dialogic
innovatie • interactie

Nulmeting IBP-normenkader voor het Funderend Onderwijs

Onderzoekers
Guido de Moor MSc MA
dr. Max Kemman
Melvin Hanswijk MSc LLM
Niels Nederlof MA

Opdrachtgevers:
Programma Digitaal Veilig Onderwijs

Publicatienummer:
2023.014-2315

Datum:
Utrecht, juni 2023

Inhoudsopgave

Managementsamenvatting

In opdracht van het programma Digitaal Veilig Onderwijs (DVO) 'Bit by bit' heeft Dialogic een nulmeting uitgevoerd naar de stand van zaken op het vlak van informatiebeveiliging in het funderend onderwijs aan de hand van het Normenkader IBP FO. Naast de nulmeting is zijn ook de obstakels en uitdagingen in kaart gebracht bij dit nieuwe normenkader. Voor dit onderzoek is een gevarieerde, nationale steekproef gemaakt van 15 schoolbesturen met spreiding naar sector, grootte en geografische spreiding. Deze schoolbesturen hebben een vragenlijst ingevuld en zijn geïnterviewd.

Tabel 1 toont de belangrijkste uitkomsten van de nulmeting. In de steekproef van schoolbesturen voldeed **geen enkel schoolbestuur** aan het gewenste niveau van de getoetste onderdelen uit het normenkader in nulmeting.

Tabel 1 Uitsplitsing percentages per domein naar omvang schoolbesturen (Domein 8: Systeemontwikkeling bleek voor ~85% van de schoolbesturen in de steekproef niet van toepassing)

Domeinen	Percentage besturen dat norm haalt (n=15)
1: Bestuur	27%
2: Organisatie	13%
3: Risicomanagement	20%
4: Personeelsbeheer	7%
5: Configuration Management	27%
6: Incident/Problem Management	47%
7: Change Management	27%
8: Systeemontwikkeling	N.V.T.
9: Datamanagement	13%
10: Identity & Access Management	27%
11: Security Management	7%
12: Fysieke Beveiliging	13%
13: IT-operatie	27%
14: Bedrijfscontinuïteitsmanagement	20%
15: Ketenbeheer	13%

De belangrijkste tekortkomingen van schoolbesturen ten opzichte van de norm zijn als volgt:

1. **Single points of failure.** De meeste verantwoordelijkheden en procedures ten aanzien van IBP zijn benoemd, maar we zien in de praktijk dat de uitvoering afhankelijk is van een kleine groep individuen binnen een schoolbestuur. Omdat de werkprocessen vaak niet gedocumenteerd zijn, resulteert dit in de situatie dat de uitval van één individu grote gevolgen kan hebben voor de continuïteit van de uitvoering.
2. **Bewustwording.** De respondenten geven aan dat op het vlak van bewustwording rondom IBP bij zowel bestuurders als onderwijspersoneel nog grote stappen gezet dienen te worden. Dit gebrek aan awareness heeft op dit moment een negatief effect op de naleving van beheersmaatregelen.
3. **Continuïteit.** Bij het grootste gedeelte van de respondenten is er naast een procedure voor het melden van incidenten geen crisis- of herstelplan opgesteld. Hierdoor is het zeer de vraag of schoolbesturen tijdens een groot incident de normale

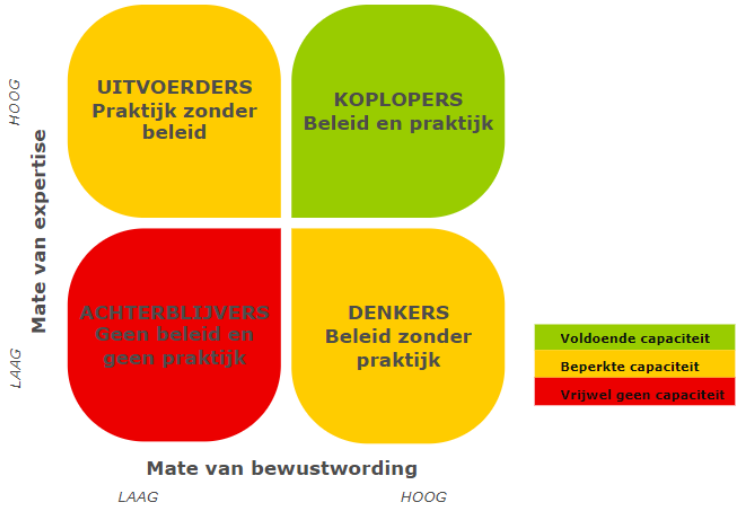
bedrijfsvoering kunnen doorzetten. Ook regelmatige tests met het terugzetten van back-ups worden door het merendeel van de schoolbesturen niet uitgevoerd.

4. **Monitoring en logging.** Op basis van deze steekproef kan gesteld worden dat er vaak geen specifiek beleid opgesteld is wat betreft monitoring en logbestanden. Hierdoor wordt er geen gebruik gemaakt van informatie om incidenten preventief te detecteren en te voorkomen.
5. **Leveranciersmanagement.** We zien dat de meeste schoolbesturen hun eigen beleid niet vertalen in aanvullende eisen boven op de standaardovereenkomsten van leveranciers. Als reden wordt gegeven dat het als individueel schoolbestuur lastig onderhandelen is, terwijl bijvoorbeeld op het vlak van back-ups en het beheer van toegangsrechten de standaardovereenkomst van een leverancier niet voldoet aan het opgestelde beleid.

Ten aanzien van de gepercipieerde obstakels en uitdagingen voor schoolbesturen bij het implementeren van het normenkader zijn er drie thema's die door respondenten als het meest prangend werden ervaren:

1. **Bewustwording.** Zowel het gebrek aan bewustwording bij bestuurders als het onderwijspersoneel heeft een negatief effect op de implementatie van het normenkader. Wanneer we het hebben over bewustwording bij bestuurders doelen we op het besef dat informatiebeveiliging, en het mitigeren van risico's op dit vlak, essentieel is de bedrijfsvoering van een schoolbestuur. Een lage mate van bewustwording bij onderwijspersoneel kan resulteren in het niet uitvoeren van beheersmaatregelen.
2. **Expertise.** Het gebrek aan expertise wordt vaak genoemd als een belangrijk obstakel. 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 die beschikbaar is voor IBP is ook een belangrijk obstakel. Een tekort aan beschikbare capaciteit hangt in de praktijk vaak samen met de vrees dat het vrijmaken van capaciteit voor IBP conflicteert met de uitvoering van het reguliere onderwijs.

Voor het bepalen van de ondersteuningsbehoefte is het handig om schoolbesturen op te delen in categorieën van gelijksoortige behoeftes qua ondersteuning. Op basis van de nulmeting en de drie belangrijksten obstakels en uitdagingen voor schoolbesturen zijn er een viertal archetypische schoolbesturen gevisualiseerd in de onderstaande figuur.



Figuur 1 Matrix met archetypische schoolbesturen met percentage aandeel in gehele populatie

- **Koplopers (~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 (~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 (~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 (~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.

Voor de toekomstige implementatie van het normenkader en ondersteuning vanuit het Programma DVO richting schoolbesturen zijn de volgende drie aandachtspunten van belang:

1. **Beschikbaar stellen van audit-tooling voor schoolbesturen.** Uit dit onderzoek blijkt dat schoolbesturen moeite hebben om zelfstandig een nulmeting ten aanzien van het normenkader. Het programma DVO moet aandacht besteden aan het ondersteunen van deze schoolbesturen, want de nulmeting is de basis voor verdere implementatie van het normenkader. Ondersteuning van schoolbesturen is mogelijk door het beschikbaar te stellen van een laagdrempelige methodiek aan schoolbesturen, zodat men zelfstandig een interne audit kunnen uitvoeren.
2. **Integreren in toetsingskader IBP FO**. Bij de ontwikkeling van een methodiek of tooling voor een zelfstandige audit dient DVO te overwegen om de verschillende NBA Volwassenheidsniveaus te integreren in het Toetsingskader IBP FO. Dit stelt schoolbesturen namelijk in staat om hun voortgang gedetailleerder te monitoren. Deze actie kan opgepakt worden binnen de programmalijn *Sturen op basis van normen* waar de doorontwikkeling van het toetsingskader is belegd.
3. **Een duidelijk zichtbaar ondersteuningsaanbod dat aansluit op de behoeften van scholen.** We stellen op basis van de gesprekken met schoolbesturen vast dat bestaande ondersteuningsmogelijkheden, zoals bijvoorbeeld het Template IBP-beleidsplan en de prioritering binnen het normenkader via de 'Voorlopige starttabel', vaak niet bekend zijn bij de doelgroep. Daarom is het van belang om het duidelijk te communiceren over ondersteuningsmogelijkheden, zowel bij bestaande hulpverlening als ondersteuningsaanbod dat nog ontwikkeld dient te worden.

1 Introductie

In opdracht van het programma Digitaal Veilig Onderwijs (DVO) 'Bit by bit' heeft Dialogic innovatie & interactie een nulmeting uitgevoerd naar de stand van zaken op het vlak van informatiebeveiliging in het funderend onderwijs. De aanleiding van deze nulmeting is de introductie van het nieuwe normenkader voor IBP in het funderend onderwijs. Binnen de nulmeting is er ook een analyse uitgevoerd naar de belangrijkste obstakels, uitdagingen en ondersteuningsbehoefte van schoolbesturen ten aanzien van de implementatie van het normenkader. Hieronder bespreken wij eerst de achtergrond en aanleiding van het IBP FO normenkader (paragraaf 1.1). Daarna behandelen we doelstelling van het onderzoek en de hieruit volgende onderzoeksvragen (paragraaf 1.2). Vervolgens bespreken we de onderzoeksmethode die gebruikt is om tot een beantwoording van de onderzoeksvragen te komen (paragraaf 1.3). Tot slot bevat dit hoofdstuk een leeswijzer voor de rest van het rapport (paragraaf 1.4).

1.1 Introductie IBP FO normenkader

Het programma Digitaal Veilig Onderwijs (DVO)[1] is opgestart in 2023 (en heeft een looptijd tot en met 2027) om de digitale veiligheid van het funderend onderwijs in Nederland te verhogen. In dit programma werken het Ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-Raad samen om scholen te ondersteunen om stappen te zetten naar een digitaal veilige leeromgeving voor alle leerlingen in het funderend onderwijs. Het programma richt zich op het aanpakken van verschillende aspecten van digitale veiligheid, waaronder informatiebeveiliging en privacy. De Adviesgroep Regie op ICT van de PO-Raad en de VO-raad heeft vorig jaar opgeroepen tot minimale normen voor informatiebeveiliging en privacy om zo naar een basisnorm toe te werken in de hele sector.[2] OCW investeert structureel 6 miljoen euro om de digitale veiligheid in het primair en voorgezet onderwijs naar een hoger niveau te tillen.[3] Hiertoe is er onder andere een normenkader ontwikkeld voor scholen. Ook wordt er geïnvesteerd in bewustwording, professionalisering en centrale ondersteuning. De overheid kiest voor een meer centrale regie waarbij gestuurd gaat worden op normen. Ook komt er ondersteuning voor de schoolbesturen om aan de normen te voldoen.

Het Normenkader informatiebeveiliging en privacy voor het Funderend Onderwijs[4] (IBP FO) is normstellend voor scholen om stapsgewijs tot een digitaal veilige schoolomgeving te komen. Hierbij valt bijvoorbeeld te denken aan het op vertrouwelijke wijze verwerken en beveiligen van gegevens van leerlingen, ouders en medewerkers. Schoolbesturen en hun medewerkers zijn hier verantwoordelijk voor. Het IBP FO-normenkader biedt de schoolbesturen een gestructureerde aanpak om hun informatiebeveiliging en privacybeheer te verbeteren en te voldoen aan de wet- en regelgeving op dit gebied. Het is een set van normen en voorbeeldmaatregelen die speciaal ontwikkeld is voor instellingen in het funderend onderwijs.

Het normenkader IBP FO bestaat uit twee delen, het eerste deel gaat specifiek over informatiebeveiliging en het tweede deel over privacy. Het kader informatiebeveiliging bevat vijftien domeinen. In Tabel 2 staan deze domeinen benoemd.

---

[1] [digitaalveiligonderwijs.nl]

[2] [poraad.nl]

[3] [voraad.nl]

[4] [aanpakibp.kennisnet.nl]

Domeinen Normenkader IBP FO
Domein 1: Bestuur
Domein 2: Organisatie
Domein 3: Risicomanagement
Domein 4: Personeelsbeheer
Domein 5: Configuration Management
Domein 6: Incident/Problem Management
Domein 7: Change Management
Domein 8: Systeemontwikkeling
Domein 9: Datamanagement
Domein 10: Identity & Access Management
Domein 11: Security Management
Domein 12: Fysieke Beveiliging
Domein 13: IT-operatie
Domein 14: Bedrijfscontinuïteitsmanagement
Domein 15: Ketenbeheer

Tabel 2 De 15 domeinen van het Normenkader IBP FO

Deze vijftien domeinen kennen allemaal een aantal normen. Elke norm wordt kort beschreven in het normenkader en wijst schoolbesturen op de belangrijkste aandachtspunten met betrekking tot informatiebeveiliging. Daarnaast staat er per norm een aantal concrete voorbeelden beschreven om de aandachtspunten inzichtelijk te maken en zijn ook voorbeeldmaatregelen opgenomen. Het normenkader is een 'levend document' dat regelmatig geactualiseerd wordt om te blijven voldoen aan de veranderende wet- en regelgeving en de nieuwste kennis en ontwikkelingen.

De vastgestelde normen voor informatiebeveiliging komen overeen met het derde volwassenheidsniveau uit het Volwassenheidsmodel informatiebeveiliging.[5] Het volwassenheidsmodel heeft als doel om auditors en directies van organisaties een leidraad en handvatten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging.

In onderstaande tabel zijn de vijf verschillende niveaus binnen het volwassenheidsmodel benoemd en toegelicht. Niveau 3 Uitgebreide werking is dikgedrukt weergegeven, omdat dit niveau als het gewenste niveau voor het Normenkader IBP FO is vastgesteld. In dit onderzoek kijken we daarom alleen naar de mate waarin schoolbesturen voldoen aan tenminste volwassenheidsniveau 3.

[5] [nba.nl]

Volwassenheidsniveau		Toelichting
1	Ad hoc	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.
2	Opzet, bestaan en beperkte werking	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.
3	**Uitgebreide werking**	**Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.**
4	PDCA	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.
5	Externe goedkeurende verklaring	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.

Tabel 3 Volwassenheidsmodel Informatiebeveiliging

Voor privacy is binnen het funderend onderwijs een dergelijk normenkader nog niet opgesteld, de verwachting is dat het Programma DVO in de tweede helft van 2023 wordt opgeleverd. Aangezien de normen voor privacy nog in ontwikkeling zijn, valt privacy buiten de scope van dit onderzoek. Verschillende IBP-normen over gegevensbescherming raken echter óók aan privacy, waardoor dit aspect ten dele terugkomt in de nulmeting. Hier gaan we in paragraaf 1.3.3 verder op in.

1.2 Doelstelling van het onderzoek

De doelstelling van het onderzoek is drieledig en richt zich op 1) een algemeen beeld dat kan dienen als **nulmeting** van het IBP-beleid en -praktijk van schoolbesturen, 2) een **verschilanalyse** tussen dat beeld van de huidige situatie en de gewenste norm en 3) een duiding van de belangrijkste obstakels, uitdagingen en ondersteuningsbehoefte van schoolbesturen ten aanzien van het implementeren van het normenkader. Deze driedeling levert de volgende onderzoeksvragen op:

1. *Wat is het huidige niveau van informatiebeveiliging en privacy bij schoolbesturen in het funderend onderwijs?*
    a. *Wat zijn de verschillen tussen schoolbesturen op het vlak van informatiebeveiliging en privacy?*
    b. *Welke variabelen hebben impact op de het IBP-beleid van schoolbesturen?*
2. *Hoe verschilt de huidige staat van informatiebeveiliging en privacy met de gewenste normen uit het IBP-normenkader voor het funderend onderwijs?*
3. *Op welke facetten van het IBP-normenkader zien schoolbesturen de meeste obstakels en uitdagingen voor zichzelf?*
4. *Hoe kan de ondersteuning van de schoolbesturen op deze facetten worden vormgegeven?*

De inhoud van de eerste twee onderzoeksvragen en bijbehorende deelvragen komen aan bod bij de nulmeting in Hoofdstuk 2 en de laatste twee onderzoeksvragen worden behandeld in Hoofdstuk 3. In Hoofdstuk 4 zal er een concreet antwoord op de onderzoeksvragen worden gegeven.

1.3 Onderzoeksopzet

In deze paragraaf wordt de methodologie van het onderzoek besproken waarmee we tot beantwoording van de onderzoeksvragen komen. De verschillende onderdelen van de onderzoeksopzet zullen hieronder apart worden toegelicht: het opstellen van de steekproef, de oriënterende vragenlijst en interviews voor de nulmeting en de duiding van de belangrijkste obstakels, uitdagingen en ondersteuningsbehoefte van schoolbesturen.

1.3.1 Opstellen van de steekproef

Om tot een valide beantwoording van de onderzoeksvragen te komen is het van belang om de variëteit tussen schoolbesturen in het funderend onderwijs te ondervangen in het onderzoek. De schoolbesturen in het funderend onderwijs zijn bijvoorbeeld erg verschillend van elkaar in termen van omvang. Zo zijn er 83 schoolbesturen in het primair onderwijs waarbij 20 of meer basisscholen zijn aangesloten, maar zijn er ook 365 schoolbesturen waar maar één school onder valt.

