te handhaven. Toezicht levert informatie over de kwaliteit van publieke taken door zelfstandige organisaties. Toezicht informeert minister, parlement en samenleving over praktijkontwikkelingen en de effecten van beleid. Toezicht ondersteunt de ministeriële verantwoordelijkheid en heeft een maatschappelijke functie.

Tot slot gaat governance over verantwoording. Dat houdt in dat de organisatie belanghebbenden voldoende informatie geeft, zodat ze kunnen beoordelen of de organisatie zijn doelen behaalt en of de sturing, beheersing en het toezicht ze voldoende vertrouwen geeft over het presteren van de organisatie. (Toolbox 2009, p.12-13)

Organisaties moeten zich aan wet- en regelgeving houden. Toezicht bevordert de naleving en informeert stakeholders daarover. Maar je kunt er ook op andere manieren dan met toezicht voor zorgen dat organisaties zich aan de regels houden. Bijvoorbeeld met zelfregulering:

Zelfregulering houdt in dat maatschappelijke partijen in bepaalde mate zelf verantwoordelijkheid nemen voor het opstellen en/of uitvoeren en/of handhaven van regels, indien nodig binnen een wettelijk kader. (…) [G]*econditioneerde zelfregulering* [betekent dat] *de overheid* (…) *een doel*

[36] Bron: Nederlandse Corporate Governance Code, 2022 pg. 5.

[stelt] *en* (…) *daarbij gebruik*[maakt] *van het middel zelfregulering. Bij zuivere overheidsregulering of wetgeving stelt de overheid een doel en stelt tevens ook de middelen vast om tot het gestelde doel te komen en zorgt daarbij voor toezicht en handhaving.* (Baarsma e.a., 2004, p.8)

Uit hetzelfde onderzoek (Baarsma e.a., 2004, p.6) komt naar voren dat zelfregulering een kostenvoordeel heeft ten opzichte van overheidsregulering: *Dit geldt zeker indien 100 procent naleving (volledige effectiviteit) niet noodzakelijk is om publieke belangen op een acceptabele wijze te borgen; wetgeving is dan vaak een duur alternatief, omdat de nalevingskosten veelal hoger zijn dan bij zelfregulering.*

De andere kant van dit verhaal is dat *de kosten van metatoezicht een kostenpost* [vormen] *in het nadeel van zelfregulering. Hiermee wordt gedoeld op de kosten die de overheid moet maken om de sector van afstand in de gaten te houden; in het geval van wetgeving is de overheid direct betrokken en is er (veel) minder noodzaak tot dergelijke algemene alertheid van de kant van de overheid.* (p.11)

Er speelt echter meer dan alleen een kostenafweging in de keuze voor toezicht of zelfregulering. Om zelfregulering tot een succes te maken, is een van de vereisten dat de sector aan drie randvoorwaarden voldoet, aldus Baarsma e.a. (2003, p.6):

- *Er moet een bepaald niveau van kennis aanwezig zijn binnen de sector.*
- *Er moet draagvlak zijn binnen de sector.*
- *De organisatiegraad van de betrokken branche/beroepsgroep moet 'voldoende' zijn.*

Daarnaast kan een stimulerende rol van de overheid wenselijk, en soms noodzakelijk, zijn.

Literatuur:

Bovens, M. en T. Schillemans (2009): Publieke verantwoording: begrippen, vormen en beoordelingskaders. In: Bovens, M. en T. Schillemans, 2009, Handboek publieke verantwoording. Den Haag: Lemma, p. 19 – 34

Baarsma, B., C. Koopmans, J. Mulder, M. de Nooij, C. Zijderveld (2004): Goed(koop) geregeld: Een kosten-baten analyse van wetgeving en zelfregulering. Stichting voor Economisch Onderzoek, Amsterdam

Baarsma, B., Felsö, F., Geffen, S. van, Mulder, J., Oostdijk, A. (2003): Zelf doen? Inventarisatiestudie van zelfreguleringsinstrumenten. Stichting voor Economisch Onderzoek, Amsterdam

Bijlage (2) Nadere informatie Nulmeting

In dit onderzoek is gekeken naar de mate waarin schoolbesturen voldoen aan tenminste 'Volwassenheidsniveau 3': wat inhoudt dat *'beheersingsmaatregelen zijn gedocumenteerd en op gestructureerde en geformaliseerde wijze worden uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst'.*

Uit een lijst van 60 aanmeldingen door schoolbesturen is een selectie van 15 schoolbesturen gemaakt. Het gaat om een gevarieerde, nationale steekproef met spreiding op: omvang van het schoolbestuur, onderwijssectoren: PO, VO, (V)SO en geografische ligging.

