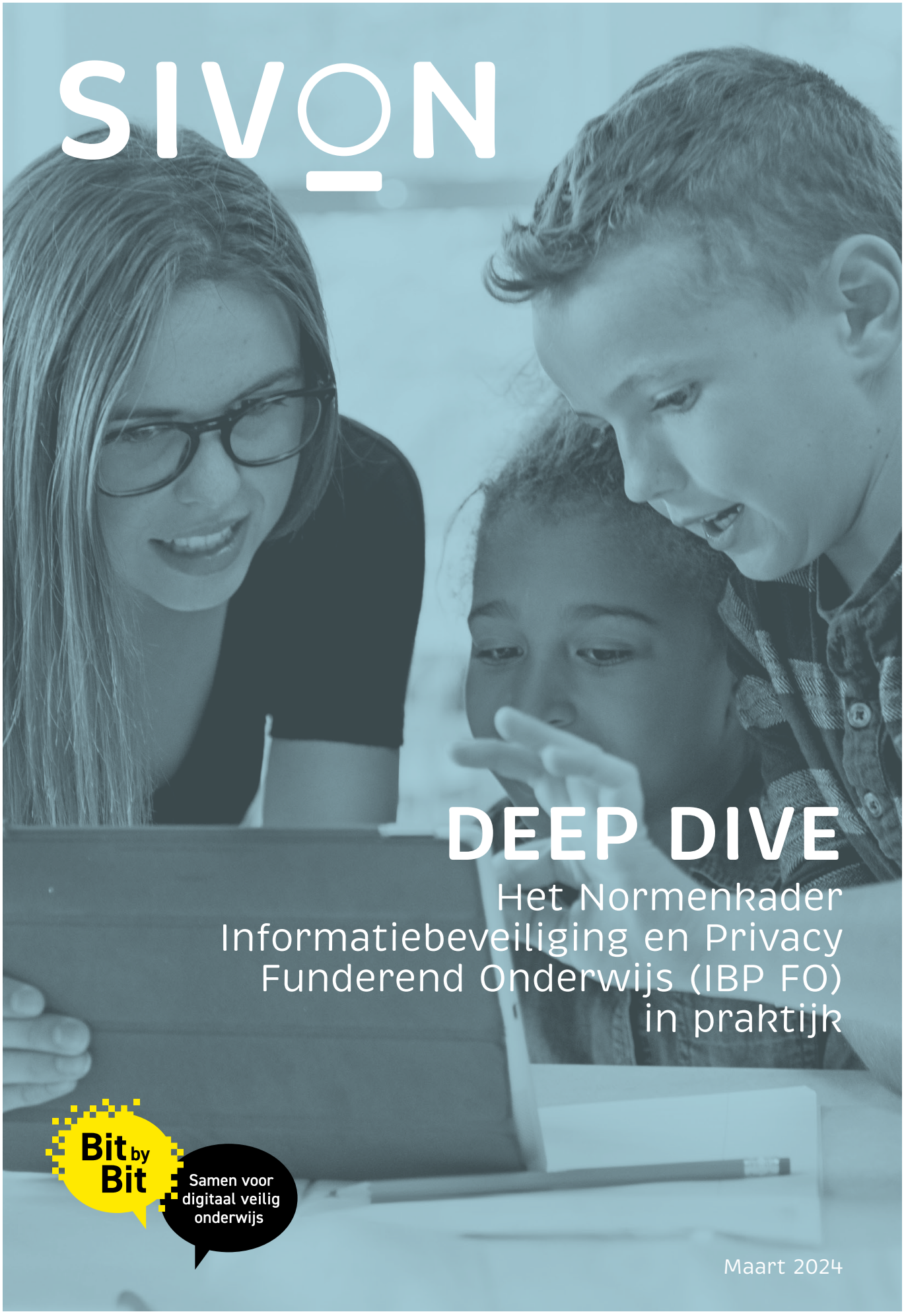

SIVON
DEEP DIVE
Het Normenkader
Informatiebeveiliging en Privacy
Funderend Onderwijs (IBP FO)
in praktijk
Bit by Bit
Samen voor digitaal veilig onderwijs
Maart 2024

1. Inleiding

In het project Deep Dive* heeft SIVON de IBP-status van veertien schoolbesturen binnen het primair en voortgezet onderwijs getoetst via een assessment. De basis van dit assessment, was het *Normenkader Informatiebeveiliging en Privacy voor Funderend Onderwijs (IBP FO).* In dit normenkader staan 15 domeinen met in totaal 69 normen voor informatiebeveiliging. In dit rapport vind je de samenvatting van de resultaten van de veertien schoolbesturen. Ook geven we weer welke producten en diensten de onderwijssector nodig heeft om het Normenkader IBP FO goed te kunnen uitvoeren.