Bij de start van het onderzoek is aan schoolbesturen verzocht of ze wilden deelnemen aan het onderzoek. Deze uitvraag heeft plaatsgevonden via verschillende kanalen, waaronder het Netwerk IBP, de ledenlijst van SIVON en de Adviesgroep Regie op ICT. Vervolgens is uit een lijst van 60 aanmeldingen een selectie van 15 schoolbesturen samengesteld. Deze 15 besturen vormen een gevarieerde, nationale steekproef met spreiding op een aantal dimensies, te weten de omvang van het schoolbestuur (het aantal vestigingen dat onder het schoolbestuur valt), de onderwijssector(en) waarin het bestuur actief is (po, vo, (v)so) en geografische ligging. Zie in de onderstaande Tabel 4 de indeling van de steekproef naar omvang van de schoolbesturen.

Omvang schoolbestuur	Definitie	Aantal in steekproef
Klein	1 t/m 4 instellingen onder bestuur	3
Middel	5 t/m 20 instellingen onder bestuur	6
Groot	Meer dan 20 instellingen onder bestuur	6

Tabel 4 Steekproef indeling naar omvang van schoolbestuur

Om een vergelijking te kunnen maken tussen het funderend onderwijs als geheel en de steekproef is in Tabel 5 een overzicht opgenomen van het aantal instellingen, met uitsplitsing naar onderwijssector, en leerlingen opgenomen.

Variabele	Funderend onderwijs	Steekproef
Aantal instellingen	**8.031**	**290**
• Aantal PO	6056	214
• Aantal VO	1450	40
• Aantal (V)SO	525	36
Aantal leerlingen	**~2.400.000**	**~80.000**

Tabel 5 Vergelijking funderend onderwijs[6] en steekproef

De geografische spreiding van schoolbesturen in de steekproef is weergegeven in Figuur 2.

[6] De cijfers ten aanzien van het funderend onderwijs zijn afkomstig van ocwincijfers.nl

Figuur 2 Kaart met geografische spreiding schoolbesturen

1.3.2 Oriënterende vragenlijst

De geselecteerde respondenten hebben een oriënterende vragenlijst toegestuurd gekregen. Deze vragenlijst bestond uit de 15 domeinen van het normenkader met per domein een aantal stellingen die corresponderen met een bepaald 'volwassenheidsniveau' voor dit onderdeel. Hiermee konden schoolbesturen laagdrempelig een inschatting maken van de stand van zaken op het vlak van IBP binnen het bestuur. De vragenlijst is opgenomen in Bijlage 2 van dit rapport.

Deze vragenlijst is gebruikt vanwege verschillende redenen. Allereerst was voorafgaand aan het onderzoek de verwachting dat de inhoud van het normenkader voor (een deel van) de schoolbesturen onderdelen bevat waar individuen buiten het bestuur zicht op hebben, bijvoorbeeld voor de technische onderdelen van het normenkader. De vragenlijst was daarmee voor de schoolbesturen een middel om intern navraag te doen bij de personen bij wie deze kennis aanwezig is. Deze individuen konden vervolgens aanschuiven bij het interview waarin de daadwerkelijke nulmeting wordt uitgevoerd. De vragenlijst was daarmee een middel om te borgen dat bij het interview de juiste respondenten aanwezig waren.

Daarnaast is de vragenlijst ingezet om de respondenten op de vijftien domeinen van het normenkader voorafgaand aan het interview een interne analyse uit te voeren ten behoeve van de nulmeting. De uitkomsten van de vragenlijst vormden het startpunt voor het interview waarin de uitkomsten gezamenlijk met de respondenten zijn gevalideerd. We hebben op detailniveau met de respondenten de status quo omtrent IBP in kaart gebracht en op deze wijze is getracht de validiteit van de nulmeting binnen dit onderzoek te waarborgen.

1.3.3 Interviews

Met de 15 schoolbesturen zijn interviews afgenomen waarin een tweeledige opzet is gehanteerd: (1) valideren van de uitkomsten van de vragenlijst en het vaststellen van de nulmeting en (2) reflecteren op de belangrijkste obstakels en uitdagingen ten aanzien van de implementatie van het normenkader op schoolbesturen anderzijds. Deze twee separate doelstellingen worden hieronder toegelicht.

Nulmeting

De uitkomsten van de vragenlijst zijn bij de interviews gevalideerd op basis van statements uit het (NBA) Toetsingskader Informatiebeveiliging IBPDOC3.[7] Dit toetsingskader is ontwikkeld voor het mbo, maar verschilt inhoudelijk niets van het normenkader IBP Funderend Onderwijs. Daarbij is het normenkader IBP FO nog niet geoperationaliseerd in bespreekbare stellingen en bovendien nog binair; een schoolbestuur kan alleen voldoen of niet voldoen aan een bepaalde norm. Het Toetsingskader Informatiebeveiliging IBPDOC3 is daarentegen wél geoperationaliseerd in bespreekbare stellingen, waarbij ook de volwassenheidsniveaus 1-5 zijn toegelicht. Omdat het voor de nulmeting van belang is dat schoolbesturen kunnen reflecteren op hun niveau ten opzichte van de vastgestelde norm, hebben we in dit onderzoek gebruik gemaakt van dit Toetsingskader. Op deze manier konden wij gestructureerd bepalen hoever de besturen van het gewenste volwassenheidsniveau 3 vandaan zitten en welke stappen zij moeten ondernemen om aan het gewenste niveau te voldoen.

Het toetsingskader bevat 101 statements. Het was binnen dit onderzoek niet haalbaar om deze allemaal met de besturen te behandelen. In totaal zijn uit de 101 statements van het toetsingskader 27 statements geselecteerd, om een werkbaar maar zo volledig mogelijk beeld op te halen. Zoals eerder benoemd is de scope van het onderzoek inhoudelijk beperkt tot informatiebeveiliging, omdat de normen voor het FO voor privacy nog niet ontwikkeld zijn, maar een aantal van de geselecteerde statements raakt ook aan gegevensbescherming ten behoeve van privacy. Zodoende kijken we ook vooruit naar privacy.

De 27 statement zijn onder te verdelen in zes clusters (zie Tabel 6). Langs de lijnen van deze clusters worden in Hoofdstuk 2 de uitkomsten van de nulmeting uitgelicht. Deze clusters zijn afkomstig uit de benchmark IBP-E,[8] die voor het eerst in 2015 binnen de mbo-sector is uitgevoerd.

Clusters
Beleid en Organisatie
Personeel, Studenten en Gasten
Ruimte en Apparatuur
Continuïteit
Toegangsbeveiliging en Integriteit
Controle en Logging

Tabel 6 Zes clusters uit het IBPDOC3 Toetsingskader

[7] [mbodigitaal.nl]

[8] [mbodigitaal.nl]

De relatie tussen de bovenstaande clusters en de domeinen van de het IBP FO normenkader is weergeven in de tabel in Bijlage 3.

Duiding van belangrijkste obstakels, uitdagingen en ondersteuningsbehoefte schoolbesturen

De tweede helft van het interview is gebruikt voor de bespreking van onderzoeksvragen 3 en 4. De respondenten hebben, mede op basis van de nulmeting binnen het eigen schoolbestuur, gereflecteerd op wat voor hen de belangrijkste obstakels en uitdagingen zijn voor het voldoen aan het normenkader. Vervolgens is besproken welke ondersteuning mogelijk en gewenst is voor het verhelpen van deze obstakels en uitdagingen.

1.4 Leeswijzer

In Hoofdstuk 2 van deze rapportage worden de uitkomsten van de nulmeting nader beschreven. Hierin wordt de actuele stand van zaken op het vlak van IBP in het funderend onderwijs toegelicht. Daarnaast wordt er ingegaan op welke stappen er noodzakelijk zijn voor het behalen van het gewenste volwassenheidsniveau 3. In Hoofdstuk 3 wordt ingegaan op de meest voorkomende obstakels en uitdagingen. Ook bespreken we mogelijke vormen van ondersteuning bij het overkomen van deze obstakels en uitdagingen. Tenslotte wordt deze rapportage in Hoofdstuk 4 afgesloten met de beantwoording van de onderzoeksvragen en conclusies op basis van de voorgaande hoofdstukken.

2 Nulmeting

In dit hoofdstuk gaan we in op de uitkomsten van de nulmeting, waarin de stand van zaken op het vlak van IBP in het funderend onderwijs in kaart zijn gebracht. Zoals toegelicht in paragraaf 1.3.3 worden de uitkomsten geschetst op het niveau van de zes clusters.

2.1 Nulmeting per cluster

Hieronder wordt per cluster ingegaan op het vastgestelde **huidige volwassenheidsniveau**. De uitkomsten van de nulmeting worden gerapporteerd via de structuur die in Tabel 7 is weergegeven:

- De eerste kolom bevat het nummer van een statement uit het eerdergenoemde IBP-DOC3-toetsingskader. In dit geval is het eerste statement van cluster 1 als voorbeeld genomen. Het nummer is opgebouwd uit het clusternummer en een volgnummer.
- De tweede kolom bevat de titel van het statement.
- In de derde kolom is het percentage gegeven van de schoolbesturen dat minimaal Niveau 3 scoort op de beheersmaatregel uit het toetsingskader en daarmee voldoet aan de norm. Onderaan deze kolom wordt het percentage schoolbesturen getoond dat voldoet aan alle normen van het cluster.
- De kolommen Niveau 1, Niveau 2 en Niveau 3(+) tonen de verdeling van de aantallen geraadpleegde schoolbesturen voor de volwassenheidsniveaus. Niveau 3, 4 en 5 zijn samengevoegd in Niveau 3(+), omdat voor het behalen van de norm Niveau 3 voldoet.

Statement	Cluster 1: Beleid en Organisatie	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
1.1	**Beleidsregels voor informatiebeveiliging**	33%	2	8	5
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***33%***			

Tabel 7 Voorbeeldtabel voor de rapportage van de nulmeting per cluster

Daarnaast is per cluster een **verschilanalyse** gemaakt tussen het huidige niveau en het gewenste niveau. Daarbij wordt expliciet gekeken naar de benodigde stappen om het gewenste niveau te behalen.

2.1.1 Cluster 1: Beleid en Organisatie

Het eerste cluster, Beleid en Organisatie, gaat met name over de inrichting van beleidsmaatregelen. Deze normen geven richting en ondersteuning om de informatiebeveiliging in te richten in lijn met organisatie-doelstellingen, bij het vaststellen van procedures en verantwoordelijkheden en bij het uitoefenen van controle op leveranciers. Het cluster bevat daarmee belangrijke randvoorwaarden voor de invulling van de overige normen.

Nulmeting

In Tabel 8 zijn de uitkomsten van de nulmeting voor Cluster 1: Beleid en Organisatie weergegeven. We stellen het volgende vast:

- Op basis van de interviews blijkt het overgrote deel van het IBP-beleid opgesteld te zijn in 2018 bij de introductie van de AVG. Sindsdien is het gros van de beleidsdocumenten niet meer up-to-date gebracht en controle op de naleving van de

maatregelen is vaak niet georganiseerd. Dit levert de situatie op dat er voor diverse onderdelen wel beleidsmaatregelen zijn geformuleerd, maar dat uitvoering van deze maatregelen toch als inconsistent en/of informeel bestempeld moet worden (zie scores bij statement 1.1 in Tabel 7).

- In het geval van een informatiebeveiligingsincident zijn (management)verantwoordelijkheden en -procedures vaak wel benoemd, maar afhankelijk van een beperkt aantal individuen die voor een breed scala aan onderwerpen verantwoordelijk zijn. Dit leidt in de praktijk tot potentiële *single points of failure* en conflicterende taken die de kans op risico van toevallig of opzettelijk misbruik vergroten (zie scores bij statements 1.17 en 1.21 in Tabel 7).
- Het merendeel van de respondenten maakt op dit moment geen gebruik van een classificatiemethodiek, zoals de (BIV-)classificatie of het ROSA-classificatiemodel, om de gevoeligheid en het belang van bepaalde informatie te duiden. Classificeren van informatie vindt in de praktijk vaak plaats op basis van individuele expertise. Hierdoor is het vaak niet vast te stellen of de beveiligingsmaatregelen in lijn zijn met de eisen die de organisatie stelt voor informatie van die desbetreffende classificatie (zie scores bij statements 1.7 en 1.14 in Tabel 7).
- Op het vlak van IBP-beleid gericht op leveranciersmanagement en ketenbeheer hebben met name de kleinere besturen geen extra beveiligingsaspecten afgedwongen in de overeenkomsten (SaaS, SLA, NDA) met leveranciers. Vaak wordt bij de overeenkomst de leverancier gevolgd in plaats van dat schoolbesturen op basis van opgesteld beleid zelf hun eisen richting de leverancier formuleren. Verwerkersovereenkomsten zijn in vrijwel alle gevallen wel afgesloten (zie scores bij statements 1.15 en 1.16 in Tabel 7).

Statement	Cluster 1: Beleid en Organisatie	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
1.1	Beleidsregels voor informatiebeveiliging	33%	2	8	5
1.7	Classificatie van informatie	20%	9	3	3
1.14	Analyse en specificatie van informatiebeveiligingseisen	20%	5	7	3
1.15	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	20%	3	9	3
1.16	Toeleveringsketen van informatie- en communicatietechnologie	27%	1	10	4
1.17	Verantwoordelijkheden en procedures	20%	2	10	3
1.18	Rapportage van informatiebeveiligingsgebeurtenissen	47%	1	7	7
1.21	Scheiding van taken	27%	4	7	4
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***0%***			

Tabel 8 Uitkomsten van de nulmeting voor Cluster 1: Beleid en Organisatie

Over het hele cluster genomen scoort **0%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **geen enkel schoolbestuur** haalt dus volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 gelden de volgende aandachtspunten:

- Het *up-to-date* brengen van het in de praktijk vaak verouderde IBP-beleid. Een aantal (kleinere) schoolbesturen geeft aan dat dit als een uitdaging wordt gezien, omdat bestuurders niet afdoende zicht hebben op welke componenten er in een IBP-

beleidsstuk meegenomen dienen te worden. Deze doelgroep kan gebruik maken van het Template IBP-beleidsplan[9] van Kennisnet.

- Voor een geformaliseerde en gestructureerde respons op incidenten is het raadzaam om instructies te formuleren, zodat men minder afhankelijk is van individuen. Op deze manier kan het proces ook worden uitgevoerd als individuen wegvallen.
- De adaptatie van een informatie-classificatiemethodiek is noodzakelijk voor het verkrijgen van inzicht in de gevoeligheid en belang van informatie. Hier kan het Certificeringsschema informatiebeveiliging en privacy ROSA[10] voor worden gebruikt.
- Het opstellen van aanvullend IBP-beleid gericht op leveranciersmanagement. Momenteel volgen de schoolbesturen in de praktijk vaak de overeenkomsten die vanuit de leverancier worden opgesteld, zonder zelf extra beveiligingsaspecten aan de overeenkomsten toe te voegen. Kennisnet, SIVON, de PO-Raad en de VO-raad zijn nog bezig met de ontwikkeling van een Handreiking Leveranciersmanagement.

2.1.2 Cluster 2: Personeel, Studenten en Gasten

Het tweede cluster, Personeel, Studenten en Gasten, richt zich op de menselijke kant van informatiebeveiliging. Met name de bewustwording op het vlak van IBP speelt een belangrijke rol en ook de toekenning van (toegangs-)rechten en verantwoordelijkheden op functieniveau is een belangrijk onderdeel van dit cluster.

Nulmeting

In Tabel 9 zijn de uitkomsten van de nulmeting voor Cluster 2: Personeel, Studenten en Gasten weergegeven. We stellen het volgende vast:

- Hoewel het gros van de schoolbesturen trainingen, lezingen en e-learnings voor het stimuleren van bewustwording rondom informatiebeveiliging en privacy in het IBP-beleid hebben opgenomen, geven respondenten aan dat er op het vlak van bewustwording bij het onderwijspersoneel nog een wereld valt te winnen. Met name het naleven van alledaagse beheersmaatregelen, zoals bijvoorbeeld het uitvoeren van het 'clear desk- en 'clear screen'-beleid, loopt achter op de gewenste norm (zie scores bij statements 2.2 en 2.4 in Tabel 8).
- Op het vlak van toegangsrechten geven veel respondenten aan dat toegang tot systemen nog handmatig is ingeregeld. Dit zorgt in de praktijk voor een gebrek aan een actueel overzicht en vergroot het risico dat bij een functiewijziging de toegangsrechten niet worden ingetrokken of gewijzigd (zie score bij statement 2.3 in Tabel 8).

Statement	Cluster 2: Personeel, Studenten en Gasten	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	27%	5	6	4
2.3	**Toegangsrechten intrekken of aanpassen**	20%	4	8	3
2.4	**Clear desk'- en 'Clear screen'-beleid**	20%	3	9	3
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***7%***			

Tabel 9 Uitkomsten van de nulmeting voor Cluster 2: Personeel, Studenten en Gasten

[9] [kennisnet.nl]

[10] [edustandaard.nl]

Over het hele cluster genomen scoort **7%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **<u>één enkel schoolbestuur</u>** haalt dus volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 gelden de volgende aandachtspunten:

- De interne trainingen en opleidingen zijn momenteel vaak beschikbaar, maar ook nog vrijblijvend. Voor een vastgestelde en gestructureerde uitvoering van het beleid dienen de beheersmaatregelen instellingsbreed uniform te worden uitgevoerd. Dit is mogelijk door de trainingen periodiek en consequent uit te voeren en de voortgang te rapporteren aan de bestuurder.
- Het beheer van toegangsrechten is kwetsbaar als het handmatig door individuen wordt uitgevoerd. Een koppeling vanuit het HR-systeem aan andere applicaties maakt het mogelijk om op functieniveau het beheer te automatiseren. Deze maatregel zorgt ervoor dat na een wijziging van een functie, de toegangsrechten automatisch worden aangepast aan de nieuwe functie zonder dat daar een handmatige handeling aan ten grondslag hoeft te liggen.