De doelstelling van het onderzoek richt zich op:
A. Algemeen beeld: **nulmeting** van het IBP-beleid en de -praktijk bij schoolbesturen met een **verschillen analyse** tussen dat beeld (huidige situatie) en de gewenste norm.
B. Duiding van de **belangrijkste obstakels, uitdagingen en ondersteuningsbehoefte** van schoolbesturen bij het implementeren van het Normenkader.

A: Algemeen beeld IBP-Beleid en IBP-Praktijk met verschillen analyse:

Koplopers (beschikken over beleid en praktijk) (~10%).

Het schoolbestuur heeft een gestructureerde en geformaliseerde uitvoering van de beveiliging van informatie; de beheersmaatregelen zijn vastgelegd in beleid en er binnen het bestuur voldoende expertise en capaciteit beschikbaar is om de beheersmaatregelen uit te voeren.

Uitvoerders (beschikken over praktijk zonder beleid) (~25%).

Dit zijn de besturen waarbij een hoge mate van IBP-expertise aanwezig is, gecentreerd bij een kleine groep, maar die vanwege een laag IBP-bewustwording in de breedte van de organisatie niet voldoen aan de norm.

Denkers (beschikken over beleid zonder praktijk) (~25%).

Het type schoolbestuur dat een hoge mate van bewustwording heeft over het belang van IBP; dit wordt vaak veroorzaakt doordat de organisatie een incident heeft meegemaakt. De noodzaak van IBP is daarom evident, maar vanwege de lage mate van expertise komt men in de praktijk niet tot een gestructureerde uitvoering van de beheersmaatregelen omdat er simpelweg te weinig kennis aanwezig is.

Achterblijvers (beschikken niet over beleid of praktijk) (~40%).
Deze besturen zijn onbewust onbekwaam, omdat bij hen zowel het bewustwording als de expertise op het vlak van IBP ontbreekt. In de praktijk zijn dit veelal kleine schoolbesturen die aangeven dat het inrichten van informatiebeveiliging kannibaliserend zou zijn voor het geven van onderwijs.

<u>Thema's incl. alle statements gerelateerd aan scores op volwassenheidsniveau 3:</u>
1. Beleid en Organisatie: scoort **0%** van de schoolbesturen.
2. Personeel, Studenten en Gasten: scoort **7%** van de schoolbesturen.
3. Ruimte en Apparatuur: scoort **13%** van de schoolbesturen.
4. Continuïteit: scoort **20%** van de schoolbesturen. Drie schoolbesturen halen daarmee volledig het genormeerde niveau.
5. Toegangsbeveiliging en Integriteit: scoort **20%** van de schoolbesturen. Drie schoolbesturen halen daarmee volledig het genormeerde niveau.
6. Controle en Logging: scoort **7%** van de schoolbesturen. Eén enkel schoolbestuur haalt dus volledig het genormeerde niveau.

Overall:
In de steekproef van schoolbesturen voldeed **geen enkel schoolbestuur** aan het gewenste niveau van de getoetste onderdelen uit het Normenkader in nulmeting.

De basis op orde
Voor het op orde brengen van de basis zijn de volgende domeinen van belang: Bestuur, Organisatie, Incident/Problem Management, Change Management, Datamanagement, Fysieke Beveiliging (beveiligingsmaatregelen) en Bedrijfs-continuïteitsmanagement.

Bij de domeinen Organisatie, Datamanagement en Fysieke Beveiliging voldoen het minste schoolbesturen aan de norm. Op deze domeinen dient dus de meeste additionele inspanning van schoolbesturen plaats te vinden om de basis op het vlak van informatiebeveiliging op orde te hebben.