De Deep Dive is als volgt verdeeld over de onderwijssectoren

	Klein	Midden	Groot
vo	3	2	
Combinatie po en vo	1		3
po	3	2	

* Deep Dive is een van de projecten binnen het programma *Digitaal Veilig Onderwijs* (DVO). Met dit programma bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

2. Het assessment

In het assessment zijn de vijf volwassenheidsniveau's gehanteerd die horen bij het normenkader van de Nederlandse Beroepsorganisatie van Accountants (NBA). Per norm is een score gegeven die hoort bij het geconstateerde volwassenheidsniveau. De vijf volwassenheidsniveau's vind je in de tabel. Niveau 1 is het laagst en niveau 5 het hoogst haalbare. Volwassenheidsniveau 3 is het doel.

Volwassenheidsniveau	Omschrijving
1 Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.
2 Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde maar op informele wijze uitgevoerd.
3 Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.
4 Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.
5 Continue verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risico-management raamwerk, waarbij continu gezocht wordt naar verbetering.

Tabel 1. De vijf volwassenheidsniveau's

Ervaren auditors hebben de assessments binnen de veertien schoolbesturen uitgevoerd. Tijdens een assessment wordt gesproken met de verantwoordelijken voor informatiebeveiliging, privacy, IT, facilitair, inkoop en bestuur.

3. Samenvatting

Het gemiddelde geconstateerde volwassenheidsniveau is 1,9 op een schaal van 5. Uit de assessments blijkt dat de implementatie van informatiebeveiliging nog niet op het gewenste niveau van 3 ligt. Het streven is dat scholen in 2027 op dat niveau zitten.

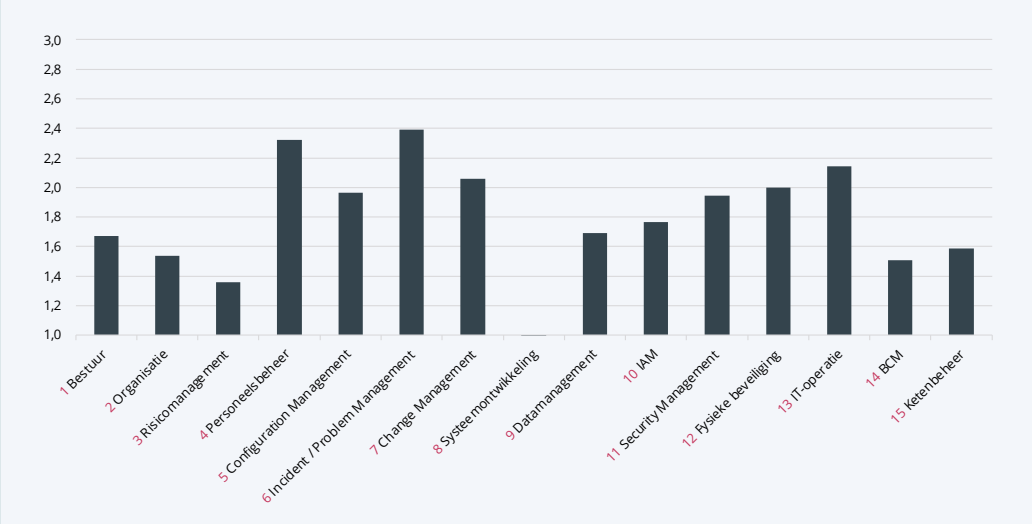
Er zijn meerdere aanbevelingen:

1. Voer een onderzoek uit naar de mogelijkheden van een sectorbreed kenniscentrum IBP.
2. Centraliseer leveranciersmanagement op sectorniveau.
3. Start een onderzoek naar welke vorm van dienstverlening het beste aansluit per type schoolbestuur.
4. Ontwikkel voor schoolbesturen een standaard aanpak voor het Normenkader IBP FO.
5. Initieer grotere bewustwording bij schoolbesturen met meer nadruk op het belang van IB.
6. Stel op korte termijn handreikingen ter beschikking aan schoolbesturen.
7. Bespreek welke wijzigingen in het Normenkader IBP FO wenselijk zijn.