2.1.3 Cluster 3: Ruimte en Apparatuur

Het derde cluster omvat ruimten en apparatuur en raakt daarmee aan de ICT binnen een schoolbestuur. De nadruk binnen dit cluster ligt op het bijhouden van informatie over de hard- en software en de toegang van individuen tot deze IT-componenten.

Nulmeting

In Tabel 10 zijn de uitkomsten van de nulmeting voor Cluster 3: Ruimte en Apparatuur weergegeven. We stellen het volgende vast:

- Op het vlak van (fysieke toegangs-) beveiliging van apparatuur op scholen is met de introductie van Cloud-gebaseerd werken een groot deel van de beveiliging van apparatuur afgevangen; server- en patchkasten zijn grotendeels uitgefaseerd. Hierdoor is de kans op incidenten verkleind, maar tegelijkertijd ontbreken bij veel schoolbesturen gestructureerde en geformaliseerde beheersmaatregelen op het vlak van fysieke toegang (zie score bij statement 3.4 in Tabel 9).
- Beleid voor verwijderen/hergebruiken apparatuur en up-to-date overzicht van de apparatuur en de bijbehorende gebruikers zijn daarentegen in veel gevallen wel formeel vastgelegd en controle op naleving vindt ook geregeld plaats. (zie scores bij statements 3.14 en 3.16 in Tabel 9).

<u>Cluster 3</u>	Cluster 3: Ruimte en Apparatuur	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
3.4	Fysieke toegangsbeveiliging	13%	6	7	2
3.14	Veilig verwijderen of hergebruiken van apparatuur	40%	3	6	6
3.16	Inventariseren van bedrijfsmiddelen	27%	4	7	4
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***13%***			

Tabel 10 Uitkomsten van de nulmeting voor Cluster 3: Ruimte en Apparatuur

Over het hele cluster genomen scoort **13%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **twee schoolbesturen** halen daarmee volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 gelden de volgende aandachtspunten:

- De meeste schoolbesturen hebben beleid opgesteld voor de fysieke toegangsbeveiliging, maar de naleving van dit beleid is in de praktijk vaak informeel. Zo is er tijdens de interviews herhaaldelijk aangegeven dat sleutels voor afgesloten ruimten toch worden uitgeleend aan (ongeautoriseerde) derden. Dit vraagt om gestructureerde en geformaliseerde uitvoering van beheersmaatregelen voor fysiek toegangsbeleid.
- Configuratiedatabases, zoals Topdesk, worden in toenemende mate gebruikt binnen het funderend onderwijs. Bij het actueel houden van deze overzichten is men afhankelijk van het onderwijspersoneel en tijdens de interviews is aangegeven dat de controle op de inventarisatie beter moet en kan. Periodieke controles, bijvoorbeeld middels steekproeven, helpen om de beheersmaatregelen te formaliseren.

2.1.4 Cluster 4: Continuïteit

Het vierde cluster richt zich op het borgen van de continuïteit van de bedrijfsvoering, met name ten aanzien van de ICT-infrastructuur. In de context van het onderwijs raakt dit aan het primaire proces van het verzorgen van onderwijs en het bekijken welke zaken randvoorwaardelijk zijn hiervoor.

Nulmeting

In Tabel 11 zijn de uitkomsten van de nulmeting voor vierder cluster ten aanzien van continuïteit weergegeven. We stellen het volgende vast:

- Ten aanzien van systeemontwikkeling, Domein 8 van het Normenkader, geven vrijwel alle respondenten aan dat deze norm niet van toepassing is op hun schoolbestuur. Softwareontwikkeling vindt namelijk niet plaats binnen de organisatie. Het gemiddelde voor dit statement is weergeven als "N.V.T" omdat slechts voor twee besturen een volwassenheidsniveau is vastgesteld (zie score bij statement 4.2 in Tabel 9).
- Op het vlak van back-ups geven meerdere respondenten aan dat met de leverancier overeengekomen is tot hoe ver back-ups teruggezet moeten kunnen worden, maar dat slechts zelden wordt getest met het terugzetten van de back-ups. Enkel na een incident wordt data opgevraagd en teruggeplaatst. Hierdoor wordt de effectiviteit van het beleid pas duidelijk in een crisissituatie (zie score bij statement 4.5 in Tabel 9).
- Een groot deel van de schoolbesturen heeft een methodiek voor de documentatie van informatiebeveiligingsincidenten. Ze worden hierbij ondersteunt door applicaties, zoals bijvoorbeeld Yoursafetynet, waarin incidenten gestructureerd kunnen worden geregistreerd (zie score bij statement 4.13 in Tabel 9).
- Een crisis- en/of herstelplan is bij de meeste schoolbesturen niet opgesteld; pas wanneer een incident plaatsvindt, wordt er met een select groepje gekeken hoe een probleem verholpen kan worden. Ook is vaak niet helder beschreven hoe de informatiebeveiligingscyclus kan blijven functioneren tijdens een incident. Als de mailserver er bijvoorbeeld uitligt, kunnen nieuwe incidenten vaak niet via een andere weg worden gemeld (zie score bij 4.14).

Statement	Cluster 4: Continuïteit	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
4.2	Scheiding van ontwikkel-, test- en productieomgevingen	N.V.T.			
4.5	Back-up van informatie	27%	8	3	4
4.13	Respons op informatiebeveiligingsincidenten	47%	2	6	7
4.14	Informatiebeveiligingscontinüiteit implementeren	20%	8	4	3
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***20%***			

Tabel 11 Uitkomsten van de nulmeting voor Cluster 4: Continuïteit

Over het hele cluster genomen scoort **20%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **drie schoolbesturen** halen daarmee volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 gelden de volgende aandachtspunten:

- Het formuleren van een crisis- en herstelplan waarin staat beschreven welke acties er worden ondernomen om de continuïteit van het onderwijsproces te borgen.
- Het toetsen van het beleid op continuïteit in de praktijk, door bijvoorbeeld een (OZON-)crisisoefening. Op deze manier kunnen beheersmaatregelen worden getoetst om de effectiviteit aan te tonen. Momenteel vinden dit soort toetsen, bijvoorbeeld op het gebied van back-ups, te weinig en ad hoc plaats.

2.1.5 Cluster 5: Toegangsbeveiliging en Integriteit

Het vijfde cluster, Toegangsbeveiliging en Integriteit, bevat beheersmaatregelen gericht op de toegang tot data (vertrouwelijkheid) en de integriteit ervan. De beheersmaatregelen zijn gericht op het classificeren van informatie, toegang tot systemen en wijzigingenbeheer.

Nulmeting

In Tabel 12 zijn de uitkomsten van de nulmeting voor Cluster 5: Toegangsbeleid en Integriteit weergegeven. We stellen het volgende vast:

- Vrijwel alle schoolbesturen hebben een toegangsbeleid gebaseerd op het 'least privilege'-principe waarbij men geen toegang heeft tot een systeem, tenzij dit vanuit het functieprofiel noodzakelijk is. Ook is bij het merendeel van de schoolbesturen een beleid op het gebruik van wachtwoorden ingevoerd en is twee-factor-authenticatie (2FA) in toenemende maat de standaard (zie scores bij statements 5.1, 5.7 en 5.8 in Tabel 11).
- Bij functiewijzigingen kan het voorkomen dat de toegangsrechten van een individu aangepast dienen te worden en, zoals besproken bij Cluster 2, worden deze wijzigingen momenteel grotendeels handmatig uitgevoerd. Dit vergroot het risico op fouten en de belasting op individuen (zie score bij statement 5.3 in Tabel 11).
- Op het vlak van wijzigingenbeheer is het grootste deel van de activiteiten uitbesteedt aan externe IT-leveranciers. Wijzigingen waarbij persoonsgegevens betrokken zijn behoeven extra aandacht, maar voor schoolbesturen is het vaak niet duidelijk hoe de leverancier te werk gaat. Daarentegen is het in toenemende mate het geval dat

er bij de inkoopvoorwaarden wordt gecontroleerd dat de leverancier gecertificeerd is op het vlak van IBP (zie score bij statement 5.27 in Tabel 11).

Statement	Cluster 5: Toegangsbeveiliging en Integriteit	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
5.1	Beleid voor toegangsbeveiliging	53%	1	6	8
5.3	Registratie en afmelden van gebruikers	40%	1	8	6
5.7	Geheime authenticatie-informatie gebruiken	53%	2	5	8
5.8	Beperking toegang tot informatie	33%	5	5	5
5.27	Bescherming van testgegevens	29%	6	4	4
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***20%***			

Tabel 12 Uitkomsten van de nulmeting voor Cluster 5: Toegangsbeveiliging en Integriteit

Over het hele cluster genomen scoort **20%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **drie schoolbesturen** halen daarmee volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 in de geselecteerde statements uit Cluster 5 zijn voor schoolbesturen de volgende aandachtspunten van belang:

- Het inregelen van (automatische) monitoring van toegangsrechten op gebruikersniveau. Zoals besproken bij Cluster 2 vergroot de handmatige toetsing van toegangsrechten door individuen het risico op fouten, met name bij functiewijzigingen. Daarom is het wenselijk om dit proces te automatiseren, bijvoorbeeld met een koppeling van het HR-systeem met andere applicaties.
- Het expliciteren van werkprocessen rondom wijzigingenbeheer bij de leverancier. Dit kan binnen de bestaande overeenkomsten, of via aanvullende overeenkomsten zoals een SLA. Op deze manier kunnen schoolbesturen vaststellen dat het wijzigingenbeheer, met name als hier persoonsgegevens bij betrokken zijn, verloopt via de standaarden uit het eigen beleid.

2.1.6 Cluster 6: Controle en Logging

Het laatste cluster gaat over controle en logging en bevat daarmee beheersmaatregelen gericht op de registratie van gebruikersacties in het systeem, alsook de naleving en aanpassing van deze maatregelen op basis van analyses op deze acties.

Nulmeting

In Tabel 13 zijn de uitkomsten van de nulmeting voor Cluster 6: Controle en Logging weergegeven. We stellen het volgende vast:

- Zoals eerder besproken heeft het gros van de schoolbesturen de toegangsrechten van systemen gekoppeld aan concrete functies. Daar worden veelal autorisatiematrices voor gebruikt, maar tijdens de interviews kwam naar voren dat de rollen van deze matrices niet altijd gekoppeld kunnen worden met de systemen van leveranciers. Een concreet voorbeeld dat genoemd werd is dat facilitair medewerkers de functie van leerkracht krijgen toegekend, omdat hun daadwerkelijke rol niet is opgenomen binnen een systeem (zie score bij statement 6.1 in Tabel 12).
- Concreet beleid op logbestanden is vaak niet vastgesteld door schoolbesturen; de logging is beschikbaar in de systemen, maar er zijn geen concrete eisen wat betreft

de inhoud van deze bestanden gedefinieerd. Er wordt dus gelogd, maar deze informatie wordt niet proactief ingezet om veiligheidsrisico's vroegtijdig op te sporen en te beperken (zie score bij statement 6.2 in Tabel 12).

- De naleving en beoordeling van het beveiligingsbeleid wordt uitgevoerd door een selecte groep individuen met beperkte capaciteit. De audits zijn vaak gericht op specifieke onderdelen van het beleid, zoals datalekken of toegangsrechten, maar een overkoepelende audit over het gehele beleid wordt vaak niet uitgevoerd. Gelet op de technische naleving worden er door een beperkt aantal besturen sporadisch penetratietesten of andere kwetsbaarheidsbeoordelingen op hardware en software uitgevoerd. Met name bij de kleinere besturen is er echter te weinig kennis beschikbaar voor de uitvoering van deze technische testen (zie scores bij statements 6.9 en 6.10 in Tabel 12).

Statement	Cluster 6: Controle en Logging	Percentage besturen dat voldoet aan norm	Niveau 1	Niveau 2	Niveau 3 (+)
6.1	Beoordeling van toegangsrechten van gebruikers	33%	4	6	5
6.2	Gebeurtenissen registeren	20%	7	5	3
6.9	Naleving van beveligingsbeleid en -normen	27%	5	6	4
6.10	Beoordeling van technische naleving	20%	8	4	3
	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements	***7%***			

Tabel 13 Uitkomsten van de nulmeting voor Cluster 6: Controle en Logging

Over het hele cluster genomen scoort **7%** van de schoolbesturen op alle statements minimaal volwassenheidsniveau 3; **<u>één enkel schoolbestuur</u>** haalt dus volledig het genormeerde niveau.

Verschilanalyse

Voor het behalen van het gewenste volwassenheidsniveau 3 gelden de volgende aandachtspunten:

- Het formuleren van concreet beleid op logbestanden kan helpen bij het vaststellen van duidelijke criteria over welke informatie in logbestanden dient te staan. Op deze manier kan de informatie uit de bestanden ook daadwerkelijk gebruikt worden om veiligheidsrisico's vroegtijdig op te sporen en te beperken.
- Het vergroten van de beschikbare capaciteit voor de controle op de naleving van beveiligingsbeleid. Wat betreft de technische naleving van het beleid, kan het wenselijk zijn om in contact te treden met leveranciers voor de technische controle wanneer de expertise op dit vlak niet binnen organisatie aanwezig is.

2.1.7 Conclusie

Voor een volledig overzicht van de nulmeting op clusterniveau zijn in Tabel 14 de percentages van schoolbesturen opgenomen die de norm halen op alle getoetste statements in een cluster. De 0% bij Cluster 1 t/m 6 geeft aan dat er in de nulmeting **<u>geen enkel schoolbestuur</u>** voldoet aan de norm voor alle getoetste statements.

Clusters	Percentage schoolbesturen dat Niveau 3 (+) haalt op alle statements
Cluster 1: Beleid en Organisatie	0%
Cluster 2: Personeel, Studenten en Gasten	7%
Cluster 3: Ruimte en Apparatuur	13%
Cluster 4: Continuïteit	20%
Cluster 5: Toegangsbeveiliging en Integriteit	20%
Cluster 6: Controle en Logging	7%
Cluster 1 t/m 6	**0%**

Tabel 14 Totaal overzicht nulmeting op clusterniveau

Bij Cluster 4: Continuïteit en Cluster 5: Toegangsbeveiliging en Integriteit is het percentage dat voldoet aan de norm het hoogste (20%). Bij Cluster 1: Beleid en Organisatie is dit percentage het laagst (0%), maar hierbij moet worden opgemerkt dat het aantal getoetste statements het hoogst was, namelijk acht. Hiermee is de kans groter dat een schoolbestuur niet voldoet aan tenminste één van de beheersmaatregelen.

2.2 Verdiepende analyse

In paragraaf 2.1 zijn de uitkomsten van de nulmeting binnen zes clusters beschreven en toegelicht. Dit gedeelte van de rapportage staat in het teken van verdiepende analyses en uitsplitsingen om de uitkomsten van de nulmeting verder te duiden.

2.2.1 Uitsplitsing naar omvang van schoolbesturen

In paragraaf 2.1 zijn de uitkomsten van de nulmeting weergegeven op het niveau van de zes clusters. Tabel 15 toont het percentage van de schoolbesturen dat voldoet aan de norm op het niveau van de 15 domeinen, met een uitsplitsing gemaakt naar de kleine, middelgrote en grote schoolbesturen.

Domeinen	Percentage kleine besturen dat norm haalt (n=3)	Percentage middelgrote besturen dat norm haalt (n=6)	Percentage grote besturen dat norm haalt (n=6)	**Totaal percentage besturen dat norm haalt (n=15)**
1: Bestuur	0%	50%	17%	**27%**
2: Organisatie	0%	0%	33%	**13%**
3: Risicomanagement	33%	0%	33%	**20%**
4: Personeelsbeheer	0%	0%	17%	**7%**
5: Configuration Management	67%	17%	17%	**27%**
6: Incident/Problem Management	33%	50%	50%	**47%**
7: Change Management	33%	33%	17%	**27%**
8: Systeemontwikkeling	N.V.T.	N.V.T.	N.V.T.	**N.V.T.**
9: Datamanagement	0%	17%	17%	**13%**
10: Identity & Access Management	33%	33%	17%	**27%**
11: Security Management	0%	17%	0%	**7%**
12: Fysieke Beveiliging	33%	17%	0%	**13%**
13: IT-operatie	33%	33%	17%	**27%**
14: Bedrijfscontinuïteitsmanagement	33%	33%	0%	**20%**
15: Ketenbeheer	0%	33%	0%	**13%**

Tabel 15 Uitsplitsing percentages per domein naar omvang schoolbesturen

Een analyse van de scores in Tabel 15 levert een aantal inzichten op. Allereerst geven schoolbesturen van verschillende omvang te kennen dat de normen uit Domein 8: Systeemontwikkeling niet van toepassing zijn op de bedrijfsvoering, aangezien de schoolbesturen binnen de steekproef geen softwareontwikkeling in eigen huis uitvoeren.

Voor de **kleine schoolbesturen** in de steekproef geldt dat de grootste verschillen ten opzichte van het totale gemiddelde gevonden worden in de domeinen Bestuur (1), Datamanagement (8) en Ketenbeheer (15). Op basis van de gesprekken blijkt dat de kleine schoolbesturen geen methodiek hanteren voor de classificatie van informatie. Hierdoor kan het juiste beschermingsniveau niet worden vastgesteld en dit ondermijnt het onderhouden van de volledigheid, beschikbaarheid, juistheid en de bescherming van gegevens. Tevens blijkt uit de gesprekken dat op het vlak van Ketenbeheer de kleine besturen minder controle hebben op de beveiligingsvereisten bij hun leveranciers. Zo worden er minder aanvullende afspraken gemaakt, in bijvoorbeeld SLA's, op basis van het eigen opstelde IBP-beleid. De kleinere besturen nemen veelal de beveiligingsvereisten van de leveranciers over.