B: Obstakels, uitdagingen en ondersteuningsbehoefte

Drie thema's werden door respondenten als meest prangend ervaren, namelijk:
1. **Bewustwording.** Het gebrek hieraan bij zowel bestuurders als het onderwijspersoneel heeft een negatief effect op de implementatie van het Normenkader. Bij bestuurders wordt gedoeld op het besef dat informatiebeveiliging, en het mitigeren van risico's op dit vlak, essentieel is voor de bedrijfsvoering van een schoolbestuur. Een lage mate van bewustwording bij onderwijspersoneel kan resulteren in het niet uitvoeren van beheersmaatregelen.
2. **Expertise.** Dit gaat om technische, juridische en beleidsmatige expertise en het ontbreken van deze kennis speelt het sterkst bij schoolbesturen waarbij de IBP-rollen niet worden uitgevoerd door experts, maar 'regulier' onderwijspersoneel.
3. **Capaciteit.** Het gebrek aan (interne en externe) capaciteit beschikbaar voor IBP is ook een belangrijk obstakel. Een tekort hangt in de praktijk vaak samen met de vrees dat het vrijmaken van capaciteit voor IBP conflicteert met de uitvoering van het reguliere onderwijs.

Ondersteuningsbehoefte op basis van de onder A vermelde archetypes: Koplopers (ca. 10%), Uitvoerders (ca. 25%), Denkers (ca. 25%) en Achterblijvers (ca. 40%) geeft de Nulmeting een koppeling met de verwachte ondersteunings-behoefte op domeinniveau per archetype. Verder is een nadere specificering aangebracht naar welke van de domeinen belangrijk zijn voor het op orde krijgen van de basis en het mitigeren van de hoge risico's.

Bijlage (3) Interne Governance bij FO

School A: Grote school (21.000 leerlingen)

Interne Organisatie:
De bestuurlijke leiding ligt bij de Raad van Bestuur (RvB) die bestaat uit een voorzitter en een lid van de RvB.

De Raad van Toezicht (RvT) bestaat uit zeven leden (onder wie een voorzitter en een vicevoorzitter). Twee leden van de RvT hebben kennis van IBP.

De RvB en de RvT leggen beiden verantwoording af aan de ledenvergadering.

Bij de directieraad is weinig kennis van de complexiteit van ICT-voorzieningen en de focus ligt op het primaire proces, niet wetende dat ICT-onderdeel is van dit primaire proces. In het leiderschapsprogramma pakt de school dit op.

Het bestuur is eindverantwoordelijk en hoort IBP te beleggen. Concern control of de IT-auditor heeft een rol in het beoordelen van de cybersecurity.
Deze rollen moeten in de concernstaf onafhankelijk van de uitvoering van IBP worden belegd. Functiescheiding aanbrengen is belangrijk om als bestuurder je verantwoordelijkheid te kunnen nemen: het '4-ogen-principe' binnen en buiten de organisatie, moet goed geregeld zijn.

Geld dat voor IBP wordt gereserveerd, passeert de Ouderraad en de Medezeggen-schapsraad. Daar leeft de perceptie dat het geld niet naar het onderwijs gaat, indirect is dat echter wel zo.

De school kent IBP-ers en een FG. De school heeft een gemeenschappelijke Privacy Officer (PO) op verenigingsniveau en binnen de scholengroepen.
Privacy-incidenten meldt de school bij de PO die feedback geeft over mitigatie, daarna gaat de melding door naar het AVG-bureau. Incidenten gaan via de directeur van de Shared Service Organisatie naar het bestuur. De concern-controller geeft een second opinion.

IT-organisatie:

De school heeft een eigen ondersteuningsbureau waar ongeveer 100 medewerkers werkzaam zijn binnen de SSO en concernstaf (directe medewerkers RvB). Deze medewerkers ondersteunen de scholen van onder meer met systeembeheer/ICT.

De IT-afdeling is drie jaar geleden gecentraliseerd, daarvoor werd gewerkt met verschillende IT-systemen. Centralisatie ligt moeilijk in het onderwijs: het gevoel leeft dat de autonomie wordt afgepakt. Scholen kunnen het op het gebied van IBP niet alleen doen. Een groot deel van IBP wordt uitgevoerd door een SSO: medewerkers daarvan ondersteunen de school op allerlei gebieden, waaronder IT. Op de IT-afdeling is de IT- en informatie-architectuur belegd en daar worden de technische maatregelen voor het IBP-kader opgepakt.