4. Volwassenheid schoolbesturen

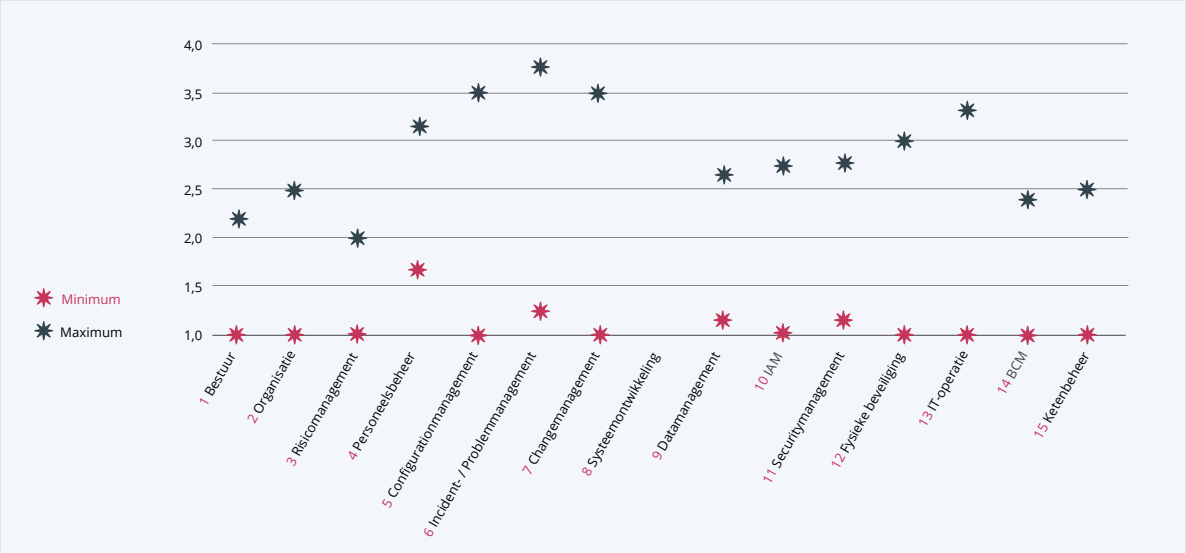
Het totale geconstateerde volwassenheidsniveau van de veertien schoolbesturen varieert tussen de 1,5 en 2,7. Het gemiddelde volwassenheidsniveau is 1,9. Geen enkel schoolbestuur voldoet hiermee volledig aan het toetsingskader. Toch zijn er wel verschillen in volwassenheid.

In onderstaande figuur vind je de gemeten volwassenheid per domein van het normenkader. Gemiddeld behalen de schoolbesturen op geen van de 15 domeinen niveau 3. Domein 8 Systeemontwikkeling ontbreekt omdat deze voor de meeste scholen niet relevant is.



Grafiek 1. Volwassenheidsniveau per domein

Kijkend naar de hoogste en laagste score per domein blijkt dat de volwassenheid divers is. Er zijn schoolbesturen die een domein niet geïmplementeerd hebben, maar ook schoolbesturen die voor sommige domeinen al boven het benodigde niveau zitten.