Opvallende lagere scores zien we bij de **middelgrote schoolbesturen** in de domeinen Personeelsbeheer (4), Configuration Management (5) en Incident/Problem Management (6). De verklaring voor deze lagere scores is dat het voor de middelgrote schoolbesturen een uitdaging is om het opgestelde beleid consistent uit te voeren op instellingsniveau. Uit de gesprekken blijkt dat de middelgrote besturen meer moeten coördineren dan de kleine besturen, maar hiervoor minder middelen of capaciteit ter beschikking hebben dan de grote besturen. Dit biedt een mogelijke verklaring.

Gebrekkige uitvoering van opgesteld beleid op instellingsniveau uit zich bij Personeelsbeheer in bewustwordingstrainingen die niet regelmatig worden gegeven en in het niet tijdig intrekken van toegangsrechten na de wijziging of beëindiging van een functie. Daarnaast hebben middelgrote besturen in termen van Configuration Management op instellingsniveau in sommige gevallen gebrekkig zicht op bedrijfsmiddelen, omdat de inventarisatie niet *up-to-date* is. Tenslotte ziet men bij Incident/Problem Management dat er op instellingsniveau niet op informatiebeveiligingsincidenten wordt gereageerd in overeenstemming met de gedocumenteerde procedures. Dit blijkt onder andere uit grote verschillen tussen het aantal incidenten dat per instelling aan een bestuur wordt gerapporteerd.

Lagere scores bij de **grote schoolbesturen** die noemenswaardig zijn komen uit de domeinen Change Management (7) en Bedrijfscontinuïteitsmanagement (14). Zo bleek uit een aantal gesprekken dat grote besturen op het vlak van Change Management niet altijd heldere afspraken hebben met leveranciers over wijzigingenbeheer, of intern beleid hebben opgesteld over hoe wijzingen doorgevoerd dienen te worden. Hierdoor is het niet altijd vast te stellen dat wijzigingen op een gestructureerde en gestandaardiseerde wijze worden uitgevoerd. Bij Bedrijfscontinuïteitsmanagement zien we dat de helft van de grote schoolbesturen in de steekproef geen cybercrisis- of herstelplan heeft opgesteld. Daarnaast zijn oefeningen en simulaties op het vlak van (cyber-)crises eerder uitzondering dan regel, terwijl juist voor grote schoolbesturen de impact van een crisis bijzonder groot kan zijn.

2.2.2 Uitsplitsing naar verschillende sectoren binnen het funderend onderwijs

Naast de analyse van de omvang van schoolbesturen kunnen we ook uitsplitsen naar sectoren binnen het funderend onderwijs. Belangrijk hierbij is dat een schoolbestuur in meerdere onderwijssectoren actief kan zijn, dus de sectoren zijn niet wederzijds uitsluitend. Voor deze uitsplitsing is het dus niet mogelijk om soortgelijke tabellen te maken als bij de uitsplitsing naar omvang.

Uitbesteding van IT in het primair onderwijs

Op basis van de steekproef kan gesteld worden dat schoolbesturen in het primair onderwijs de IT in hoge mate hebben uitbesteed aan IT-leveranciers en slechts weinig beheer zelf uitvoeren. Het is voor schoolbesturen in het primair onderwijs dus van groot belang om solide ketenbeheer en leveranciersmanagement in te regelen ten behoeve van IBP. We

hebben echter in paragraaf 2.2.1 vastgesteld dat juist op het vlak van ketenbeheer de kleinere schoolbesturen lager scoren dan de grotere schoolbesturen. Dit hangt op bepaalde wijze samen met de hoge mate van het outsourcen van IT, waardoor bij schoolbesturen in het primair onderwijs ook intern minder kennis op het vlak van IT aanwezig is. Dit maakt het lastiger voor een bestuur om vast te stellen welke aanvullende eisen in de overeenkomsten met IT-leveranciers moeten worden opgenomen. In de praktijk worden daarom vaak de standaardovereenkomsten van de leverancier overgenomen.

In tegenstelling tot het primair onderwijs zien we bij schoolbesturen in het voortgezet onderwijs dat er vaak wel een interne IT-afdeling met een bepaalde mate van expertise aanwezig is. Dit heeft volgens respondenten een positief effect op het technische gedeelte van het IBP-beleid van een schoolbestuur, omdat men intern beter zicht heeft op welke vereisten op het vlak van IT van belang zijn.

Meer 'dreiging' vanuit leerlingen in het voortgezet onderwijs

Verschillende respondenten die actief zijn in het voortgezet onderwijs gaven aan dat de 'dreiging' vanuit leerlingen een belangrijke invloed heeft op het IBP-beleid van een bestuur. In meerdere interviews werd benoemd dat een significant deel van de incidenten door leerlingen wordt veroorzaakt. Zo zijn er voorbeelden genoemd van leerlingen die DDoS-aanvallen uitvoeren of wijzigingen doorvoeren op de laptop van een docent als deze niet vergrendeld wordt. Dit soort praktijken ziet men in het primair onderwijs in veel mindere mate terug. Schoolbesturen in het voortgezet onderwijs dienen zich hier bewust van te zijn om deze typen incidenten te voorkomen.

Informatie-uitwisseling met externe partijen in het speciaal onderwijs

In de steekproef zijn bewust schoolbesturen opgenomen die actief zijn in het (voorgezet) speciaal onderwijs om te onderzoeken of deze onderwijssector op een bepaalde wijze afwijkt van de overige sectoren binnen het funderend onderwijs. De respondenten hebben tijdens de gesprekken aangegeven dat dit niet noodzakelijkerwijs het geval is, maar dat er binnen het speciaal onderwijs wel sprake is van een hogere frequentie van informatie-uitwisseling met externe (zorg-)partijen. Hierdoor is het binnen het speciaal onderwijs van extra belang om het ketenbeheer (bijvoorbeeld in de vorm van verwerkersovereenkomsten) op orde te hebben.

2.2.3 Vergelijking met prioritering binnen normenkader

De eerder uitgelichte scores per domein schetsen een totaalbeeld van de stand van zaken op het vlak van IBP bij schoolbesturen, maar voor een individueel bestuur is het prettig om prioriteiten aan te brengen tussen de normen. Hierdoor kan een schoolbestuur aan de slag met concrete onderdelen binnen het normenkader. De Voorlopige starttabel van Kennisnet[11] heeft het normenkader opgedeeld in verschillende fases, zodat men eerst aan de slag kan met het op orde brengen van de basis en het mitigeren van de hoge risico's. Hieronder zullen we deze fases langs de uitkomsten van de nulmeting leggen om te zien hoe deze zich tot elkaar verhouden.

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 Bedrijfscontinuïteitsmanagement. In de

[11] [aanpakibp.kennisnet.nl]

onderstaande tabel is een selectie gemaakt van de percentages van schoolbesturen dat op deze domeinen de norm haalt.

Domeinen	Percentage kleine besturen dat norm haalt (n=3)	Percentage middelgrote besturen dat norm haalt (n=6)	Percentage grote besturen dat norm haalt (n=6)	**Totaal percentage besturen dat norm haalt (n=15)**
1: Bestuur	0%	50%	17%	**27%**
2: Organisatie	0%	0%	33%	**13%**
6: Incident/Problem Management	33%	50%	50%	**47%**
7: Change Management	33%	33%	17%	**27%**
9: Datamanagement	0%	17%	17%	**13%**
12: Fysieke Beveiliging	33%	17%	0%	**13%**
14: Bedrijfscontinuïteitsmanagement	33%	33%	0%	**20%**

Tabel 16 Percentage schoolbesturen dat aan de norm voldoet voor de 'basis op orde'-domeinen, uitgesplitst naar omvang van schoolbesturen

Duidelijk is dat het percentage besturen dat de norm haalt bij Incident/Problem Management met 47% het hoogst is. De helft van de middelgrote en grote schoolbesturen heeft de processen rondom het detecteren, melden en verhelpen van beveiligingsincidenten volgens de norm op orde; bij de kleine besturen ligt dit percentage met 33% net wat lager (al is daar door de lage *n* geen percentage tussen de 33 en 66 mogelijk).

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.

Mitigeren hoge risico's

Voor de mitigatie van de hoge risico's zijn de volgende onderdelen van belang: Risicomanagement, Personeelsbeheer (het veiligheidsbewustwording bij medewerkers en technisch veilige omgeving voor wijzingen), Identity en Access Management, Security Management (het beheer fysieke toegangsrechten), IT-operatie (back-up en herstel), Bedrijfscontinuïteitsmanagement en Leveranciersmanagement. In Tabel 17 is een selectie gemaakt van de percentages van schoolbesturen dat op deze domeinen de norm haalt. De tabel toont aan dat zelfs bij de domeinen met de hoogste scores hooguit een kwart van de besturen voldoet aan de norm. Hiermee heeft slechts een klein deel van de besturen de maatregelen genomen om de hoge risico's op het vlak van informatiebeveiliging te mitigeren.

Domeinen	Percentage kleine besturen dat norm haalt (n=3)	Percentage middelgrote besturen dat norm haalt (n=6)	Percentage grote besturen dat norm haalt (n=6)	**Totaal percentage besturen dat norm haalt (n=15)**
3: Risicomanagement	33%	0%	33%	**20%**
4: Personeelsbeheer	0%	0%	17%	**7%**
7: Change Management	33%	33%	17%	**27%**
8: Systeemontwikkeling	N.V.T.	N.V.T.	N.V.T.	**N.V.T.**
9: Datamanagement	0%	17%	17%	**13%**
10: Identity & Access Management	33%	33%	17%	**27%**
11: Security Management	0%	17%	0%	**7%**
12: Fysieke Beveiliging	33%	17%	0%	**13%**
13: IT-operatie	33%	33%	17%	**27%**
14: Bedrijfscontinuïteitsmanagement	33%	33%	0%	**20%**
15: Ketenbeheer	0%	33%	0%	**13%**

Tabel 17 Percentage schoolbesturen dat aan de norm voldoet voor de 'mitigeren hoge risico's'-domeinen, uitgesplitst naar omvang van schoolbesturen

Met name op het vlak van Personeelsbeheer en Security Management dient er een grote slag door de schoolbesturen te worden gemaakt; slechts 7% van de besturen haalt op deze domeinen de voorgeschreven norm. De voornaamste redenen hiervoor zijn reeds genoemd. Bij Personeelsbeheer zien we dat beleid t.a.v. awareness dat op bestuursniveau is geformuleerd op instellingsniveau vaak niet als zodanig wordt uitgevoerd. Daarnaast blijkt het proces rondom functiewijzingen in systemen foutgevoelig doordat het op basis van individueel handwerk plaatsvindt. Bij Security Management lopen schoolbesturen achter ten opzichte van de norm doordat het beleid op en processen rondom logging en monitoring niet zijn geformuleerd of in de praktijk inconsistent worden uitgevoerd. Daardoor kunnen besturen op dit gebied niet proactief sturen op het detecteren van risico's en een daarmee preventief incidenten voorkomen.

3 Obstakels en ondersteuning voor schoolbesturen

In dit hoofdstuk bespreken we de uitkomsten van de interviews ten aanzien van de obstakels en uitdagingen die schoolbesturen verwachten bij implementatie van het normenkader (paragraaf 3.1) en mogelijkheden voor ondersteuning bij deze obstakels en uitdagingen op het niveau van archetypische schoolbesturen (paragraaf 3.2).

3.1 Obstakels en uitdagingen

In dit deel wordt er ingegaan op obstakels en uitdagingen om aan het IBP-normenkader te voldoen. Dit doen we aan de hand van drie thema's die door respondenten als het meest prangend werden ervaren, namelijk bewustwording, expertise en capaciteit. Deze thema's zullen in de onderstaande paragrafen worden gekoppeld aan de domeinen uit het normenkader. Belangrijk om te vermelden is dat er bij de potentiële impact van het normenkader ook gedacht kan worden aan tweede en derde orde effecten, zoals het stijgen van ICT-kosten voor besturen door een hoog aantal noodzakelijke mitigaties in de systemen of aanpassingen van lerarenopleidingen om toekomstig personeel conform het normenkader onderwijs te geven. Dit type effecten wordt niet meegenomen in de nulmeting van Dialogic; dit onderzoek richt op het directe effect van het normenkader op schoolbesturen. Daarbij kijken we zoals gezegd naar obstakels en uitdagingen die schoolbesturen ervaren bij het implementeren van het normenkader en de verwachte ondersteuningsbehoefte die daaruit volgt.

3.1.1 Bewustwording

Bewustwording is een van de meest frequent terugkerende thema's in de interviews geweest. Het gaat dan met name om bewustwording bij bestuurders, maar ook het bewustwording van het onderwijspersoneel speelt een belangrijke rol. Wanneer we het hebben over bewustwording bij bestuurders doelen we op het besef dat informatiebeveiliging, en het mitigeren van risico's op dit vlak, essentieel zijn voor de bedrijfsvoering van een schoolbestuur. Wanneer dit besef niet aanwezig is zien we dat terug in lagere volwassenheidsniveaus bij Domein 1: Bestuur, Domein 3: Risicomanagement en Domein 14: Bedrijfscontinuïteitsmanagement. Volgens respondenten komt het nog te veel voor dat bestuurders risico's gerelateerd aan informatiebeveiliging niet op waarde schatten en niet voldoende prioriteit aan informatiebeveiliging toekennen.

Een veelgenoemd punt is de vrees van bestuurders dat informatiebeveiliging conflicteert met de reguliere onderwijspraktijk. De redenering van sommige bestuurders is dat middelen en personeel maar één keer kunnen worden ingezet en dat elke euro of FTE die wordt ingezet ten behoeve van informatiebeveiliging dus niet kan worden ingezet voor het verschaffen van goed onderwijs. Hoewel hier inderdaad een passende balans in moet worden gevonden, leeft bij veel respondenten het beeld dat veel bestuurders het risico van een incident niet goed op waarde weten te schatten. We zien inderdaad dat het bewustwording omtrent het belang van informatiebeveiliging vaak pas ontstaat op het moment dat incidenten plaatsvinden: pas na een incident wordt er echt (of meer) geïnvesteerd in informatiebeveiliging, wat impliceert dat het risico van een incident zwaarder wordt gewogen dan daarvoor, ondanks dat het

werkelijke risico nauwelijks veranderd is. Dit duidt erop dat een bestuurder dit risico onderschatte totdat het mis ging.[12]

Verschillende respondenten verwachten dat het normenkader een positieve impact op IBP-bewustwording zal hebben, doordat het IBP-functionarissen een concrete handreiking geeft om het gesprek met hun bestuurder aan te gaan. Het wordt makkelijker om duidelijk te maken waar men momenteel staat en waar men zou moeten staan. Sommige respondenten noemen het idee van een benchmark, zodat schoolbesturen kunnen zien waar ze staan ten opzichte van andere besturen.

Naast bewustwording van bestuurders speelt ook het bewustwording binnen de rest van de organisatie een belangrijke rol. Bij de interviews is meermaals gesteld dat het onderwijspersoneel doorgaans weinig affiniteit heeft met informatiebeveiliging en vreest dat inspanningen om informatiebeveiliging binnen hun schoolbestuur te verbeteren ten koste gaat van hun reguliere werkzaamheden. Het belang van informatiebeveiliging dient daarom ook aangekaart te worden bij het onderwijspersoneel. Deze mensen zijn namelijk belast met de uitvoering van beleid dat door bestuurders wordt opgesteld. Een lage mate van bewustwording kan resulteren in het niet uitvoeren van beheersmaatregelen, dit zorgt o.a. voor een lager volwassenheidsniveau in Domein 4: Personeelsbeheer. Het *clear desk* en *clear screen*-beleid blijkt bijvoorbeeld iets dat in een lesomgeving vaak als onhandig wordt ervaren en waarvan de naleving moeilijk te controleren is. Ook voor het afsluiten van klaslokalen of serverkasten (Domein 12: Fysieke Beveiliging) is een schoolbestuur afhankelijk van de mate van bewustwording van medewerkers over de betreffende risico's. Ook meer in algemene zin blijkt uit de nulmeting dat controle op de naleving van IBP-beleid vaak maar in geringe mate gebeurt. Veel is daarom afhankelijk van de eigen wil van medewerkers om zich aan het beleid te houden, wat bewustwording erg belangrijk maakt.

3.1.2 Expertise

Het gebrek aan expertise is tijdens de interviews vaak aangehaald als obstakel. Dit kan dan gaan om technische, juridische en/of beleidsmatige expertise. Wanneer één persoon verantwoordelijk is voor alle IBP gerelateerde zaken, wat met name voorkomt bij kleine organisaties, heeft die persoon het technische of juridische deel (of beide) er vaak bij gekregen, zonder daar een achtergrond in te hebben. Een aantal respondenten gaf tijdens het gesprek aan dat hen de functie van security officer bij de introductie van de AVG in 2018 is toebedeeld, zonder dat men eerder ervaring in deze rol had. Met name bij kleine besturen in het primair onderwijs komt het voor dat een leraar of medewerker van het secretariaat deze functies erbij krijgt. Ook zien we, wederom met name in het primair onderwijs, dat het voorkomt dat de IT in zo'n sterke mate wordt uitbesteed dat er intern geen of nauwelijks IT-kennis meer is.