Verantwoording & Toezicht

In de overleggen met de Raad van Toezicht (RvT) is IBP een agendapunt. De RvT treedt 'supporting' op en daagt uit, neemt niet de rol van 'politieagent' aan, maar probeert mee te denken, te sparren en geeft advies.

De school verricht self-assessments op het gebied van IBP. Vier keer per jaar heeft de school intern overleg over de inrichting van de organisatie en het risicomanagement waar IBP, onderdeel van is.

De school verantwoordt zich over IBP in het jaarverslag en kent een uitgebreid Planning & Controlsysteem. De informatievoorziening verloopt via een vast format door gesprekken van het bestuur met de directeuren, waarbij de directeuren spreken met de hoofden per vestiging. Het primaire proces is onder meer onderwerp van gesprek.
De informatie uit die gesprekken neemt de school op in het Jaarverslag. Business Control controleert de informatie.

De afgelopen jaren is het IBP/AVG-beleid gecontroleerd tijdens de accountantscontrole. Onderdeel van deze controle zijn de processen en procedures in het kader van de IBP/AVG. De school voldoet in de basis aan de wet- en regelgeving in het kader van IBP/AVG, en kan op basis daarvan doorgroeien in volwassenheidsniveau.

School B: Middelgrote school 4.500 leerlingen

Interne Organisatie:

De RvB bestaat uit twee leden onder wie een voorzitter.
De RvT bestaat uit vijf leden onder wie een voorzitter en een vicevoorzitter.

De school kent een Gemeenschappelijke Medezeggenschapsraad.

De RvT bestaat uit portefeuillehouders voor HR, Financiën, Onderwijs etc. Er zijn geen leden die diepgaande IT-kennis hebben. Inrichting en de aanpak van toezicht is niet vastomlijnd is/niet voorgeschreven volgens de school.

In totaal spreken RvT en de RvB elkaar tien keer per jaar. De RvT neemt beslissingen onafhankelijk van de RvB. De RvB rapporteert zelf over IT en ervaart dat opmerkingen van de RvT het bestuur goed bij de les houdt en dat het de RvB scherp houdt door commissievergaderingen (vanuit een breder perspectief).
Binnen een expertgroep bedrijfsvoering wordt nieuw beleid vanuit het Normenkader besproken en geaccordeerd en vervolgens voorgelegd aan het directeurenoverleg als voorgenomen beleid. De RvB stelt na bespreking binnen de Medezeggen-schapsraad deze documenten vast.

De school maakt gebruik van een FG die in dienst is van drie besturen en slechts 1 tot 2 keer per week voor betrokken school werkt. Dit werkt op basis van een abonnement waarbij betrokkene 24/7 te bereiken is.

IT-organisatie:

De school beschikt over een Stafbureau met 13 medewerkers.
Eén medewerker binnen dit Stafbureau is volledig voor IT werkzaam en vervult eveneens de rol van PO, manager/verantwoordelijke IBP en Security Officer.

Het Functioneel beheer wordt in onderlinge afstemming vormgegeven, hiervoor is niet maar één medewerker verantwoordelijk. Vanuit de gezamenlijke informatiebehoefte specificeert de school wat er nodig is. De rol van Informatiemanager is verdeeld over SO, FB en ICT en de FG: zij bepalen welke informatie nodig is. Het ICT-beheer is bij drie partijen ondergebracht.

De IT-medewerker bepaalt samen met een aantal ICT-ambassadeurs binnen de school de inhoud van de ICT-werkplaatsen waarin goodpractices, ICT leerkracht- en leerling vaardigheden, privacy en beveiliging, onderhoud en beheer van devices worden behandeld.

Als een leerkracht een app wil installeren, moet deze dat melden bij de IT-medewerker en de FG. Als de app veilig is volgens de App-checker van de school, wordt deze binnen de beveiligde omgeving opgenomen. Alleen daarin opgenomen apps mogen worden gebruikt. Downloaden van apps/programma's op de C-schijf is niet mogelijk/toegestaan en betrokkene wordt aangesproken als dat toch gebeurt.