Grafiek 2. Spreiding volwassenheid per domein

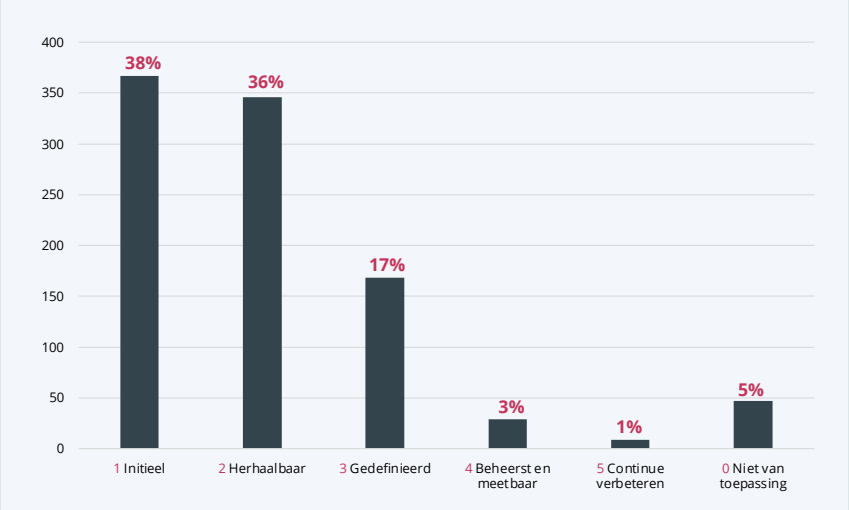
De top 3 van de meest volwassen domeinen uit het normenkader:

- Incident & Problem management (6). Het belang van een goed incidentenproces is evident.
- Personeelsbeheer (4) waarbij het resultaat nog negatief wordt beïnvloed doordat een vereiste als awareness bij de meeste schoolbesturen ontbreekt. Anders voldeed dit domein bij de meesten aan het vereiste volwassenheidsniveau.
- IT-operatie (13). Dit komt omdat dit onderdeel vaak belegd is bij een externe IT-partner.

De top 3 van minst volwassen domeinen uit het normenkader:

- Nagenoeg geen enkel schoolbestuur voldoet aan Risicomanagement (domein 3).
- Business Continuity (14) waaronder ook crisismanagement, ontbreekt bijna volledig.
- De informatiebeveiligingsorganisatie (2) met een beschrijving van taken en verantwoordelijkheden in de organisatie ontbreekt nagenoeg.

Gelet op de 69 normen valt 38% in volwassenheidsniveau 1 en 36% in niveau 2. Het percentage dat minimaal aan niveau 3 voldoet, is 21% en 5% is niet van toepassing (voornamelijk domein 8 Systeemontwikkeling).



Grafiek 3. Aantal normen per volwassenheidsniveau

Uitschieters in volwassenheidsniveau's van normen

Op de 69 normen zijn er zowel positieve als negatieve uitschieters.

ID	Domein	Titel	Gemiddeld
1.2	Bestuur	Beleid	2,5
4.1	Personeelsbeheer	Werving	2,9
4.2	Personeelsbeheer	Certificering, training en scholing	2,5
4.4	Personeelsbeheer	Verandering of beëindiging van functie	2,8
6.2	Incident & Problem Management	Incident-escalatie	2,6
11.11	Security Management	Network security	2,5

tabel 2. Positieve uitschieters met een gemiddelde volwassenheidniveau van 2,5 of hoger

ID	Domein	Titel	Gemiddeld
1.4	Bestuur	Architectuur	1,2
1.5	Bestuur	Onafhankelijke assurance	1,1
2.2	Organisatie	Functiescheiding	1,4
3.1	Risicomanagement	Raamwerk voor informatierisicomanagement	1,2
3.2	Risicomanagement	Risicobeoordeling	1,4
3.3	Risicomanagement	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	1,5
9.1	Datamanagement	Data en systeemeigenaarschap	1,4
9.2	Datamanagement	Classificatie	1,3
11.3	Security Management	Mobiele apparaten en telewerken	1,2
11.4	Security Management	Logging	1,3
11.5	Security Management	Testen van, inspectie van en toezicht op beveiliging	1,5
11.10	Security Management	Cryptographic Key Management	1,5
14.1	BCM	Bedrijfscontinuïteitsplanning	1,4
14.2	BCM	Testen van Disaster Recovery	1,1
14.5	BCM	Crisismanagement	1,3
15.2	Ketenbeheer	Service Level Management	1,5
15.3	Ketenbeheer	Leveranciersrisicomanagement	1,4
15.4	Ketenbeheer	Interne beheersing bij derden	1,2

tabel 3. Negatieve uitschieters met een gemiddelde volwassenheidniveau van 1,5 of lager

5. Succesfactoren

In onderstaande tabel vind je een overzicht van belangrijke factoren uit de assessments, die direct invloed hebben op het wel of niet succesvol implementeren van het normenkader.