Het gebrek aan expertise is in algemene zin een uitdaging voor de ontwikkeling van schoolbesturen op IBP-gebied, maar het is ook een concreet obstakel bij de implementatie van het normenkader. Het opstellen en uitvoeren van IBP-beleid voor meer technische IT-onderwerpen in het normenkader, concreet Domein 7: Change Management, Domein 10: Identity en Access Management en Domein 13: IT-operatie, kan ingewikkeld zijn wanneer er weinig technische expertise in huis is. Ook zien we dat het opstellen van beleid een uitdaging is,

[12] Er zijn ook andere mogelijke verklaringen voor toenemende investeringen in informatiebeveiliging na een incident, bijvoorbeeld dat bestuurders die net een incident hebben gehad het risico van nóg een incident juist *overschatten*, of dat zij willen laten zien dat ze zich inzetten om nog een incident te voorkomen. Er kunnen meerdere verklaringen tegelijk van toepassing zijn, maar in de interviews komt de verklaring naar voren die wij hier in de hoofdtekst noemen.

zeker wanneer de in-house kennis vooral van technische aard is of de rol van IBP-functionaris nieuw is voor de organisatie, simpelweg omdat men niet weet hoe de documenten eruit moeten zien en wat er precies in moet staan. Dit resulteert in een lager volwassenheidsniveau in Domein 1: Bestuur, Domein 2: Organisatie en Domein 6: Incident/Problem Management. In deze domeinen worden namelijk processen en procedures ontwikkeld en dit vereist specifieke kennis en vaardigheden.

Beperkte expertise is dus een obstakel waar het normenkader zelf vermoedelijk minder impact op zal hebben, in tegenstelling tot bewustwording zoals hiervoor besproken. Wel is onze verwachting dat het normenkader de besturen in het funderend onderwijs die momenteel onbewust onbekwaam zijn op het vlak van IBP, zullen opschuiven naar bewust onbekwaam.

3.1.3 Capaciteit

Verbonden aan de eerdere onderwerpen van bewustwording en expertise, is capaciteit. Hiermee wordt zowel de interne capaciteit bedoeld, het aantal FTE dat intern beschikbaar is voor IBP, als de externe capaciteit in de vorm van ondersteuning van buitenaf. Hier wordt ook de relatie met de vorige twee onderwerpen direct duidelijk: wanneer een schoolbestuur zich goed bewust is van IBP-risico's en het belang van goed IBP-beleid, zal er eerder afdoende capaciteit voor IBP worden vrijgemaakt dan wanneer het bestuur de risico's en mogelijke gevolgen niet overziet. Als het bestuur deze capaciteit beschikbaar stelt kan een gebrek aan interne expertise worden opgevangen door bijvoorbeeld werving, bijscholing of het aan boord halen van externe expertise.

Verschillende respondenten wijzen erop dat er binnen hun bestuur geen extra budget of personeel voor IBP wordt vrijgemaakt, omdat de bestuurder vreest dat dit conflicteert met de beschikbare capaciteit voor het onderwijs, zie ook paragraaf 3.1.1 over bewustwording. Dit kan leiden tot het beschikbaar stellen van te weinig capaciteit voor IBP. Zelfs wanneer een bestuurder zich volledig bewust is van IBP-risico's kan het echter zo zijn dat er simpelweg niet genoeg capaciteit in de organisatie is om alles goed te regelen. Aan de ICT-kant moet er voor de implementatie van het normenkader bijvoorbeeld capaciteit beschikbaar zijn om hard- en software te beheren (Domein 5: Configuration Mangement), de data in deze systemen te classificeren (Domein 9: Datamanagement) en de IT-infrastructuur te beschermen en te testen (Domein 11: Security Management). Met name bij kleinere besturen lijkt dit te wringen. Ook gaven een aantal respondenten van schoolbesturen uit krimpregio's aan dat afnemende inschrijvingen van leerlingen het IBP-beleid verder onder druk zet.

Ook de extern beschikbare capaciteit kan een obstakel vormen bij de implementatie van het normenkader, in bijzonder bij het borgen van Domein 15: Ketenbeheer. Zo maken verschillende maken gebruik van een externe FG voor het opstellen van verwerkersovereenkomsten omdat ze niet groot genoeg zijn om een FG intern in dienst te nemen. Sommige organisaties vangen dit op door de krachten en werkzaamheden te bundelen met andere organisaties en gezamenlijk een FG aan te nemen. Deze mensen moeten dan beschikbaar zijn en de krapte op de arbeidsmarkt vormt hier een obstakel. De krapte op de ICT-arbeidsmarkt is bekend en in kaart gebracht, ook voor de onderwijssector[13]. Cijfers voor de arbeidsmarkt voor juridisch personeel in het onderwijs zijn niet bekend, maar de algemene krapte op de arbeidsmarkt geeft geen reden om aan te nemen dat de situatie voor deze beroepsgroep sterk afwijkt van overige beroepen. Dit obstakel speelt ook bij bijvoorbeeld het werven van ICT-ers.

[13] [pr-edict.nl]

3.1.4 Koppeling bewustwording, expertise en capaciteit aan domeinen normenkader

In de bovenstaande paragrafen is er een koppeling gemaakt tussen bewustwording, expertise en capaciteit en de domeinen uit het normenkader. In de onderstaande tabel zijn de koppelingen samengevat. Wanneer een domein niet staat genoemd bij, bijvoorbeeld, bewustwording, betekent dit niet dat bewustwording geen rol speelt bij de het implementeren van de voorbeeldmaatregelen uit dat domein, maar dat de nadruk volgens de onderzoekers ligt bij een ander thema.

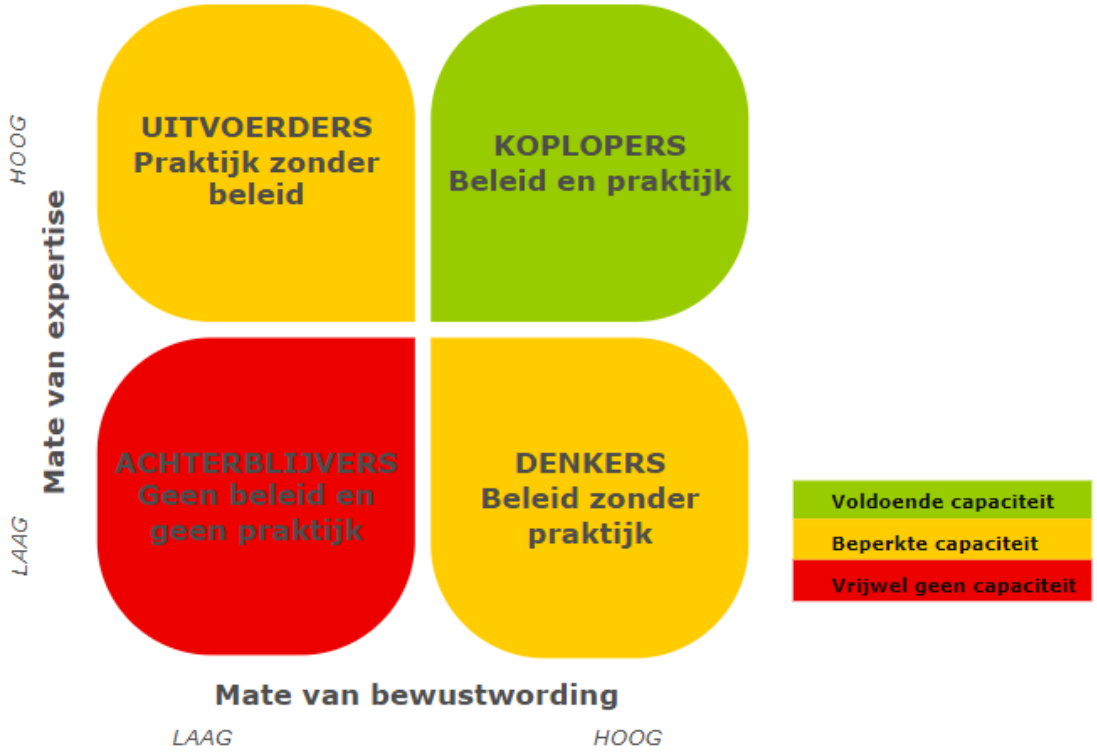
Thema	Koppeling met domeinen uit Normenkader IBP FO
Bewustwording	Domein 1: Bestuur Domein 3: Risicomanagement Domein 4: Personeelsbeheer Domein 12: Fysieke Beveiliging Domein 14: Bedrijfscontinuïteitsmanagement
Expertise	Domein 1: Bestuur Domein 2: Organisatie Domein 6: Incident/Problem Management Domein 7: Change Management Domein 10: Identity en Access Management Domein 13: IT-operatie
Capaciteit	Domein 5: Configuration Management Domein 9: Datamanagement Domein 11: Security Management Domein 15: Ketenbeheer

Tabel 18 Koppeling van de obstakelthema's Bewustwording, Expertise en Capaciteit aan de domeinen van het Normenkader IBP FO

3.2 Archetypische schoolbesturen en hun ondersteuningsbehoefte

Voor het bepalen van de ondersteuningsbehoefte is het handig om schoolbesturen op te delen in categorieën van gelijksoortige behoeftes qua ondersteuning. Deze indeling kan niet gemaakt worden op basis van bijvoorbeeld de omvang of sector van een schoolbestuur. Schoolbesturen met dezelfde omvang kunnen namelijk verschillen van elkaar ten aanzien van het huidige niveau van informatiebeveiliging.

Dialogic heeft daarom onderzocht of er archetypes van schoolbesturen aangewezen kunnen worden op basis van de uitkomsten van de nulmeting die ook herkenbaar zijn voor de schoolbesturen zelf. Op basis van de meest genoemde obstakels kunnen deze archetypes worden opgesteld. Wanneer de drie thema's Bewustwording, Expertise en Capaciteit met elkaar worden gekruist, ontstaat er namelijk een beeld van een aantal 'archetypische' schoolbesturen en hun bijbehorende ondersteuningsbehoefte. Figuur 3 toont deze kruising in een matrix: de horizontale as geeft de mate van bewustwording op het vlak van IBP binnen een schoolbestuur aan; de verticale as geeft de mate van expertise op het vlak van IBP binnen een schoolbestuur. De mate van bewustwording en aanwezige expertise leiden tot de mate van capaciteit. De drie kleuren geven de beschikbare capaciteit voor IBP binnen een bestuur aan, zie de legenda aan de rechterkant van de matrix.



Figuur 3 Matrix met archetypische schoolbesturen

Door het kruisen van de drie thema's ontstaan er vier archetypes, namelijk **Koplopers**, **Uitvoerders**, **Denkers** en **Achterblijvers**. Deze archetypes zijn opgesteld om een grofmazig beeld te geven van de typen schoolbesturen binnen de gehele populatie. De vier archetypes worden hieronder verder toegelicht.

3.2.1 Koplopers

Deze categorie van schoolbesturen staat rechtsboven in de matrix en kenmerkt zich door een hoge mate van IBP-bewustwording en een hoge mate van expertise. Het bestuur 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.

Uit de nulmeting blijkt dat de Koplopers met name de grote schoolbesturen zijn, waar naast een bewust bestuurder ook een CISO zorgt voor een grote mate aan expertise. Uit de nulmeting blijkt overigens dat ook de Koplopers nog niet volledig voldoen aan het IBP-normenkader. Dit type schoolbestuur heeft echter de middelen in huis om zelfstandig het gewenste volwassenheidsniveau te bereiken.

3.2.2 Uitvoerders

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, zie links bovenin de matrix. Uitvoerders zijn vaak schoolbesturen waarbij één of een aantal individuen in de staf veel verstand hebben van IBP en vaak ad hoc reageren op incidenten, zonder dat de beheersmaatregelen in instructies of werkbeschrijvingen zijn vastgelegd. Deze individuen hebben vaak een technische of juridische achtergrond en voelen zich sterk verantwoordelijk voor de informatiebeveiliging en

trekken alle taken die hierbij horen naar zich toe (of krijgen deze toebedeeld). Hierdoor is er ondanks een hoge mate van expertise slechts beperkte capaciteit voor IBP beschikbaar. Dit resulteert in single points of failure, omdat de informatiebeveiliging niet gecontinueerd kan worden als de expert wegvalt door ziekteverzuim of verloop.

Op basis van de steekproef kan gesteld worden dat de Uitvoerders veelal besturen zijn met een kleine maar gepassioneerde IBP-afdeling. Het Programma DVO kan deze besturen ondersteunen op het vlak van het versterken van bewustwording, bijvoorbeeld vanuit de programmalijn *Schoolorganisatie en gedrag*, zodat verantwoordelijkheid voor uitvoering van de informatiebeveiliging gevoeld wordt door de hele organisatie in plaats van een groep individuen. Hoger bewustwording leidt namelijk tot minder ad hoc activiteiten in het oplossen van incidenten en dat geeft meer ruimte voor documentatie. Hierdoor kan een bestuur de overstappen maken van 'brandjes blussen' naar brandpreventie.

3.2.3 Denkers

De Denkers betreft het type schoolbestuur dat een hoge mate van bewustwording heeft over het belang van IBP, maar waar expertise nog mist, zie rechts onderin de matrix. Het bewustwording is geregeld ontstaan doordat het schoolbestuur 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.

De Denkers zijn veelal schoolbesturen waar een gebrek is aan ervaren personeel op het vlak van IBP. Deze groep heeft het meeste baat bij het beschikbaar maken van externe expertise waar gebruikt van kan worden gemaakt. Dit kan door het delen van best practices (bijv. over een Koploper), maar met name ook door het inregelen van een loket waarbij men terecht kan met vragen over specifieke IBP-thema's.

3.2.4 Achterblijvers

Deze laatste groep van besturen is 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. Het IBP-beleid bij deze besturen is non-existent of onvolledig en er is vrijwel geen capaciteit beschikbaar om beheersmaatregelen uit te voeren.

De categorie Achterblijvers bestaat uit een grote groep van kleine schoolbesturen, waarvoor IBP ver af staat van de dagelijkse praktijk. De Achterblijvers hebben de grootste stappen te zetten, maar zijn daarmee ook het meest relevant voor het programma DVO. Bij deze besturen zal de eerste stap zijn om het bewustwording te verhogen, zodat ook bij hen de noodzaak van IBP helder is. Wanneer de besturen vervolgens *bewust* onbekwaam zijn is voor hen ook het beschikbaar stellen van externe expertise van waarde.

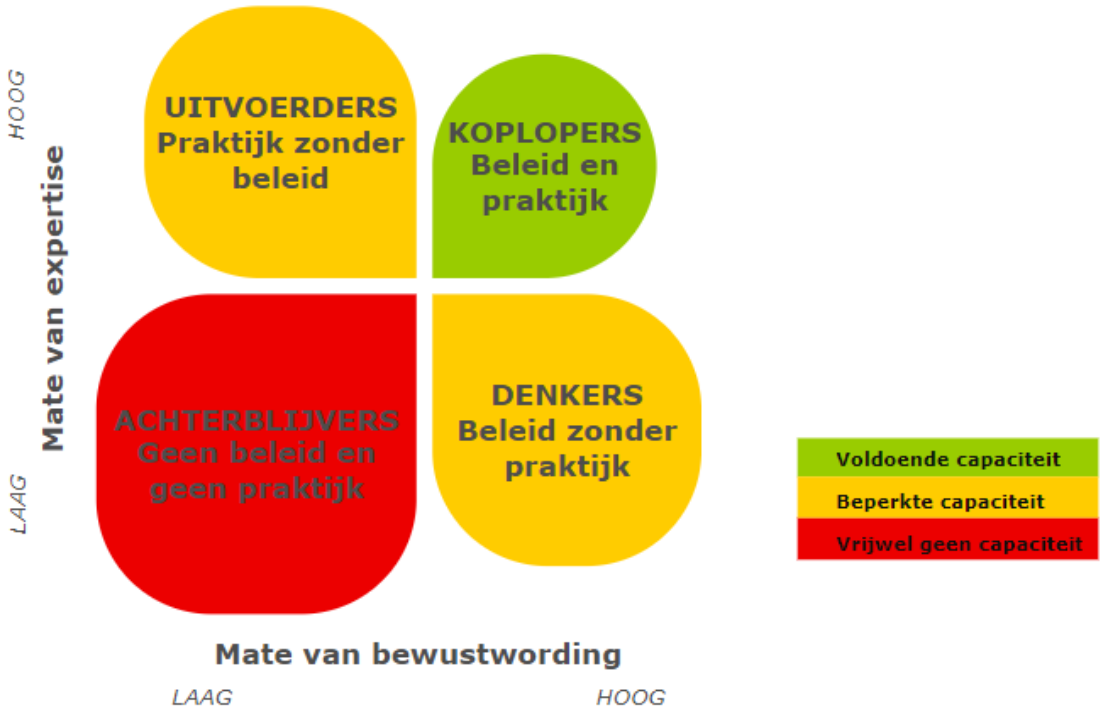
3.2.5 Ondersteuningsbehoefte van de archetypische schoolbesturen

In Tabel 19 is op basis van de nulmeting en de gesprekken met schoolbesturen een inschatting gemaakt van het aandeel per archetype in de gehele populatie van schoolbesturen. De percentages zijn bedoeld als indicatie van het aandeel van een archetypisch bestuur in de gehele populatie. Ook is er in de tabel een koppeling gemaakt met de (verwachte) ondersteuningsbehoefte op domeinniveau op basis van de koppeling tussen de thema's bewustwording, expertise en capaciteit en de domeinen onder 3.1.1, 3.1.2 en 3.1.3. Voorbeeld: de Uitvoerders hebben een laag bewustwording en beperkte capaciteit en hun ondersteuningsbehoefte is dus gericht op de domeinen die relevant zijn voor deze thema's. Ook is er in de tabel een uitsplitsing gemaakt naar welke van de domeinen van belang zijn voor het op orde krijgen van de basis en het mitigeren van de hoge risico's.