Het IBP Plan van de school kent een datalek procedure. Bij een vermoeden van een datalek wordt contact gelegd met de IT-medewerker, die meestal in overleg met de FG bepaalt of melding bij de AP nodig is.

Een keuze voor een ondersteunende tool voor IBP heeft de school nog niet gemaakt. De school maakt gebruik van zelf ontwikkelde excel sheets voor het verwerkingsregister en autorisaties.

Verantwoording & Toezicht

De school verantwoordt zich over IBP in het jaarverslag. De voorzitter van de RvB stelt een Veiligheidsverslag op met daarin thema's als fysieke, sociale en digitale veiligheid. Het veiligheidsverslag is veel breder dan de tekst in het jaarverslag (waarin een samenvatting kent van het veiligheidsverslag). Nadere vragen hierover kunnen worden gericht aan de scholen: de verantwoordelijkheid ligt bij het bestuur.

Een audit op het Normenkader wordt door Kennisnet aangeboden: 'deepdives'. Het is de bedoeling dat je daarmee een duidelijk beeld krijgt van waar je staat. De school heeft nog in overweging om deze audit via Kennisnet te laten uitvoeren of via een andere partij een audit/toets laat uitvoeren.

De school geeft aan dat de accountant controleert, een verslag en een actualiteitenlijst (toekomstgericht) opstelt die inhoudelijk niet over IBP gaan. De expertise van de accountant ligt niet bij deze thema's.
Thema's worden met de RvT en de RvB besproken in het kader van de verantwoording en bij bespreking van de bevindingen van de accountant.

School C: Kleine school 520 leerlingen

Interne Organisatie:
De RvB bestaat uit zes leden: er is een uitvoerend deel (één lid) en een toezichthoudend deel (vijf leden) van de RvB.
Alle bestuursleden gezamenlijk vormen het bestuur van de vereniging.

De vijf toezichthoudende bestuurders zijn ouders die IBP moeten kunnen begrijpen, zij zijn heel kritisch en laten zich regelmatig scholen: een aantal van hen heeft achtergrondkennis over ICT. Echter het zijn en blijven goedwillende vrijwilligers en geen technologen.
In de basis vragen toezichthoudende bestuursleden aan het uitvoerend bestuurslid hoe het nou werkt, zodat ze er kritisch over kunnen meedenken. Het is niet zo dat onderling regelmatig wordt gesproken over IBP. Als dat de bedoeling is dan daar een format voor moeten komen volgens de school.

Aanvullende scholing voor de toezichthoudende bestuursleden wordt door een partij verzorgd, die besturen van kleine scholen ondersteunt en het bestuur begeleidt in hun ontwikkeling rond toezicht en toezichthouden. Het opleidingsaanbod bevat echter geen IBP. De school acht het goed om dergelijke partijen te betrekken bij de ontwikkeling van een wijze waarop ook dit IBP-thema aan bod komt.

De school kent een vereniging waaraan de RvB verantwoording aflegt tijdens de ALV. Ouders van leerlingen zijn tegelijkertijd lid van de vereniging.

De school maakt nog geen gebruik van FG-as-a-service maar gaat dat wel doen.

IT-organisatie:

Deze school beschikt over een 'ICT-clubje' dat bestaat uit leerkrachten en waar het onderwerp IBP op de agenda staat. Dat is een punt van zorg: ICT zou zo maar een dagtaak kunnen zijn. Deze leerkrachten zijn nu o.a. bezig met, hoe kun je leerkrachten leren wat two-factor-authentication is, met de implementatie van beveiligd mailen en met een tweede cloud opslag.

De school geeft een voorbeeld van een leverancier van leermiddelen, inrichting en ICT voor onderwijs, kinderopvang en zorg. Deze partij beheert het netwerk en weet wat de school gebruikt en wat er nodig is om het veilig te gebruiken.
Diezelfde partij bekijkt vanuit het Normenkader wat deze kan doen om vanuit zijn rol te voldoen aan het kader.

Verantwoording & Toezicht

De school voert geen zelfevaluaties uit. Als een dergelijke zelfevaluatie echter ontwikkeld zou worden en toepasbaar zou zijn, dan zou de school die gebruiken.