Factoren die bijdragen aan succes	Factoren die succes bemoeilijken
Commitment vanuit het schoolbestuur om beveiliging op een hoger niveau te brengen	
	Geen prioriteit aan IB waardoor geen draagvlak ontstaat.
	Onbegrip over de haalbaarheid om aan het Normenkader IBP FO te voldoen.
Bestuurder met affiniteit IT (vooral bij kleinere besturen).	
Bij grotere besturen een leidinggevende met affiniteit IT.	
	Geen affiniteit met IT van schoolbestuur waardoor alles als vreemd en overbodig wordt ingeschaald. Ervaren het als papieren romp-slomp in plaats van een kader voor groei.
Volledige IT is uitbesteed aan een IT-partner die ISO27001 gecertificeerd is en alle IT gerelateerde diensten levert.	Versplinterde uitbesteding of uitbesteding aan een minder professionele partij.
Ondersteunende diensten als IT, Facilitair, HR en Inkoop zijn bovenschools georganiseerd.	Hoge mate van autonomie van individuele scholen binnen een schoolbestuur waardoor de ondersteunende diensten divers zijn vormgegeven.
Gebruik maken van handreikingen/ standaarden die voor de sector beschikbaar zijn. Regionaal overleg met collega's.	Zelf het wiel uitvinden, niet weten waar informatie te vinden is.

Tabel 4. Belangrijke factoren uit de assessments

6. Aanbevelingen

Toelichting op de aanbevelingen die zijn opgedaan uit de assessments. De eerste drie aanbevelingen worden binnen het programma Digitaal Veilig Onderwijs verder onderzocht.

1. **Voer een onderzoek uit naar de mogelijkheden van een sectorbreed kenniscentrum IBP.**
   Veel kennis en capaciteit voor IB is nu gefragmenteerd beschikbaar. Een kenniscentrum IBP verzamelt informatie uit verschillende bronnen en stelt deze beschikbaar aan het onderwijs. Schoolbesturen kunnen gerelateerde vragen stellen en ondersteuning krijgen bij dit kenniscentrum IBP.

2. **Centraliseer leveranciersmanagement op sectorniveau.**
   Schoolbesturen verwachten dat het leveranciersmanagement op centraal niveau plaatsvindt en willen erop kunnen vertrouwen dat er centraal advies wordt gegeven. Een aantal diensten is al centraal georganiseerd, zoals het toetsen van verwerkersovereenkomsten en het uitvoeren van DPIA-trajecten. Door een uitbreiding naar IB-vereisten ontzorgen we individuele schoolbesturen en ontstaat een centraal aanspreekpunt naar leveranciers.

3. **Start een onderzoek naar welke vorm van dienstverlening het beste aansluit per type schoolbestuur.**
   Afhankelijk van de grootte van het schoolbestuur en hoe het is georganiseerd, zijn er andere uitdagingen om invulling te geven aan informatiebeveiliging. Welke vorm van dienstverlening het beste aansluit per type schoolbestuur is met de opgedane informatie nog moeilijk vast te stellen waarbij verder onderzoek nodig is naar behoeftes en invulling.

Vier aanbevelingen krijgen al een plek binnen het programma DVO:

4. **Ontwikkel voor schoolbesturen een standaardaanpak voor het Normenkader IBP FO.**
   Veel schoolbesturen weten nog niet wat een goede manier van aanpak is om met het Normenkader IBP FO aan de slag te gaan. Daarom is het goed om een standaardaanpak te maken.

5. **Initieer cultuurverandering bij schoolbesturen met meer nadruk op het belang van IB.**
   Zonder draagvlak en prioriteit vanuit het schoolbestuur zijn wezenlijke verbeteringen niet haalbaar. Dat is wel voorwaardelijk om IB binnen een aantal jaren naar het gewenste niveau van volwassenheid te brengen.

6. **Stel op korte termijn handreikingen ter beschikking aan schoolbesturen.**
   Zorg dat handreikingen en diensten beschikbaar zijn, waardoor de drempel om te starten voor schoolbesturen lager wordt.

7. **Bespreek welke wijzigingen in het Normenkader IBP FO wenselijk zijn.**
   Een beter draagvlak kan ontstaan door het normenkader op een aantal punten te verbeteren. Dit kan bijvoorbeeld door het volwassenheidsmodel van vijf niveaus toe te voegen aan het normenkader met de mogelijkheid sommige normen niet van toepassing te verklaren.