Archetype (~% van populatie)	Verwachte ondersteuningsbehoefte op domeinen
Koplopers (~10%)	De verwachting is dat de Koplopers vanwege een hoge mate van bewustwording, expertise en beschikbare capaciteit geen ondersteuningsbehoefte hebben.
Uitvoerders (~25%)	**De basis op orde:** • Domein 1: Bestuur • Domein 9: Datamanagement • Domein 12: Fysieke Beveiliging • Domein 14: Bedrijfscontinuïteitsmanagement **Mitigeren hoge risico's:** • Domein 3: Risicomanagement • Domein 4: Personeelsbeheer • Domein 9: Datamanagement • Domein 11: Security Management • Domein 12: Fysieke Beveiliging • Domein 15: Ketenbeheer
Denkers (~25%)	**De basis op orde:** • Domein 1: Bestuur • Domein 2: Organisatie • Domein 6: Incident/Problem Management • Domein 7: Change Management • Domein 9: Datamanagement **Mitigeren hoge risico's:** • Domein 7: Change Management • Domein 9: Datamanagement • Domein 10: Identity en Access Management • Domein 11: Security Management • Domein 13: IT-operatie • Domein 15: Ketenbeheer
Achterblijvers (~40%)	**De basis op orde:** • Domein 1: Bestuur • Domein 2: Organisatie • Domein 6: Incident/Problem Management • Domein 7: Change Management • Domein 9: Datamanagement • Domein 12: Fysieke Beveiliging • Domein 14: Bedrijfscontinuïteitsmanagement **Mitigeren hoge risico's:** • Domein 3: Risicomanagement • Domein 4: Personeelsbeheer • Domein 7: Change Management • Domein 9: Datamanagement • Domein 10: Identity en Access Management • Domein 11: Security Management • Domein 12: Fysieke Beveiliging • Domein 13: IT-operatie • Domein 15: Ketenbeheer

Tabel 19 Aandeel van archetypes in de totale populatie van schoolbesturen en verwachte ondersteuningsbehoefte

De toevoeging van deze percentages aan Figuur 3 levert de onderstaande figuur op waarin het aandeel van de archetypes in populatie ook is gevisualiseerd.



Figuur 4 Matrix met archetypische schoolbesturen met percentage aandeel in gehele populatie

4 Conclusies

In dit laatste hoofdstuk beantwoorden we de onderzoeksvragen van de door Dialogic uitgevoerde nulmeting (4.1). Ook presenteren we belangrijke aandachtspunten voor de toekomstige implementatie van het normenkader (4.2).

4.1 Onderzoeksvragen nulmeting

4.1.1 Het huidige niveau van IBP bij schoolbesturen in het funderend onderwijs

Tabel 20 toont de kwantitatieve uitkomsten van de nulmeting. In de steekproef van schoolbesturen voldeed **geen enkel schoolbestuur** aan de norm voor alle getoetste statements in de nulmeting.

Domeinen	Percentage kleine besturen dat norm haalt (n=3)	Percentage middelgrote besturen dat norm haalt (n=6)	Percentage grote besturen dat norm haalt (n=6)	**Totaal percentage besturen dat norm haalt (n=15)**
1: Bestuur	0%	50%	17%	**27%**
2: Organisatie	0%	0%	33%	**13%**
3: Risicomanagement	33%	0%	33%	**20%**
4: Personeelsbeheer	0%	0%	17%	**7%**
5: Configuration Management	67%	17%	17%	**27%**
6: Incident/Problem Management	33%	50%	50%	**47%**
7: Change Management	33%	33%	17%	**27%**
8: Systeemontwikkeling	N.V.T.	N.V.T.	N.V.T.	**N.V.T.**
9: Datamanagement	0%	17%	17%	**13%**
10: Identity & Access Management	33%	33%	17%	**27%**
11: Security Management	0%	17%	0%	**7%**
12: Fysieke Beveiliging	33%	17%	0%	**13%**
13: IT-operatie	33%	33%	17%	**27%**
14: Bedrijfscontinuïteitsmanagement	33%	33%	0%	**20%**
15: Ketenbeheer	0%	33%	0%	**13%**
Percentage besturen dat voldoet aan alle getoetste statements	0%	0%	0%	**0%**

Tabel 20 Uitsplitsing percentages per domein naar omvang schoolbesturen

Tabel 20 geeft inzicht in de verschillen tussen schoolbesturen van verschillende omvang. Voor de **kleine schoolbesturen** in de steekproef geldt dat geen schoolbestuur voldoet aan de norm in Domein 1. De grootste verschillen ten opzichte van het totale gemiddelde worden daarnaast gevonden in de domeinen Datamanagement (8) en Ketenbeheer (15). Opvallende lagere scores zien we bij de **middelgrote schoolbesturen** in de domeinen Personeelsbeheer (4), Configuration Management (5) en Incident/Problem Management (6). Lagere scores van de categorie **grote schoolbesturen** die noemenswaardig zijn komen uit de domeinen Change Management (7) en Bedrijfscontinuïteitsmanagement (14).

4.1.2 Belangrijke tekortkomingen bij schoolbesturen ten aanzien van het normenkader

Onder paragraaf 2.1 hebben we op het niveau van de clusters uitgewerkt welke inspanningen van schoolbesturen wenselijk zijn voor het behalen van de gewenste norm. We concluderen dat er vijf belangrijke tekortkomingen zijn waarvoor maatregelen dienen te worden genomen:

1. **Single points of failure.** De meeste verantwoordelijkheden en procedures ten aanzien van IBP zijn benoemd, maar we zien in de praktijk dat de uitvoering afhankelijk is van een kleine groep individuen binnen een schoolbestuur. Omdat de werkprocessen vaak niet gedocumenteerd zijn, kan de uitval van één individu grote gevolgen kan hebben voor de continuïteit van de uitvoering.
   Maatregel: Versterken van Domein 4: Personeelsbeheer (specifiek 4.3 Afhankelijkheid van individuen) zodat rollen en verantwoordelijken niet alleen zijn benoemd, maar er ook een back-upplan is voor vitale medewerkers en afdelingen.

2. **Bewustwording.** De respondenten geven aan dat op het vlak van bewustwording rondom IBP bij zowel bestuurders als onderwijspersoneel nog grote stappen gezet dienen te worden. Dit gebrek aan awareness heeft op dit moment een negatief effect op de naleving van beheersmaatregelen.
   Maatregel: Versterken van Domein 1: Bestuur voor het bewustwording bij bestuurders, zodat een strategie en visie beschikbaar is voor alle activiteiten met betrekking tot informatiebeveiliging. Domein 4: Personeelsbeheer (specifiek 4.6 Veiligheidsbewustwording) is belangrijk voor het organisatiebreed stimuleren van bewustwording, zodat medewerkers bewust zijn van hun verantwoordelijkheid ten aanzien van informatiebeveiliging en het uitvoeren van het beleid.

3. **Continuïteit.** Bij het grootste gedeelte van de respondenten is er naast een procedure voor het melden van incidenten geen crisis- of herstelplan opgesteld. Hierdoor is het zeer de vraag of schoolbesturen tijdens een groot incident de normale bedrijfsvoering kunnen doorzetten. Ook regelmatige tests met het terugzetten van back-ups worden door het merendeel van de schoolbesturen niet uitgevoerd.
   Maatregel: Schoolbesturen dienen de (voorbeeld-)maatregelen Domein 14: Bedrijfscontinuïteitsmanagement, zoals het opstellen en testen van een bedrijfscontinuïteitsplan, over te nemen om de risico's van een groot incident te reduceren.

4. **Monitoring en logging.** Op basis van deze steekproef kan gesteld worden dat er vaak geen specifiek beleid opgesteld is wat betreft monitoring en logbestanden. Hierdoor wordt er geen gebruik gemaakt van informatie om incidenten preventief te detecteren en te voorkomen.
   Maatregel: Het overnemen van de (voorbeeld-)maatregelen uit Domein 11: Security Management (specifiek 11.4 Logging) stelt schoolbesturen in staat om tijdig ongepaste en/of ongebruikelijke activiteiten te detecteren doordat er eisen voor logs zijn opgesteld.

5. **Leveranciersmanagement.** We zien dat de meeste schoolbesturen hun eigen beleid niet vertalen in aanvullende eisen boven op de standaardovereenkomsten van leveranciers. Als reden wordt gegeven dat het als individueel schoolbestuur lastig onderhandelen is, terwijl bijvoorbeeld op het vlak van back-ups en het beheer van toegangsrechten de standaardovereenkomst van een leverancier niet voldoet aan het opgestelde beleid.
   Maatregel: Het overnemen van de (voorbeeld-)maatregelen uit Domein 15: Ketenbeheer (specifiek 15.1 Service Level Agreement en 15.3 Leveranciersrisicomanagement) maakt het mogelijk om de processen bij leveranciers te conformeren aan het interne informatiebeveiligingsbeleid van het schoolbestuur.

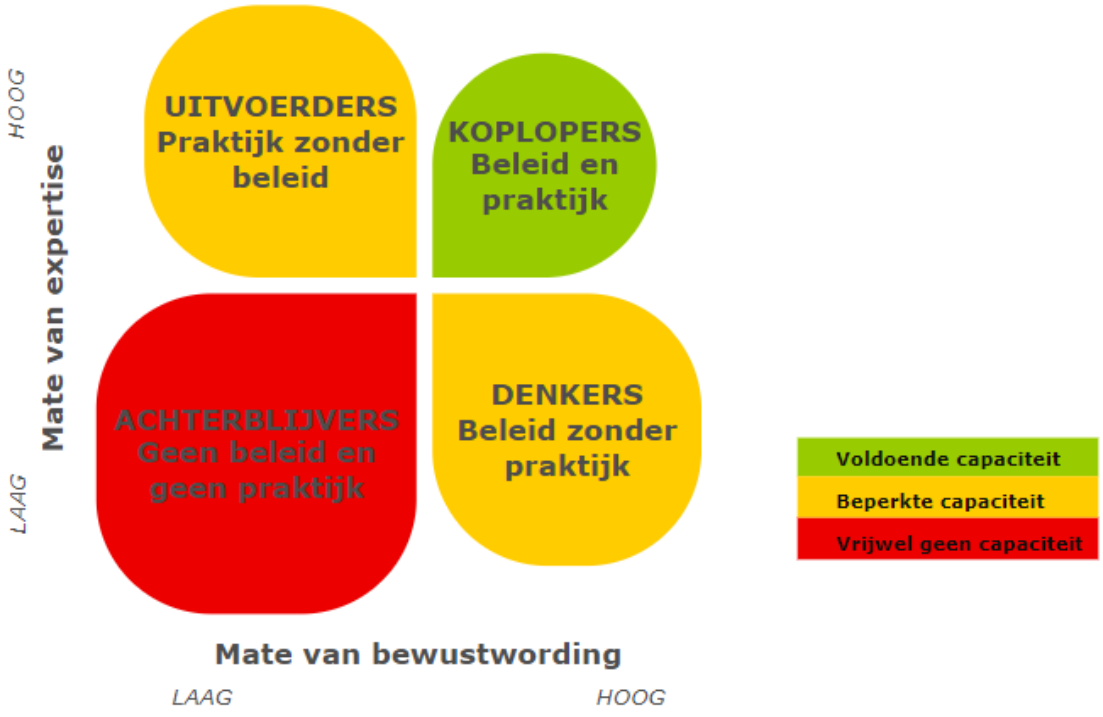
4.1.3 De obstakels voor schoolbesturen ten aanzien van de implementatie van het normenkader

We stellen vast dat er drie uitdagingen en obstakels zijn voor schoolbesturen in de implementatie van het normenkader:

1. **Bewustwording.** Zowel het gebrek aan bewustwording bij bestuurders als het onderwijspersoneel heeft een negatief effect op de implementatie van het normenkader. Wanneer we het hebben over bewustwording bij bestuurders doelen we op het besef dat informatiebeveiliging, en het mitigeren van risico's op dit vlak, essentieel is de bedrijfsvoering van een schoolbestuur. Een lage mate van bewustwording bij onderwijspersoneel kan erin resulteren dat beheersmaatregelen niet worden uitgevoerd. Meerdere respondenten verwachten echter dat de introductie van het normenkader een positief effect zal hebben op het IBP-bewustwording binnen het funderend onderwijs.
2. **Expertise.** Het gebrek aan expertise wordt vaak genoemd als een belangrijk obstakel. 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 voor IBP is ook een belangrijk obstakel. Een tekort aan beschikbare capaciteit hangt vaak samen met de vrees dat het vrijmaken van capaciteit voor IBP conflicteert met de uitvoering van het reguliere onderwijs.

4.1.4 Ondersteuning van schoolbesturen

Voor het bepalen van de ondersteuningsbehoefte is het handig om schoolbesturen op te delen in categorieën van gelijksoortige behoeftes qua ondersteuning. Op basis van de nulmeting en de drie belangrijkste obstakels en uitdagingen voor schoolbesturen stellen we vast dat er vier 'archetypes' zijn onder schoolbesturen, zie Figuur 5.



Figuur 5 Matrix met archetypische schoolbesturen met percentage aandeel in gehele populatie

De vier archetypes zijn:

- **Koplopers (~10%).** Het schoolbestuur heeft een gestructureerde en geformaliseerde uitvoering van de beveiliging van informatie. De beheersmaatregelen zijn vastgelegd in beleid en er is binnen het bestuur voldoende expertise en capaciteit beschikbaar om de beheersmaatregelen uit te voeren.
- **Uitvoerders (~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 (~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 te weinig kennis aanwezig is.
- **Achterblijvers (~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.

In Tabel 21 op de volgende pagina is op basis van de nulmeting en de gesprekken met schoolbesturen een inschatting gemaakt van het aandeel per archetype in de gehele populatie van schoolbesturen. De percentages zijn bedoeld als indicatie van het aandeel van een archetypisch bestuur in de gehele populatie. Ook is er in de tabel een koppeling gemaakt met de (verwachte) ondersteuningsbehoefte op domeinniveau per archetype. Tenslotte is er in de tabel een uitsplitsing gemaakt naar welke van de domeinen van belang zijn voor het op orde krijgen van de basis en het mitigeren van de hoge risico's.

Archetype (~% van populatie)	Verwachte ondersteuningsbehoefte op domeinen
Koplopers (~10%)	De verwachting is dat de Koplopers vanwege een hoge mate van bewustwording, expertise en beschikbare capaciteit minder ondersteuningsbehoefte hebben.
Uitvoerders (~25%)	**De basis op orde:** • Domein 1: Bestuur • Domein 9: Datamanagement • Domein 12: Fysieke Beveiliging • Domein 14: Bedrijfscontinuïteitsmanagement **Mitigeren hoge risico's:** • Domein 3: Risicomanagement • Domein 4: Personeelsbeheer • Domein 9: Datamanagement • Domein 11: Security Management • Domein 12: Fysieke Beveiliging • Domein 15: Ketenbeheer
Denkers (~25%)	**De basis op orde:** • Domein 1: Bestuur • Domein 2: Organisatie • Domein 6: Incident/Problem Management • Domein 7: Change Management • Domein 9: Datamanagement **Mitigeren hoge risico's:** • Domein 7: Change Management • Domein 9: Datamanagement • Domein 10: Identity en Access Management • Domein 11: Security Management • Domein 13: IT-operatie • Domein 15: Ketenbeheer
Achterblijvers (~40%)	**De basis op orde:** • Domein 1: Bestuur • Domein 2: Organisatie • Domein 6: Incident/Problem Management • Domein 7: Change Management • Domein 9: Datamanagement • Domein 12: Fysieke Beveiliging • Domein 14: Bedrijfscontinuïteitsmanagement **Mitigeren hoge risico's:** • Domein 3: Risicomanagement • Domein 4: Personeelsbeheer • Domein 7: Change Management • Domein 9: Datamanagement • Domein 10: Identity en Access Management • Domein 11: Security Management • Domein 12: Fysieke Beveiliging • Domein 13: IT-operatie • Domein 15: Ketenbeheer

Tabel 21 Aandeel van archetypes in de totale populatie van schoolbesturen en verwachte ondersteuningsbehoefte

4.2 Aandachtspunten

Voor de toekomstige implementatie van het normenkader en ondersteuning vanuit het Programma DVO richting schoolbesturen zijn de volgende drie aandachtspunten van belang:

1. **Beschikbaar stellen van audit-tooling voor schoolbesturen.** Uit dit onderzoek blijkt dat schoolbesturen moeite hebben om zelfstandig een nulmeting ten aanzien van het normenkader. Het programma DVO moet aandacht besteden aan het ondersteunen van deze schoolbesturen, want de nulmeting is de basis voor verdere implementatie van het normenkader. Ondersteuning van schoolbesturen is mogelijk door het beschikbaar te stellen van een laagdrempelige methodiek aan schoolbesturen, zodat men zelfstandig een interne audit kunnen uitvoeren. Het zelfstandig uitvoeren van een audit levert een bestuur meer kennis en kunde ten aanzien van informatiebeveiliging oplevert, en daarnaast zou het vanwege het grote aantal schoolbesturen in het funderend onderwijs bijzonder uitdagend om deze audit centraal uit te voeren. Daarnaast hebben schoolbesturen tijdens de gesprekken meermaals aangegeven behoefte te hebben aan een benchmark om hun ontwikkeling aan af te meten en een reguliere meting zou invulling geven aan deze behoefte. Bij de programmalijn *Sturen op basis van normen* van DVO worden herhaalde metingen ten behoeve van het monitoren van het groeipad al benoemd, maar op basis van deze nulmeting blijkt dat deze metingen ook van belang zijn voor de informatievoorziening en bewustwording van de schoolbesturen.
2. **Integreren NBA volwassenheidsniveaus in toetsingskader IBP FO**. Bij de ontwikkeling van een methodiek of tooling voor een zelfstandige audit dient DVO te overwegen om de NBA Volwassenheidsniveaus te integreren in het Toetsingskader IBP FO. Dit stelt schoolbesturen namelijk in staat om hun voortgang gedetailleerder te monitoren. Deze actie kan opgepakt worden binnen de programmalijn *Sturen op basis van normen* waar de doorontwikkeling van het toetsingskader is belegd.
3. **Een duidelijk zichtbaar ondersteuningsaanbod dat aansluit op de behoeften van scholen.** We stellen op basis van de gesprekken met schoolbesturen vast dat bestaande ondersteuningsmogelijkheden, zoals bijvoorbeeld het Template IBP-beleidsplan en de prioritering binnen het normenkader via de 'Voorlopige starttabel', vaak niet bekend zijn bij de doelgroep. Daarom is het van belang om het duidelijk te communiceren over ondersteuningsmogelijkheden, zowel bij bestaande hulpverlening als ondersteuningsaanbod dat nog ontwikkeld dient te worden.