De school heeft in de risicoparagraaf van het jaarverslag expliciet opgenomen dat IBP een aandachtsgebied is.

De school is niet regelmatig in gesprek met toezichthouders over IBP. Als dat de bedoeling zou zijn, dan zou daar een format voor moeten komen zo stelt de school.

Bij de accountantsonderzoeken gaan de meest kritische vragen over financiën en over wat je hebt gedaan als school. Over IBP zegt de accountant niets en stelt daar ook geen vragen over.

Bijlage (4) Geïnterviewde stakeholders

PO-Raad
Is de sectorvereniging voor het primair onderwijs (PO) en behartigt de belangen van de schoolorganisaties in het basisonderwijs, speciaal basisonderwijs en (voortgezet) speciaal onderwijs.
Gesproken met: voorzitter PO-Raad.

VO-Raad
Is de vereniging van scholen in het voortgezet onderwijs (VO). De raad behartigt de belangen van het voortgezet onderwijs bij overheid, politiek, bedrijfsleven en maatschappelijke organisaties.
Gesproken met: vice-voorzitter VO-Raad.

PO- en VO-Raad treden op als één team en hebben een adviesfunctie aan de opdrachtgever. De Raden dragen bij aan draagvlak onder hun leden en aan bewustwording en professionalisering van bestuurders en schoolleiders.

Kennisnet
Kennisnet ondersteunt scholen bij een professionele inzet van ICT en zorgt ervoor dat technologie wordt benut om de kwaliteit en toegankelijkheid van het onderwijs te verbeteren en om veiligheids- en ICT-risico's te beheersen.
Kennisnet heeft drie rollen:

- Expert en gids voor scholen en besturen die keuzes moeten maken over de inzet van ICT.
- Ontwikkelaar en dienstverlener van publieke ICT-voorzieningen.
- Keten- en Sectorarchitect van de (sectorale en boven sectorale) ICT-infrastructuur in het onderwijs.

Kennisnet adviseert de PO- en de VO-Raad.
Kennisnet wordt gefinancierd door het Ministerie van OCW
Kennisnet is geen coöperatie maar wordt door OCW gefinancierd en biedt ook diensten aan, aan derden buiten de sectorleden.
Gesproken met: directeur-bestuurder Kennisnet en een MT-lid Kennisnet.

SIVON
SIVON helpt scholen bij het realiseren en doorontwikkelen van veilig en toekomstig digitaal onderwijs, nu en in de toekomst. SIVON adviseert, ontzorgt en behartigt de belangen van scholen, zodat die zich kunnen richten op hun primaire taak: het verzorgen van het allerbeste onderwijs.

- SIVON vertegenwoordigt de belangen van het onderwijs in onderhandeling met leveranciers en techbedrijven.
- Geeft advies, ontzorgt en faciliteert kennisdeling voor ieder kennisniveau
- Levert hoogwaardige dienstverlening en infrastructuur

SIVON adviseert de opdrachtgever:

- Gezien de tussenpositie die SIVON inneemt tussen marktpartijen en schoolbesturen, en
- Gezien de vertaling die SIVON kan maken tussen behoefte van het onderwijs en concrete dienstverlening.

SIVON is een coöperatie van onderwijsbesturen in het PO en VO.
SIVON (PO/VO) is lid is van SURF (HO)
Gesproken met: voorzitter SIVON en een Programmamanager SIVON.

SURF
SURF werd in 1986 opgericht 'Samenwerkende Universitaire RekenFaciliteiten' en is verder gegroeid aan de hand van ontwikkelingen op het gebied van aanbestedingen, benutten schaalvoordelen etc.

SURF is nu een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen waarin de leden hun krachten bundelen. Binnen SURF werken universiteiten, hogescholen, MBO-instellingen, UMC's en onderzoeksinstellingen samen om de best mogelijke digitale diensten in te kopen of te ontwikkelen en om kennisdeling te stimuleren door steeds te blijven innoveren.

SURF bestaat al zo'n 37 jaar is door de leden opgericht: zij zijn ook eigenaar.
SURF wordt gefinancierd door haar leden.
Gesproken met: lid RvB SURF en Productmanager SURF.

Edu

Edu-Standaard:
Edu-Standaard ontzorgt scholen met standaarden voor informatie-uitwisseling tussen onderwijsinstellingen, DUO, OCW en leveranciers.
De Standaardisatieraad vormt het bestuurlijk orgaan van Edustandaard.
Dit is de Standaardisatieraad die scholen ontzorgt met standaarden voor informatie-uitwisseling tussen onderwijsinstellingen, DUO, OCW en leveranciers.
Edu-Standaard is aangesloten op de Informatiekamer van OCW en daarmee afgestemd op de wet- en regelgeving van de overheid. De Informatiekamer is het gremium waarin de overheid en het onderwijs op strategisch en bestuurlijk niveau met elkaar spreken over vraagstukken die voortvloeien uit toegenomen digitalisering, data hoeveelheid en datastromen. De Datakamer is het voorportaal van de informatiekamer en het gremium voor meer tactische vraagstukken op hetzelfde terrein.

Edu-K:
Een samenwerking van de PO-Raad, de VO-Raad, de MBO-Raad en het ministerie OCW, brancheorganisaties voor educatieve uitgevers, distribiteurs en softwareleveranciers. Deze entiteit is door de publiek-private samenwerkende keten (scholen en leveranciers van digitale leermiddelen) al in 2011 in het leven geroepen.
Kennisnet was oprichter en penvoerder van Edu-K.
Edu-K is opdrachtgever van Edu-V en wordt op termijn ook Edu-V.

Edu-V:
Is een programma en in feite de voortzetting van Edu-K inclusief alles om de governance en handhaving te regelen en partijen beter te binden. Doelstelling is om op één plek de regie te organiseren en om het toezicht op afspraken te regelen. Momenteel is het programma Edu-V twee jaar operationeel. Er zijn vijf technisch-inhoudelijke werkgroepen en een aantal werkgroepleden uit zowel de publieke als private organisaties: dus zowel vanuit leveranciers en vanuit scholen.

De stichting Edu-V wordt niet 'de baas', maar het is wel het punt waar alles bij elkaar komt en beoogt voor de verschillende partijen in de leermiddelenketen de regierol helder en duidelijk te beleggen.
Dezelfde partijen als in Edu-K en Edu-V zitten in Edu-Standaard.
Gesproken met: gedelegeerd opdrachtgever en een Programmamanager Edu-V.

CERT (Computer Emergency Response Team)
Voor het Funderend Onderwijs is dit in oprichting binnen Kennisnet.
Het gaat over een gespecialiseerd team van ICT-professionals dat beveiligingsincidenten oplost.
Gesproken met: Kwartiermaker CERT (Kennisnet) en Adviseur Kennisnet.

Inspectie van het Onderwijs

Houdt toezicht op de kwaliteit van onderwijs en of scholen en opleidingen voldoen aan wet- en regelgeving en hun financiën op orde hebben. De onderwijsbesturen zijn hiervoor verantwoordelijk: het toezicht begint en eindigt bij hen.
Eens in de vierjaar wordt een uitgebreid onderzoek verricht bij ieder bestuur en zijn scholen: 'het vierjaarlijks onderzoek bestuur en scholen'. Vervolgtoezicht hangt af van de beoordeling die de inspectie geeft aan de kwaliteitszorg door het bestuur. Daarnaast wordt jaarlijks een analyse uitgevoerd op basis van de gegevens waarover de inspectie beschikt.
Met de Inspectie van het Onderwijs hebben we *twee afzonderlijke gesprekken* gevoerd: zowel met de Directie als met (financieel) inspecteurs.
Gesproken met:
- Directeur Toezicht Voortgezet Onderwijs Inspectie van het Onderwijs.
- Een Strategische Adviseur, twee Financieel Inspecteurs en een Inspecteur Hoger Onderwijs Inspectie van het Onderwijs.

Autoriteit Persoonsgegevens
Alle mensen hebben recht op bescherming van hun persoonsgegevens. Het is zelfs een grondrecht. De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die zich sterk maakt voor dit recht. En die zorgt dat iedereen zich aan de privacywetgeving houdt.
Gesproken met: twee inspecteurs Systeemtoezicht Autoriteit Persoonsgegevens.