Bijlage 1. Overzicht interviewrespondenten

In Tabel 22 zijn de schoolbesturen weergegeven die in de steekproef van de nulmeting zijn meegenomen. Ook is er per bestuur aangegeven in welke onderwijssector men actief is.

Schoolbestuur	PO	VO	SO	SBO	VSO
Stg. Openbaar Basisonderwijs Duin- en Bollenstreek	X				
Samenwerkingsstichting voor Voortgezet Onderwijs Uden		X			
St. Viviani	X				
Ver. Oecumenisch Onderwijs in Maarn	X				
Stg. Prot. Chr. V.O. Nijverdal		X			
Stg. Chr. Voortg. Onderwijs Alblasserwaard-Vijfheerenland		X			
Stg. v. CVO Zuid-West Fryslân		X			
Laurentius Stichting voor Kathol. Primair Onderwijs	X	X	X		
Stichting VierTaal			X		X
Stichting Twijs	X		X	X	X
Stichting BOOR	X	X	X	X	X
Stichting Surplus	X			X	
Nestas Scholengroep (fusie OPOD en SKOBA)	X			X	
Servicebureau MosaLira	X		X	X	X
Stichting Primair Onderwijs Leudal en Thornerkwartier	X			X	

Tabel 22 Schoolbesturen en bijbehorende onderwijssectoren

Bijlage 2. Oriënterende vragenlijst

Toelichting nulmeting IBP-normenkader Funderend Onderwijs

In opdracht van Kennisnet voert Dialogic onderzoek uit naar de impact van het nieuwe normenkader voor informatiebeveiliging en privacy (IBP) voor het funderend onderwijs (FO). In het programma **Digitaal Veilig Onderwijs** (DVO) wordt in opdracht van het ministerie van OCW programmatisch samengewerkt door OCW, de VO-raad, de PO-Raad, Kennisnet en SIVON om het FO digitaal veiliger te maken.

Het belang van informatiebeveiliging en privacy heeft de afgelopen jaren een enorme vlucht genomen. Niet alleen de komst van de AVG, maar ook het feit dat in toenemende mate berichten in het nieuws komen over datalekken, cyberincidenten en beveiligingsissues, maakt dat deze onderwerpen niet meer weg te denken zijn uit het pakket aan verantwoordelijkheden voor elke organisatie, ook onderwijsinstellingen. Het **Informatiebeveiliging en privacy normenkader** (IBP-normenkader) geeft de minimale eisen aan waar een schoolbestuur aan moet voldoen op het gebied van informatiebeveiliging en privacy. Het is de ambitie van het ministerie van OCW om deze normen wettelijk te verankeren voor schoolbesturen. Het normenkader gaat daarmee handvatten bieden aan schoolbesturen voor de invulling van wet- en regelgeving.

Scholen krijgen geruime tijd om de werkzaamheden te verrichten die nodig zijn om aan het normenkader te voldoen, maar de daadwerkelijke impact van de nieuwe IBP-normen in het FO is nog onduidelijk. Deze informatie is nodig om vanuit het programma een realistisch groeipad op te stellen voor scholen en de meest effectieve ondersteuningsmaatregelen te treffen. Onderdeel van onze nulmeting is het in kaart brengen van de huidige situatie en de nog te nemen stappen voor schoolbesturen om aan het normenkader-IBP voldoen. De doelstelling van de opdracht is om het bestuurlijk overleg van het programma DVO te voorzien van een grondig onderbouwde analyse van de huidige situatie en impact van het IBP-normenkader op scholen in het FO. De analyse vormt daarmee een belangrijk deel van de informatie die benodigd is voor het programma om te bepalen welke acties en maatregelen benodigd zijn om gewenste doelen te behalen.

Het uitgangspunt van de nulmeting is om met een **beperkte representatieve steekproef** een omvattend beeld te krijgen van de sector. Uw schoolbestuur is geselecteerd voor deze steekproef en wij gaan graag met u in gesprek om de status quo van IBP binnen uw bestuur in kaart te brengen aan de hand van het nieuwe normenkader. Door uw deelname aan het onderzoek krijgt u inzage in de stand van zaken op het vlak van informatiebeveiliging en privacy binnen uw schoolbestuur en bent u in een vroeg stadium betrokken bij het identificeren van de impact van het nieuwe kader. De uitkomsten van dit gesprek worden niet rechtstreeks met de opdrachtgever gedeeld, maar worden verwerkt in een rapportage waar we op geaggregeerd niveau uitspraken doen over de stand van IBP in het FO.

Ter voorbereiding van dit gesprek willen wij u vragen om aan de hand van een aantal stellingen een **interne analyse** te doen naar de huidige stand van uw IBP-beleid. De uitkomsten hiervan dienen als input voor het interview. De stellingen vind u op de volgende pagina's van dit document. Aangezien het normenkader betrekking heeft op verschillende onderdelen van uw organisatie, raden wij aan om bij het invullen van de analyse samen te werken met de relevante betrokkenen (IT, HR, IBP'ers, etc.) binnen uw schoolbestuur. Deze betrokkenen zijn ook welkom om aan te sluiten bij het gesprek dat wij gezamenlijk zullen voeren na afronding van de analyse.

Nulmeting door schoolbestuur & betrokkenen

Ter voorbereiding van het gesprek willen wij u vragen om een interne analyse uit te voeren naar de huidige stand van IBP binnen uw organisatie. Om u daarbij te helpen hebben wij het nieuwe IBP-normenkader ten behoeve van dit onderzoek opgedeeld in een aantal concrete onderdelen. Per onderdeel krijgt u een aantal stellingen die corresponderen met een bepaald '**volwassenheidsniveau'** voor dit onderdeel. Er zijn vijf van deze volwassenheidsniveaus per onderdeel en deze niveaus moeten als volgt geïnterpreteerd worden:

Omschrijving volwassenheids-niveau		Toelichting
1	**Maatregelen zijn ad hoc**	Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2	**Maatregelen bestaan en worden op consistente wijze uitgevoerd**	Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3	**Maatregelen zijn gedocumenteerd en de uitvoering is aantoonbaar**	Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.
4	**Er is een verbetercyclus aanwezig en gedocumenteerd**	De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is gedocumenteerd.
5	**Er is een bedrijfsbrede aanpak van risico's**	Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.

In de volgende tabel geven wij aan welke personen/afdelingen binnen uw organisatie waarschijnlijk het best in staat zijn om de stellingen per onderdeel te beoordelen. De uitvoering zal echter per organisatie verschillen en de indeling is dus geen vaststaand gegeven. Zo zullen bij een sommige scholen niet al deze normen van toepassing zijn vanwege de hoge mate van uitbestede IT-dienstverlening binnen het funderend onderwijs.

Respondent	Onderdeel
Schoolbestuur	1. Bestuur 2. Organisatie 3. Risicomanagement 12. Fysieke beveiliging 14. Bedrijfscontinuïteitsmanagement
IT	5. Configuration Management 6. Incident/Problem Management 7. Chance Management 8. Systeemontwikkeling 9. Datamanagement 10. Identity & Access Management 11. Security Management 13. IT-operatie 15. Ketenbeheer
HR	4. Personeelsbeheer

Voor elk van deze 15 onderdelen krijgt u een aantal stellingen te zien die indicatief zijn voor een bepaald **volwassenheidsniveau**. Deze stellingen zijn afkomstig uit **toetsingskaders** die worden gebruikt om de praktische invulling van een IBP-normenkader te toetsen.

U kunt op basis van de stellingen een keuze maken over welk niveau het **best overeenkomt** met de situatie binnen uw schoolbestuur. Zie hieronder een ingevuld voorbeeld voor het onderdeel **Organisatie** waar voor volwassenheidsniveau 2 is gekozen:

Volwassenheidsniveau		Nulmeting
1	• Eigenaarschap, rollen en verantwoordelijkheden zijn niet of nauwelijks toegewezen. • Er vindt geen of nagenoeg geen functiescheiding plaats.	☐
2	• Rollen die cruciaal zijn voor het managen van informatierisico's zijn benoemd en toegewezen. • Rollen en verantwoordelijkheden zijn gescheiden maar niet formeel vastgesteld.	☒
3	• Alle rollen op het gebied van het managen van informatierisico's zijn vastgesteld en toegewezen. • De scheiding van rollen en verantwoordelijkheden is gedefinieerd, goedgekeurd en grotendeels geïmplementeerd.	☐
4	• Eigenaarschap, verantwoordelijkheid en aansprakelijkheid worden periodiek getoetst.	☐
5	• Periodiek worden er database checks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheiding.	☐

U kunt de interne analyse voor uw organisatie uitvoeren vanaf de volgende pagina.

1. Bestuur

De onderdelen binnen **Bestuur** geven richting en ondersteuning om de informatiebeveiliging in te richten in lijn met organisatiedoelstellingen, risicobereidheid en wet- en regelgeving. De strategie en visie van een schoolbestuur op informatiebeveiliging en cybersecurity zijn de basis voor beleid en concrete plannen op het vlak van IBP.

Per volwassenheidsniveau staan in de tabel hieronder een aantal stellingen die indicatief zijn voor dat niveau. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Implementatie en uitvoering van maatregelen op het gebied van informatiebeveiliging gebeurt ad hoc. • Er is geen beleid opgesteld of er zijn enkele beleidsstukken in concept. • Er is geen informatiebeveiligings- of cyber security plan of roadmap opgesteld.	☐
2	• Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld. • Er is (informatie)beveiligingsbeleid waarin de meest relevante aspecten van informatiebeveiliging zijn opgenomen. • Er is een informatiebeveiligings- en/of cybersecurity plan of roadmap opgesteld.	☐
3	• Strategie en visie zijn goedgekeurd door het senior management en worden actief gecommuniceerd naar medewerkers en leveranciers. • Informatiebeveiligingsbeleid is goedgekeurd door het senior management en is digital of hard copy beschikbaar. • Het plan of roadmap is goedgekeurd door het senior management en wordt gecommuniceerd naar gebruikers en stakeholders.	☐
4	• Het IBP-beleid wordt periodiek geëvalueerd, geactualiseerd en goedgekeurd op een passend managementniveau.	☐
5	• De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen en wordt indien noodzakelijk bijgesteld.	☐

2. Organisatie

Het is belangrijk om informatiebeveiliging op de juiste wijze vorm te geven binnen de organisatie. De medewerkers op het hoogste niveau binnen de organisatie dragen een belangrijke verantwoordelijkheid. Zij zijn dan ook degenen die afwegingen dienen te maken voor informatiebeveiliging, zoals risicobereidheid en kosten-batenanalyses.

Onderstaande stellingen hebben betrekking op hoe IBP is georganiseerd binnen uw organisatie en hoe verantwoordelijkheden zijn verdeeld. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Eigenaarschap, rollen en verantwoordelijkheden zijn niet of nauwelijks toegewezen. • Er vindt geen of nagenoeg geen functiescheiding plaats.	☐
2	• Rollen die cruciaal zijn voor het managen van informatierisico's zijn benoemd en toegewezen. • Rollen en verantwoordelijkheden zijn gescheiden maar niet formeel vastgesteld.	☐
3	• Alle rollen op het gebied van het managen van informatierisico's zijn vastgesteld en toegewezen. • De scheiding van rollen en verantwoordelijkheden is gedefinieerd, goedgekeurd en grotendeels geïmplementeerd.	☐
4	• Eigenaarschap, verantwoordelijkheid en aansprakelijkheid worden periodiek getoetst.	☐
5	• Periodiek worden er database checks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheiding.	☐

3. Risicomanagement

Dit domein bevat de normen die bijdragen aan het op gestructureerde wijze identificeren en beheersen van risico's op het gebied van informatiebeveiliging. Daarvoor is het nodig om in een raamwerk of beleid te beschrijven hoe risicomanagement wordt toegepast binnen de organisatie en wie daar allemaal een rol in hebben.

Onderstaande stellingen hebben betrekking op hoe risicomanagement op het vlak van IBP is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Informatierisico's zijn niet of worden ad hoc bepaald. • Risicoanalyses worden zelden gedaan en zijn afhankelijk van individuen. • Er is geen plan voor het aanpakken of mitigeren van risico's.	☐
2	• Beleid en processen voor Information Risk Management zijn opgesteld. • Risicoanalyses worden uitgevoerd als onderdeel van het Risk Management proces. • Plannen voor het aanpakken en mitigeren van risico's zijn gemaakt, maar niet formeel vastgelegd.	☐
3	• Er is organisatiebreed beleid voor Information Risk Management dat is goedgekeurd door het senior management. • Er is een beschrijving voor het uitvoeren van een Data Protection Impact Assessment (DPIA). • Door duidelijke en passende instructies vinden risicoanalyses consistent en herhaaldelijk plaats. • Overgebleven risico's en maatregelen zijn geïdentificeerd, geanalyseerd en gedocumenteerd.	☐
4	• Het framework voor Information Risk Management worden periodiek geëvalueerd. • Geïdentificeerde risicoreacties geven ook inzicht in de kosten en baten daarvan.	☐
5	• Information Risk Management is volledig geïntegreerd in alle IT- en bedrijfsvoering, wordt volledig geaccepteerd en betrekt hierin personeel en leveranciers.	☐

4. Personeelsbeheer

In het domein Personeelsbeheer staan de normen die direct betrekking hebben op de medewerkers binnen een organisatie. Dit beslaat de hele cyclus van personeelsbeheer. Bij de werving van medewerkers met een verantwoordelijkheid op het gebied van informatiebeveiliging wordt aandacht besteed aan het binnenhalen van medewerkers die toegerust zijn voor de taak, medewerkers die in de organisatie zitten krijgen de benodigde opleiding om informatiebeveiligingskennis op peil te houden, en de organisatie bereidt zich voor op het vertrek van medewerkers die op een cruciale plek zitten (sleutelfunctionarissen) waarbij vertrek een risico is voor de continuïteit van de organisatie.

Onderstaande stellingen hebben betrekking op hoe personeelsbeheer in relatie tot IBP is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Activiteiten of maatregelen voor het werven van (IT) personeel zijn ad hoc geïmplementeerd en/of uitgevoerd. • Single points of failure met betrekking tot het personeel zijn niet geïdentificeerd. • Wanneer er functiewijzigingen of ontslagen plaatsvinden worden er geen ondernomen. • Overdracht van kennis is niet geïmplementeerd of wordt gedaan op ad-hoc basis. • Er zijn geen security-awareness activiteiten gedefinieerd of uitgevoerd.	☐
2	• Wervingsprocessen voor (IT-)personeel zijn gedefinieerd en geïmplementeerd. • Back-up en vervanging van belangrijke medewerkers/functies worden op afdelingsniveau geregeld. • Toegangsrechten van werknemers worden gewijzigd, opnieuw toegewezen en/of verwijderd op basis van functiewijziging en/of ontslag, maar het tijdig intrekken van toegangsrechten is niet gewaarborgd. • Kennis en vaardigheden worden vaak overgedragen op individuele basis. • Security-awareness activiteiten worden uitgevoerd op afdelingsniveau.	☐
3	• Er zijn processen geïmplementeerd om te garanderen dat het (IT) personeel goed is toegerust om bedrijfsdoelen te behalen. • Opvolgingsplanning, job rotatie en back-up van het personeel zijn geïmplementeerd. • Goedgekeurde processen zijn geïmplementeerd om kennis over te dragen en toegangsrechten opnieuw toe te wijzen of in te trekken. • Er zijn goedgekeurde processen op organisatieniveau geïmplementeerd om kennis over te dragen en gepaste documentatie-, training- en implementatiematerialen te onderhouden. • Er is een security-awareness programma opgenomen in het informatiebeveiligingsplan en wordt organisatiebreed uitgevoerd.	☐
4	• Relevante wervingsprocedures, functieomschrijvingen en security-awareness programma's worden periodiek geëvalueerd.	☐
5	• Op basis van de periodieke (zelf)evaluaties of risicoanalyses worden de wervingsprocessen, functieomschrijvingen en security-awareness programma's verbeterd.	☐

5. Configuration Management

Configuration Management (configuratiemanagement) betreft het bijhouden van alle informatie van en over IT-componenten binnen de organisatie. Je legt vast welke hardware (bijvoorbeeld computers of printers) er zijn, welke software gebruikt wordt (inclusief versienummers), welke updates er zijn uitgevoerd en welke instellingen er gehanteerd worden bij elke component. Ook de onderlinge relaties tussen de componenten worden vastgelegd.