VTOI-NVTK
VTOI-NVTK is hét platform dat alle toezichthouders uit de sectoren kinderopvang en onderwijs bij elkaar brengt. Samen vormen ze een levende vereniging. Zij geven het toezichthouderschap een stem en maken zich hard voor de continuïteit en kwaliteit van de ontwikkeling van iedereen!
VTOI-NVTK vertegenwoordigt intern toezichthouders uit de sectoren kinderopvang en onderwijs.

De VTOI-NVTK is ontstaan uit twee verenigingen: de VTOI en de NVTK:
De Vereniging voor Toezichthouders van Onderwijs Instellingen is opgericht in 2002. Het doel was en is het versterken van de positie van de intern toezichthouder in het onderwijs; door te professionaliseren, adviseren, ondersteunen en te informeren.
De Nederlandse Vereniging voor Toezichthouders in de Kinderopvang is ontstaan in 2007 ook met als doel de kwaliteit van het intern toezicht in de sector kinderopvang naar een hoger plan te tillen.
Gesproken met: Senior Beleidsadviseur VTOI-NVTK

NBA (Koninklijk Nederlandse Beroepsorganisatie van Accountants)
Is de beroepsorganisatie van de accountants in Nederland.
De organisatie is ontstaan uit een fusie van het Nederlands Instituut van Registeraccountants (NIVRA) en de Nederlandse Orde van Accountants-Administratieconsulenten (NOvAA).
Gesproken met: Coördinator Publieke Sector bij NBA.

Daarnaast hebben we gesprekken gevoerd met:
- medewerkers van het **Ministerie van VWS** in het kader van hun kennis van de governance inrichting op het Normenkader IB bij de Zorg.
Gesproken met: MT-lid I-Beleid en een Coördinerend Beleidsmedewerker.
- medewerkers van het **Ministerie van OCW** in het kader van hun kennis over de governance inrichting op het Normenkader IB in het Hoger Onderwijs.
Gesproken met: een manager en twee Senior Beleidsmedewerkers.

- **drie scholen uit het Primair en Voortgezet Onderwijs** om hun ervaringen en suggesties te delen in het kader van de in te richten governance op het Normenkader IBP bij het Funderend Onderwijs.
Gesproken met: 1. Bestuurslid, Staffunctionaris ICT en Hoofd Financiën, 2. Voorzitter van de Raad van Bestuur en 3. Algemeen directeur/Bestuurder.

Bijlage (5) Overeenkomsten en verschillen tussen de Zorg, het HO en het FO

Governance Rollen	Zorg	HO	FO
Eigenaar	Veld	Veld	N.t.b.
Beheerder	NEN met veld	SURF met veld	N.t.b.
Toezichthouder	IGJ	Geen	N.t.b.
CERT	Z-CERT	SURFcert	CERT i.o.
Facilitator	VWS	SURF	N.t.b.
Formele vastlegging governance-inrichting?	Nee	Nee	N.t.b.
Vastlegging norm in wetgeving	Ja	Nee	N.t.b.
Andere thema's	**Zorg**	**HO**	**FO**
Start Normenkader	2004 -Verplicht sinds 2008	2015 -(Tot 2019 werd de ISO-norm voor IB gebruikt)	2023
IB of IBP?	IB	IB -P is in ontwikkeling	IB -P is in ontwikkeling
Organisatiegraad	Niet onderzocht	Al het bekostigd HO is aangesloten bij koepels en SURF	98% besturen VO en 89% besturen PO lid van koepels. 70% besturen VO en 23% besturen PO lid van SIVON
Lerend vermogen	Lijkt bij grotere instellingen ingebed in organisatie-structuur	Lijkt ingebed in SURF- en organisatiestructuur	Lijkt alleen mogelijk bij grotere instellingen
Urgentiegevoel	Onder meer op basis van mogelijke imagoschade	Onder meer op basis van mogelijke imagoschade	Lijkt vooral aanwezig bij instellingen die een incident hebben meegemaakt

Bijlage (6) Visiebrief Minister OCW aan Tweede Kamer

060723
visiebrief-digitaliserin

Kamerstukken II 2022/23, 36200-VIII nr.251

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00