Onderstaande stellingen hebben betrekking op hoe configuratiemanagement is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Er is geen configuratieprocedure. • De documentatie van de configuratie is onvolledig en onbetrouwbaar.	☐
2	• Er is een configuratieprocedure vastgesteld om configuratie-items te identificeren en te onderhouden, maar deze procedure is niet geformaliseerd. • Geïnstalleerde software, configuraties en documentatie worden geregistreerd, maar de gegevensinhoud van opgenomen items is beperkt	☐
3	• Er bestaan geformaliseerde configuratieprocedures en werkmethoden om alle configuratie-items en hun attributen te identificeren en te onderhouden. • Alle middelen en wijzigingen in middelen worden gemonitord en vastgelegd in een centrale repository.	☐
4	• Er is een proces voor het periodiek evalueren van relevante documentatie, tijdige uitvoering en integriteit van het configuratie database.	☐
5	• Er wordt voortdurend geanalyseerd of er afwijkingen zijn en gevonden afwijkingen worden onderzocht.	☐

6. Incident/Problem Management

Binnen de IT zijn er diverse beheerprocessen die eigenlijk in elke organisatie aandacht horen te krijgen. Incident en problem management zijn hier onderdeel van. Bij incident management gaat het erom zo snel mogelijk verstoringen van de continuïteit te verhelpen. Door hierbij een eenduidig proces te volgen met duidelijke verantwoordelijkheden voor betrokken functionarissen, worden incidenten gestructureerd behandeld. Nadat een incident geconstateerd of gemeld wordt, wordt geanalyseerd wat er aan de hand is. Op basis daarvan wordt bekeken welke actie eventueel moet worden genomen.

Onderstaande stellingen hebben betrekking op hoe incident en problem management is ingeregeld binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Incidenten worden bijgehouden en geëvalueerd op individuele basis. • Er zijn geen plannen/procedures om een gepaste afhandeling van (cyber) beveiligingsincidenten te garanderen. • Er zijn geen procedures om oorzaak en gevolg van incidenten te identificeren.	☐
2	• Response teams zijn ongetraind en afhankelijk van enkele belangrijke individuen. • Het management erkent de noodzaak om cyberincidenten af te handelen. • De registratie en documentatie van problemen en de bijbehorende oplossingen zijn gebrekkig en inconsistent.	☐
3	• De verantwoordelijkheid voor het oplossen van een incident is toegewezen. • De organisatie kan snel reageren op een verstoring, op gepaste schaal/escalatieniveau afhankelijk van mogelijke impact. • Er is een formele plek in de organisatie waar problemen geregistreerd, gecommuniceerd, geanalyseerd en toegewezen worden aan verantwoordelijken.	☐
4	• Incidenten worden proactief geanalyseerd om oorzaken te achterhalen.	☐
5	• Het oplossen van incidenten wordt regelmatig geanalyseerd om het proces te verbeteren en tekortkomingen en trends worden aan het management gerapporteerd.	☐

7. Change Management

Change Management, ook wel wijzigingenbeheer, gaat over het beheerst doorvoeren van wijzigingen in IT. Net als Incident- en Problem Management is het een IT-beheerproces. Ook hier werk je vanuit een vastgestelde procedure. Belangrijk is dat je daarin ook aandacht hebt voor het beoordelen van impact, het stellen van prioriteiten en wie er goedkeuring geeft voor een door te voeren wijziging.

Onderstaande stellingen hebben betrekking op hoe wijzigingenbeheer plaatsvindt binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Wijzigingen worden niet of gebrekkig gedocumenteerd. • Er is geen beveiligde testomgeving gedefinieerd en ingericht voor het ontwikkelen en testen van wijzigingen. • Er is geen beleid voor de overdracht van gewijzigde systemen naar productie.	☐
2	• Er is versiebeheer geïmplementeerd voor essentiële systeemparameters. • Er is een informeel beleid voor het gebruik van een testomgeving voor het ontwikkelen en testen van wijzigingen. • Er is een informeel beleid voor de overdracht van gewijzigde systemen dat essentiële aspecten, zoals goedkeuring van het proces, bevat.	☐
3	• Wijzigingen worden gedocumenteerd. Documentatie is correct en actueel. • Formeel beleid is vastgesteld en geïmplementeerd voor de testomgeving. • Er zijn procedures voor het gebruik van OTAP omgevingen. Er zijn ook goedkeuringsprocessen.	☐
4	• De kwaliteit en effectiviteit van het Change Management proces wordt periodiek geëvalueerd.	☐
5	• Tekortkomingen en trends worden regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen.	☐

8. Systeemontwikkeling

Dit domein is vooral relevant voor schoolbesturen die (enige) softwareontwikkeling in eigen huis doen. In andere gevallen kunnen de meeste normen binnen het domein als 'niet van toepassing' verklaard worden.

Onderstaande stellingen hebben betrekking op hoe systeemontwikkeling is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Systeem- en softwareontwikkeling gebeuren ad hoc. • Er is geen beleid voor toegangsrestricties tot de productieomgeving voor ontwikkelaars.	☐
2	• Er zijn richtlijnen voor veilig coderen die niet altijd worden toegepast. • Er is een beperkt beleid bepaald voor toegang tot productie voor ontwikkelaars.	☐
3	• De organisatie heeft een gestructureerde aanpak voor interne ontwikkeling en aanschaf van software geïmplementeerd. • Ontwikkelaars hebben geen schrijftoegang tot productie, en systeembeheerders die software overzetten naar productie hebben geen schrijftoegang tot de ontwikkel-, test- en acceptatie-omgeving.	☐
4	• Er is een verplicht beveiligings- en risicotrainingsprogramma voor ontwikkelaars.	☐
5	• Op basis van ontwikkelingen in dreigingen worden periodiek risicoanalyses uitgevoerd.	☐

9. Datamanagement

In het domein Datamanagement gaat het over het onderhouden van de volledigheid, beschikbaarheid, juistheid en de bescherming van gegevens. Bij datamanagement is het van belang dat er binnen de organisatie eigenaarschap is toegewezen voor alle informatie en informatiesystemen. De informatie en de systemen dienen geclassificeerd te worden, zodat het juiste beschermingsniveau kan worden toegepast.

Onderstaande stellingen hebben betrekking op hoe datamanagement is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Er is geen formeel beleid voor data-eigenaarschap of de uitwisseling van (gevoelige) data. • Er zijn geen formeel vastgelegde procedures voor opschoning en verwijdering van data.	☐
2	• Er is beleid voor (informatie)systeem- en data-eigenaarschap. • Er is een informeel beleid voor data-uitwisseling. • Er zijn informele procedures geïmplementeerd zodat apparatuur en media die gevoelige data bevatten worden verwijderd via een centraal punt in de organisatie.	☐
3	• Beleid en procedures worden naar de hele organisatie gecommuniceerd en toegepast op bedrijfskritische data en informatiesystemen. • Data die uitgewisseld wordt buiten de organisatie moet voor versturen versleuteld worden. • Apparatuur en media met gevoelige informatie worden zoveel mogelijk opgeschoond voor gebruik of verwijdering.	☐
4	• Eigenaarschap van belangrijke data (en systemen) wordt periodiek geëvalueerd.	☐
5	• Het voldoen aan het datamanagementbeleid wordt periodiek aan het senior management gerapporteerd.	☐

10. Identity & Access Management

Identity & Access Management, afgekort IAM, draagt zorg voor het beheren van de logische toegang tot informatie, informatiediensten en externe koppelingen. Met logische toegang wordt de toegang tot systemen bedoeld. Dit begint met het bepalen welke gebruikers en rollen toegang mogen hebben en het doorvoeren van toegangsrechten.

Onderstaande stellingen hebben betrekking op hoe IAM is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Er is geen beleid voor informatietoegang. • Evaluatie wordt ad hoc door individuen gedaan.	☐
2	• Functie-eisen zijn verbonden aan gebruikers-ID's. • Er is een procedure voor Identity & Access Management voor besturingssystemen en -applicaties, maar deze is niet formeel vastgelegd.	☐
3	• Gebruikers ID's en toegangsrechten worden bijgehouden in een centrale opslag. • Ongepaste toegangsrechten worden ingetrokken.	☐
4	• Maatregelen voor gebruikersidentificatie, gebruikersauthenticatie en het afdwingen van gebruikersrechten worden up-to-date gehouden en periodiek geëvalueerd en gedocumenteerd.	☐
5	• De performance en verbeteringen van de toegangsregelsprocedure en toepassingen worden voortdurend gevolgd.	☐

11. Security Management

Security Management gaat over de meer technische kant van informatiebeveiliging. Het zorgdragen dat risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid voor een informatievoorziening zo veel mogelijk geadresseerd en gemitigeerd worden. Hiervoor zijn richtlijnen noodzakelijk die het kader beschrijven waarbinnen dit gebeurt.

Onderstaande stellingen hebben betrekking op hoe security management is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Beleid voor het gebruik en beveiliging van mobiele apparaten en/of telewerkfaciliteiten ontbreekt. • Er is geen beleid voor patchmanagement. • Het belang van IT-infrastructuur wordt onderkend, maar er mist een consistente totaalaanpak. • Er is geen netwerkbeveiligingsbeleid.	☐
2	• Er is informeel beleid voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten. • Er is een informeel beleid voor patchmanagement. • Infrastructuurbescherming en -beschikbaarheid wordt ondersteund door enkele (formele) procedures en het belang van IT-infrastructuur is duidelijk. • Er is een informeel netwerkbeveiligingsbeleid.	☐
3	• Formeel beleid en procedures voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten worden gedocumenteerd en gecommuniceerd. • IT-personeel check handmatig de patchlevels van besturingssystemen, databases en applicaties. • Er is een helder gedefinieerd en door iedereen begrepen proces voor de bescherming en beschikbaarheid van de IT-infrastructuur. • Beveiligingstechnieken worden gebruikt voor toegangsautorisatie, beheer van informatiestromen en verschillende beveiligingszones.	☐
4	• De relevante procedures worden periodiek geëvalueerd op actualiteit en uitvoering.	☐
5	• Op basis van de periodieke assessment worden de procedures geëvalueerd en verbeterd.	☐

12. Fysieke beveiliging

Bij fysieke beveiliging gaat het om de maatregelen die genomen worden om een pand of specifieke ruimten binnen een pand te beschermen. Een school heeft een vrij open karakter. Dat kenmerk maakt dat fysieke beveiliging bij de meeste scholen niet zal gaan om de beveiliging van het gehele pand, al is bijvoorbeeld een alarm voor de nacht in veel gebouwen prima denkbaar.

Onderstaande stellingen hebben betrekking op hoe fysieke beveiliging is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Het beheer van faciliteiten en apparatuur is afhankelijk van de bekwaamheid van enkele individuen. • Er zijn geen procedures vastgelegd voor de administratie van fysieke toegang.	☐
2	• Er zijn beleidskaders voor fysieke beveiliging, maar deze zijn niet volledig en worden niet consequent gehanteerd. Overtreding van regels wordt niet opgemerkt. • Er zijn informele procedures om toegang tot specifieke ruimtes te beperken.	☐
3	• Er is een alomvattend, op risico's gebaseerd beleid inzake fysieke beveiliging, dat is gedocumenteerd, gecommuniceerd en wordt ondersteund door (toegangs-)systemen. • Er worden formeel vastgelegde procedures voor de administratie van fysieke toegang toegepast.	☐
4	• Daadwerkelijke toegang (en overtredingen van het toegangsbeleid) wordt streng gecontroleerd en periodiek bekeken.	☐
5	• De omgeving wordt beheerd en bewaakt door gespecialiseerde apparatuur en hardware ruimtes worden niet meer "bemand".	☐

13. IT-operatie

De onderwerpen binnen dit domein zijn vrij technisch van aard en betreffen feitelijk een drietal standaard IT-beheeractiviteiten die geborgd dienen te worden. In welke mate dit noodzakelijk is, of beter gezegd: of dit überhaupt voor een school allemaal van toepassing is, is afhankelijk van welke IT-taken zelf uitgevoerd worden en wat er uitbesteed is.

Onderstaande stellingen hebben betrekking op hoe de IT-operatie is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Er zijn geen procedures vastgesteld voor job processing. • Er zijn geen procedures voor back-up en herstel.	☐
2	• Er zijn verschillende runbooks voor productietaken beschikbaar en deze beschrijven in het algemeen taken en interfaces voor de meest relevante systemen. • Er zijn procedures voor back-up en herstel van systemen, applicaties, data en documentatie.	☐
3	• Het runbook bevat gedetailleerde informatie en instructies. • Er zijn passende procedures en beleid voor de back-up van systemen, applicaties, data en documentatie.	☐
4	• De operationele effectiviteit van back-up- en herstelprocedures worden periodiek geëvalueerd.	☐
5	• De performance van het back-up- en herstelproces wordt periodiek aan het (senior) management gerapporteerd.	☐

14. Bedrijfscontinuïteitsmanagement

In dit domein gaan de normen over het voorbereid zijn op grote verstoringen. Dit begint bij het weten welke processen kritiek zijn en snel opgestart dienen te worden bij een verstoring. Bij het onderwijs hebben we het dan al snel over het primaire proces van het verzorgen van onderwijs en het bekijken welke zaken randvoorwaardelijk zijn om hier doorgang aan te kunnen geven. Denk bijvoorbeeld aan het hebben van een fysiek gebouw om leerlingen te ontvangen, of een ondersteunende applicatie met internet om onderwijs op afstand te kunnen verzorgen. Daarnaast moet in kaart gebracht worden welke grote calamiteiten denkbaar zijn.

Onderstaande stellingen hebben betrekking op hoe het waarborgen van de continuit van de bedrijfsvoering is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• De IT-organisatie heeft een beperkt en algemeen herstelplan voor het netwerk en de systemen. • Er worden geen extra maatregelen genomen om verlies van data te voorkomen in geval van nood bij het primaire datacenter. • Er is geen mogelijkheid tot datareplicatie.	☐
2	• In het geval van een grote onderbreking kunnen betrokken belangrijke processen en systemen wellicht worden hersteld, maar herstelactiviteiten zullen waarschijnlijk ontoereikend zijn. • De organisatie accepteert het verlies van data tussen de laatste back-up en het moment van het incident.	☐
3	• Dankzij het herstelplan kan de organisatie waarschijnlijk belangrijke operationele processen voortzetten in het geval van een grote onderbreking. • In het geval van een incident is data op korte termijn beschikbaar.	☐
4	• De kwaliteit van datareplicatie wordt minstens jaarlijks (gedeeltelijk) getoetst.	☐
5	• Business continuïteitsplannen en gerelateerde processen worden periodiek geëvalueerd.	☐

15. Ketenbeheer

Het domein Ketenbeheer gaat over controle hebben op de uitbestede IT-diensten. Zeker binnen de onderwijssector worden veel Software-as-a-Service-oplossingen gebruikt (SAAS-oplossingen). Dit biedt voordelen, want de grotere organisaties die hierin gespecialiseerd zijn hebben veelal een hoger securityniveau dan een individuele school zelf zou kunnen bereiken.

Onderstaande stellingen hebben betrekking op hoe ketenbeheer is georganiseerd binnen uw organisatie. Geef aan welk niveau het **best** overeenkomt met de situatie binnen uw schoolbestuur:

Volwassenheidsniveau		Nulmeting
1	• Er is geen contract met bijbehorend service level agreement (SLA). • Contracten en/of SLA's worden getekend zonder een gedegen risicoanalyse van de externe partij. • Interne beheersing van externe partijen wordt niet geëvalueerd.	☐
2	• Er zijn enkele afspraken gemaakt over service levels. • Er is een proces voor risicomanagement van leveranciers gedefinieerd, maar deze is slechts gedeeltelijk geïmplementeerd. • Er zijn enkele procedures gedefinieerd voor adequate interne beheersing door externe partijen.	☐
3	• SLA bevat afspraken over periodieke rapportage van geleverde diensten en performance. • Over niet-gemitigeerde of geaccepteerde risico's wordt periodiek aan het (senior) management gerapporteerd. • De status van de interne beheersmaatregelen van de externe dienstverleners wordt periodiek geëvalueerd.	☐
4	• Er zijn procedures om te garanderen dat externe dienstverleners zich aan wet- en regelgeving houden.	☐
5	• De risico's met betrekking tot het vermogen van de leverancier om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten, worden voortdurend onderzocht en beperkt.	☐

Bijlage 3. Overzicht statements uit IBPDOC3 Toetsingskader

In de onderstaande tabel tonen we een overzicht van de statements uit IBPDOC3 Toetsingskader Informatiebeveiliging die Dialogic gebruikt heeft ten behoeve van de nulmeting. Ook geven we in deze tabel de koppeling weer tussen de gebruikte statements en de domeinen uit het Normenkader IBP FO.

Cluster	Statement	Domein IBP FO
Cluster 1		
1.1	Beleidsregels voor informatiebeveiliging	1
1.7	Classificatie van informatie	9
1.14	Analyse en specificatie van informatiebeveiligingseisen	3
1.15	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	15
1.16	Toeleveringsketen van informatie- en communicatietechnologie	15
1.17	Verantwoordelijkheden en procedures	2
1.18	Rapportage van informatiebeveiligingsgebeurtenissen	6
1.21	Scheiding van taken	2
Cluster 2		
2.2	Bewustwording, opleiding en training ten aanzien van informatiebeveiliging	4
2.3	Toegansrechten intrekken of aanpassen	4
2.4	Clear desk'- en 'Clear screen'-beleid	4
Cluster 3		
3.4	Fysieke toegangsbeveiliging	12
3.14	Veilig verwijderen of hergebruiken van apparatuur	9
3.16	Inventariseren van bedrijfsmiddelen	5
Cluster 4		
4.2	Scheiding van ontwikkel-, test- en productieomgevingen	8
4.5	Back-up van informatie	13
4.13	Respons op informatiebeveligingsincidenten	6
4.14	Informatiebeveiligingscontinüiteit implementeren	14
Cluster 5		
5.1	Beleid voor toegangsbeveiliging	10
5.3	Registratie en afmdelen van gebruikers	10
5.7	Geheime autenticatie-informatie gebruiken	10
5.8	Beperking toegang tot informatie	10
5.27	Bescherming van testgegevens	7
Cluster 6		
6.1	Beoordeling van toegangsrechten van gebruikers	11
6.2	Gebeurtenissen registeren	11
6.9	Naleving van beveligingsbeleid en -normen	1
6.10	Beoordeling van technische naleving	11

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl