Digitaal Veilig Onderwijs

Programmaplan

Ministerie van Onderwijs, Cultuur en Wetenschap

Kennisnet

SIVON

PO RAAD

VO RAAD

Auteur: **Programma Digitaal Veilig Onderwijs**
Concept, ontwerp en realisatie: **Kris Kras context, content & design**
Versie: **Versie 1.0**
Datum: **23-03-2023**

Inhoudsopgave

Inleiding

AANLEIDING

De risico's op het gebied van informatiebeveiliging en privacy (IBP) in het digitale domein worden groter. Het onderwijs maakt steeds meer gebruik van leerlingdata en digitale middelen en is daardoor sterk afhankelijk van ICT. Er zijn vaker privacy- en beveiligingsincidenten, ook in het funderend onderwijs. Naar aanleiding van deze incidenten investeert de minister voor Primair en Voortgezet Onderwijs in het verhogen van de digitale veiligheid van het funderend onderwijs. Dit plan geeft hier invulling aan.

Om te zorgen voor een digitaal veilige leeromgeving voor alle leerlingen, is een gecoördineerde en integrale aanpak nodig. Overheid, onderwijsbesturen en publieke en private ondersteuningspartijen hebben hierin allemaal een rol te vervullen. Daarom neemt het ministerie van OCW het initiatief voor het programma Digitaal Veilig Onderwijs (DVO). Dit doet zij samen met haar partners: de PO-Raad, de VO-raad, SIVON en Kennisnet.

De aanpak is integraal, omdat privacy en beveiliging over zeer verschillende thema's gaan. Deze variëren van bestuurlijke aandacht en gedrag van medewerkers tot techniek en leveranciersmanagement. Daarnaast vragen het bewaken van integraliteit en de noodzaak om tempo te maken om een programmatische aanpak. Zo hoeven schoolbesturen niet zelf het wiel opnieuw uit te vinden.

Het programma biedt duidelijkheid over wat schoolbesturen kunnen doen om 'digitaal veilig' te zijn. Het zorgt daarmee voor bewustwording onder onderwijsbestuurders. Ook biedt het praktische ondersteuning aan besturen in de vorm van onder andere kennis, handreikingen, technische dienstverlening, leveranciersmanagement en praktische hulp bij incidenten. Schoolbestuurders en IBP'ers worden nadrukkelijk betrokken bij het tot stand komen van de middelen voor dit programma.

AMBITIE

De ambitie is dat elke leerling moet kunnen leren in een veilige omgeving: ongeacht op welke school de leerling zit. Digitale veiligheid is een basisvoorwaarde die op elke school in orde moet zijn.

Om dit te kunnen bewerkstelligen, moeten scholen weerbaar zijn tegen digitale dreigingen. Medewerkers moeten verstandige keuzes maken over de persoonsgegevens van leerlingen en digitale producten waarvan het onderwijs gebruikmaakt, moeten voldoen aan alle wensen en (wettelijke) eisen met betrekking tot privacy en informatiebeveiliging.

CONTEXT

De Monitor IBP (informatiebeveiliging en privacy) 2020 laat zien dat scholen in het funderend onderwijs de laatste jaren hard aan de slag zijn gegaan met het thema privacy. Tegelijkertijd wordt duidelijk dat er ook nog veel te doen is[1], bijvoorbeeld op het gebied van verwerkersovereenkomsten, Data Protection Impact Assessments (DPIA's) en bewustwording. Een school is tegenwoordig voor een belangrijk deel een ICT-organisatie. Zelfs een kleine school in het basisonderwijs heeft al gauw te maken met tweehonderd apparaten die leraren en leerlingen gebruiken. Binnen een gemiddeld schoolbestuur in het voortgezet onderwijs zijn dit er vierduizend[2 en 3]. Door de corona-lockdowns is het gebruik van digitale leermiddelen en apparaten voor les op afstand toegenomen. Dat biedt veel voordelen, maar zorgt ook dat het Nederlandse onderwijs enorm afhankelijk is van ICT.

Als er geen verbinding is met het internet of als cruciale applicaties (het leerlingadministratiesysteem, de leeromgeving of specifieke leermiddelen) niet toegankelijk zijn, staat het onderwijs stil. Er zijn hiervan al veel voorbeelden, bijvoorbeeld van lessen die niet door konden gaan na een DDoS-aanval[4]. Of een school die dagenlang geen volledig onderwijs kon geven door een aanval met ransomware[5]. Bij een ICT-storing komt ook de bedrijfsvoering onder druk te staan, bijvoorbeeld de processen rondom het betalen van salarissen of facturen.

Vier op de tien instellingen in het vo en mbo hadden in 2020 te maken met (een van) bovenstaande problemen[6].

1 https://www.kennisnet.nl/artikel/7733/monitor-ibp-2020-privacy-goed-opgepakt-meer-aandacht-nodig-voor-informatiebeveiliging/
2 Schatting, gebaseerd op een gemiddeld aantal leerlingen van 2898. https://www.vosabb.nl/wp-content/uploads/2020/06/literatuurstudie-schaalgrootte-in-het-primair-en-voortgezet-onderwijs.pdf
3 https://www.nrc.nl/nieuws/2021/02/26/gelderse-school-betaalt-losgeld-vanwege-hack-maandag-geen-les-a4033498
4 https://www.poraad.nl/schoolontwikkeling/digitalisering/advies-waarom-regie-op-ict-geen-uitstel-duldt
https://nos.nl/artikel/2374070-leerlingen-school-in-leeuwarden-verstoren-lessen-met-ddos-aanvallen
5 https://dutchitchannel.nl/703269/ransomware-aanvallen-op-onderwijsinstellingen-nemen-toe.html
6 IT-beveiliging binnen het voortgezet en middelbaar beroepsonderwijs, Kantar & Breens Network, 2021
https://breens.nl/whitepapers/whitepaper-veiligere-hybride-onderwijsomgeving/

DOELGROEPEN

De verandering moet gaan plaatsvinden binnen het schoolbestuur. We kiezen daarom het bevoegd gezag (het schoolbestuur) als de belangrijkste actor voor het goed regelen van privacy en beveiliging in het onderwijs[7].

Binnen het schoolbestuur richten we ons op twee primaire actoren. In de eerst plaats de bestuurder. Voldoende aandacht voor IBP begint bij de bestuurder. De tweede belangrijke actor is de IBP'er. Deze verzamelterm gebruiken we voor degenen die belast zijn met de uitvoeringsverantwoordelijkheid van IBP-maatregelen binnen een onderwijsorganisatie. Soms is dat binnen een bestuur één persoon, soms meerdere personen. We spreken de IBP'er aan als de persoon die we vanuit het programma ondersteuning bieden bij het in de praktijk brengen van IBP-maatregelen. Tot slot heeft ook de schoolleider een belangrijke rol in deze verandering en wordt ook deze in het programma aangesproken.

Deze afbakening houdt in dat informele vormen van leren (bijvoorbeeld met een bureau in huiswerkondersteuning of een app die ouders zelf inzetten voor het leren van hun kind) niet binnen dit programma vallen. Als een externe organisatie, app of medewerker wordt ingezet in opdracht – en daarmee onder verantwoordelijkheid – van de school, valt dit wél binnen het programma.

OORZAKEN

In het algemeen zijn er drie voorname oorzaken waardoor het funderend onderwijs onvoldoende digitaal veilig is[8]:

1. **Het is voor schoolbesturen onvoldoende duidelijk wat 'digitaal veilig' betekent en wat zij daarvoor moeten doen**

In de eerste plaats is onduidelijk wat er van schoolbesturen wordt verwacht om hun onderwijsorganisatie 'digitaal veilig' te maken. Wettelijke kaders voor informatiebeveiliging en privacy zijn open geformuleerd. Wat veilig genoeg is, is op dit moment niet eenduidig te beantwoorden. Ook is onvoldoende duidelijk welke activiteiten een schoolbestuur moet ondernemen om digitaal veilig te zijn.

2. **Schoolbesturen ervaren de consequenties van het niet goed regelen van informatiebeveiliging en privacy onvoldoende**

Hoewel er genoeg voorbeelden zijn waarin het op grote of kleinere schaal mis is gegaan binnen een school, leidt dit zelden tot grootschalige investeringen in digitale veiligheid. Veel gehoorde reacties zijn: 'Dat overkomt ons toch niet', 'Wij hebben alles goed geregeld', 'Wij zijn zo klein dat we niet interessant zijn voor zoiets' en 'Alles staat bij ons toch in de cloud'. Het start dus bij de bestuurders: zij moeten zich bewust zijn van de risico's en de verantwoordelijkheid van het schoolbestuur om digitale veiligheid goed te organiseren.

3. **Het is voor individuele schoolbesturen zeer kostbaar en in sommige gevallen nauwelijks uitvoerbaar om alle passende maatregelen op het gebied van privacy en cybersecurity te organiseren**

Het digitale beveiligingsvraagstuk is complex: de wereld van cybersecurity is omvangrijk, specialistisch en het verandert razendsnel. Ook vergen privacymaatregelen specialistische juridische kennis. De kosten van het inhuren of inkopen van expertise en uitvoeringscapaciteit zijn (vanwege schaarste op de arbeidsmarkt) hoog, nog los van de vraag of er überhaupt voldoende capaciteit beschikbaar is. Ook beveiligingsmaatregelen zelf zijn duur en vergen soms forse investeringen van een schoolbestuur.

Daarnaast is het voor individuele schoolbesturen moeilijk om specifieke maatregelen af te dwingen bij een leverancier. Dit geldt voor kleine schoolbesturen, maar ook voor grote. Google paste haar privacyvoorwaarden immers pas aan toen de voltallige Nederlandse onderwijssector samen met de Rijksoverheid optrok om te eisen dat zij Google Workspace conform de AVG konden gebruiken[9].

Tot slot zijn er binnen onderwijsinstellingen veel prioriteiten die op een meer directe, zichtbare wijze bijdragen aan de kwaliteit van het onderwijs. Qua aandacht en middelen krijgen die vaak voorrang.

BELANGRIJKSTE RISICO'S

Waarom en waartegen moeten schoolbesturen zich wapenen door digitaal weerbaar en veilig te zijn? Hieronder een aantal veelvoorkomende risico's.

Ongewenst gebruik van persoonsgegevens door leveranciers

Persoonsgegevens van leerligen en medewerkers staan bijna nooit bij de school zelf, maar in de cloud. Dat betekent dat schoolbesturen goede afspraken moeten maken met deze softwareleveranciers over wat ze wel en niet met die gegevens mogen doen. Wanneer er geen goede afspraken zijn vergroot dit de kans dat gegevens op straat komen te liggen of dat leerlingen geconfronteerd worden met reclamecampagnes of dat hun gegevens worden doorgespeeld aan andere partijen.

Ransomware als verdienmodel

Met ransomware worden systemen geblokkeerd of (persoons) gegevens gegijzeld en losgeld gevraagd, zodat het onderwijs stil komt te liggen. Hiervoor zoeken hackers al lang niet alleen meer de grote vissen op, maar is iedere organisatie, groot of klein een doelwit. Hackers kunnen ook overgaan tot het publiceren van gevoelig informatie over leerlingen en medewerkers. Dit kan niet alleen impact hebben op het primaire proces, maar ook ook bedrijfsvoering zoals het kunnen betalen van salarissen.

Handige leerlingen

Een DDoS-aanval, waarmee de systemen van een school plat komen te liggen, is online voor een paar euro voor iedereen verkrijgbaar. Het wachtwoord van het leerlingadministratiesysteem van de leraar afkijken om vervolgens je eigen cijfers aan te passen is soms een fluitje van een cent. Handige leerlingen vormen hiermee ook een dreiging voor schoolbesturen.

Personeel: een ongeluk zit in een klein hoekje

Een van de voornaamste risico's voor privacy en beveiliging zit in het gedrag van mensen, in het bijzonder van het personeel van een schoolbestuur. Een foutje is zo gemaakt: het versturen van gevoelige persoonsgegevens naar de verkeerde persoon, je laptop uitlenen aan een leerling die daarmee toegang heeft tot jouw inloggegevens of het klikken op een link in phishingmail.

7 In dit plan wordt consequent gesproken over het onderwijsbestuur als actor en juridisch verantwoordelijke. Strikt genomen ligt deze rol bij het bevoegd gezag. Hieronder kan ook een samenwerkingsverband in het kader van passend onderwijs worden verstaan. Voor de leesbaarheid van de stukken wordt de term 'schoolbestuur' gebruikt, maar deze dient gelezen te worden als 'bevoegd gezag'.

8 Kwantitatief onderzoek hiernaar is niet beschikbaar. Daarom is een nulmeting een belangrijke activiteit in de eerste fase van het programma.

9 https://sivon.nl/2021/07/akkoord-onderwijs-met-google-over-privacyrisicos/

ALGEMENE UITGANGSPUNTEN

Voor het programma Digitaal Veilig Onderwijs (DVO) zijn vier algemene uitgangspunten geformuleerd: een ketenbrede aanpak, een gefaseerde en op risico's gebaseerde uitvoering, centrale regie en kaderstelling en centrale ondersteuning en samenwerking. We lichten de vier uitgangspunten kort toe.

1. Ketenbrede aanpak
Het bereiken van digitale veiligheid binnen schoolorganisaties vraagt om een ketenbrede aanpak. Dit betekent dat zowel schoolbesturen als de landelijke (ondersteunings)partijen (zoals SIVON, Kennisnet, sectorraden en het ministerie) samen optrekken. Alleen als iedereen binnen de keten meedoet en het totaal aan activiteiten in samenhang ontwikkelt en inzet, kunnen alle schoolorganisaties digitaal veilig worden.

2. Gefaseerde en op risico's gebaseerde uitvoering
Het programma Digitaal Veilig Onderwijs (DVO) is gericht op het verminderen van risico's. We prioriteren activiteiten dan ook zoveel mogelijk op basis van de mate van risicobeperking die ze opleveren. De grootste risico's voor leerlingen en schoolbesturen moeten we het eerst wegnemen. Daarnaast is in de implementatiestrategie veel aandacht voor de balans tussen het wegnemen van risico's en de praktische uitvoerbaarheid hiervan voor scholen.

3. Centrale regie
Een grote mate van autonomie is gewenst. Tegelijkertijd is het digitaal veilig maken van het funderend onderwijs een urgente kwestie. Daarom is het belangrijk dat dit thema uit de sfeer van vrijblijvendheid wordt gehaald en er centrale regie wordt genomen. Met handhaving op basis van wetgeving als uiterste consequentie. Ook de Autoriteit Persoonsgegevens en de Onderwijsinspectie pleiten voor centrale regie.

4. Centrale ondersteuning en samenwerking
Vanuit het programma stellen we schoolbesturen in staat een digitaal veilige schoolorganisatie te realiseren. Hiervoor creëren en beheren we verschillende instrumenten, waaronder het normenkader. Belangrijk is ook het beschikbaar stellen van toepasbare kennis en ondersteuning in de vorm van stappenplannen en tools die IBP'ers kunnen inzetten binnen hun organisatie. Ook zorgen we voor sectorale risicoanalyses, een veilige landelijke ICT-infrastructuur en voeren we gezamenlijk leveranciersmanagement om te zorgen dat contracten met leveranciers de juiste maatregelen bevatten en dat deze ook regelmatig worden gecontroleerd.

OMGAAN MET DYNAMIEK

- Digitale veiligheid is aan verandering onderheven. Daarom richten we ons op digitale veiligheid duurzaam op orde krijgen en houden. Omgaan met verandering is het uitgangspunt voor schoolbesturen.
- De normen die gelden voor digitale veiligheid, en in het bijzonder de uitwerking hiervan in concrete maatregelen, zal periodiek worden herijkt. De wijze waarop en de lengte van de cycli worden nog uitgewerkt. Het betekent dat wie in januari aantoonbaar aan de geldende versie van het normenkader voldoet, niet achterover kan leunen. Immers, drie maanden na een certificering van een schoolbestuur kunnen door ontwikkelingen (nieuwe) mitigerende maatregelen nodig zijn.
- Het ondersteuningsaanbod moet ook in staat zijn mee te bewegen met ontwikkelingen. Niet alleen in de kennis die beschikbaar is, maar ook de technische ondersteuning. Waar nu multifactorauthenticatie de norm is, kan het zijn dat dit later verandert naar 'wachtwoordloos inloggen'. Sectorale coördinatie en ondersteuning hiervan moet dan tijdig geregeld worden. Deze flexibiliteit is verankerd in de programmasturing.
- En zelfs als alle scholen alle maatregelen implementeren, dan nog gaat het van tijd tot tijd mis en is er een datalek of beveiligingsincident. Ook daarvoor ontwikkelt het programma ondersteuningsaanbod: snel en adequaat reageren op incidenten, zo snel mogelijk de systemen en het onderwijs weer operationeel krijgen en leren van wat er misging.

Ook wanneer de programmaperiode is afgelopen gelden bovenstaande vier punten. Het overgrote deel van de programmaactiviteiten zullen we ook hierna in stand moeten houden en continu vernieuwen.

2

Doelen en strategie

KERNPROBLEMEN EN AANPAK

Om verandering in de hele sector funderend onderwijs te realiseren, richten we ons op de drie eerder beschreven kernproblemen:

1. Het is voor schoolbesturen onvoldoende duidelijk wat 'digitaal veilig' betekent en wat zij daarvoor moeten doen

2. Schoolbesturen ervaren de consequenties van het niet goed regelen van informatiebeveiliging en privacy onvoldoende

3. Het is voor individuele schoolbesturen zeer kostbaar en in sommige gevallen nauwelijks uitvoerbaar om alle passende maatregelen op het gebied van privacy en cybersecurity te organiseren

Onze **aanpak** gaat uit van:

- **Duidelijkheid voor alle schoolbesturen**
  Op basis van een landelijk normenkader voor informatiebeveiliging en privacy is voor alle schoolbesturen duidelijk wat zij moeten doen om digitaal veilig te zijn. Het normenkader doet recht aan de specifieke context van het funderend onderwijs en is praktisch toepasbaar. Schoolbesturen kunnen aan de hand van dit kader bepalen waar ze staan en wat hun vervolgstappen zijn.

- **Bewustwording en een stok achter de deur**
  We bieden bewustwordings- en professionaliseringsactiviteiten in het kader van digitale veiligheid en bescherming van privacy. Daarmee krijgen we schoolbesturen in beweging om hun IBP goed te regelen. Daarnaast benadrukt wet- en regelgeving dat beveiliging niet vrijblijvend is.

- **Ondersteuning zodat ieder bestuur op een (doelmatige) manier aan de slag kan**
  De opgave voor schoolbesturen op het thema informatiebeveiliging en privacy is groot. Het grootste deel van het programma gaat daarom over effectieve ondersteuning voor schoolbesturen om deze opgave te realiseren: het centraal opbouwen en verspreiden van de kennis die binnen elk bestuur nodig is, het centraal en gezamenlijk organiseren van leveranciersmanagement, publieke diensten die scholen informeren over dreigingen en kwetsbaarheden en direct bijdragen aan een adequate oplossing bij een onverhoopt cyberincident.

  Kort gezegd: we organiseren centraal wat centraal georganiseerd kan worden. Dit aanbod is dermate passend bij de behoeften van de sector, dat schoolbesturen wel andere keuzes *kunnen* maken om hun digitale veiligheid te regelen, maar dit vanuit zowel veiligheids- als doelmatigheidsoverwegingen niet zullen doen.

DRIE NIVEAUS VAN ORDENING

Het programmaplan kent drie niveaus van ordening: strategische doelen, operationele doelen en programmalijnen. Elk niveau kent zijn eigen uitgangspunt.

- **Strategische doelen**: herkenbare doelen waarvan iedereen begrijpt dat we ze na moeten streven, zowel binnen schoolbesturen als in het programma. Ze zijn voor iedereen herkenbaar: 'Ik snap dat dit is wat we geregeld zouden moeten hebben'.

- **Operationele doelen**: deze doelen zijn meetbaar. Daarom hebben wij deze doelen, ook wel normen genoemd, ingedeeld in een normenkader. Ze zijn te vertalen als: 'Dit is wat ik zou moeten doen om voor digitale veiligheid te zorgen binnen mijn schoolorganisatie'.

- **Programmalijnen**: een logische indeling van activiteiten en samenwerking binnen het programma. Neem bijvoorbeeld de professionalisering van IBP-medewerkers. Die activiteit heeft betrekking op alle inhoudelijke operationele doelen, maar is het meest logsich om op te pakken in samenhang met de professionalisering van bestuurders, schoolleiders en andere medewerkers. Dit is een voorbeeld van hoe we het programma organiseren om schoolbesturen te ondersteunen en de doelen te realiseren.

STRATEGISCHE DOELEN

Het programma Digitaal Veilig Onderwijs (DVO) wil ervoor zorgen dat elke leerling kan leren in een digitaal veilige omgeving. Om deze ambitie te verwezenlijken zijn zes strategische doelen opgesteld. Deze doelen zijn grotendeels gebaseerd op het NIST Cybersecurity Framework[10]. Dit framework wordt internationaal gebruikt en maakt inzichtelijk dat digitale veiligheid meer behelst dan alleen het nemen van beschermende maatregelen. Het gaat uit van het identificeren van risico's, het beschermen van gegevens en systemen, het detecteren van dreiging, het reageren op incidenten en het herstellen hiervan. Privacy is geen gemeengoed in het NIST-model en ook de aanwezigheid van de juiste kennis is daarvan geen expliciet onderdeel. Omdat dit belangrijke componenten zijn voor het funderend onderwijs hebben wij deze toegevoegd.

De zes strategische doelen:

1. Schoolbesturen maken doordachte keuzes over het gebruik van persoonsgegevens

Het belang van het waarborgen van privacy voor leerlingen en medewerkers vraagt dat schoolbesturen kritisch zijn op de manier waarop ze persoonsgegevens inzetten en delen. Het doel is om ervoor te zorgen dat alle schoolbesturen doordachte keuzes maken en alle medewerkers het gebruik van persoonsgegevens tot een minimum beperken en waar ze het gebruiken, dit op een zorgvuldige manier doen. Immers, hoe minder er verwerkt wordt, hoe lager het risico en de impact van incidenten.

2. Schoolbestuurders, medewerkers en ingehuurd personeel in het funderend onderwijs beschikken over de benodigde IBP-kennis en -vaardigheden

We willen dat iedereen die werkt met persoonsgegevens en hiervoor verantwoordelijk is de kennis heeft om dit op een veilige manier te doen. Schoolbestuurders hebben actuele kennis nodig om te kunnen sturen op digitale veiligheid. Meer kennisdeling tussen IBP-medewerkers van schoolbesturen en landelijke experts is een must. Tot slot moeten ook leraren en andere schoolmedewerkers weten met welk gedrag ze de digitale veiligheid van leerlingen, de organisatie en henzelf goed borgen. Door kennis over het onderwerp en de wijze waarop ze hiermee moeten omgaan op een herkenbare en passende wijze beschikbaar te stellen, leggen we een belangrijk fundament waardoor schoolbesturen de kans op en impact van incidenten kunnen verminderen.

3. Schoolbesturen kennen hun eigen informatiehuishouding, datastromen en risico's

Om privacy te waarborgen en te bepalen welke beschermende maatregelen genomen kunnen worden, hebben schoolbesturen inzicht nodig in hun eigen informatiehuishouding, datastromen en risico's. Welke systemen worden er gebruikt, welke data worden verwerkt, welke afspraken zijn hierover gemaakt en zijn de contracten in orde? Dit inzicht helpt bij het beoordelen van dreigingen voor (leveranciers van) scholen evenals het snel kunnen reageren op en herstellen van incidenten.

4. Schoolbesturen treffen maatregelen om hun gegevens en systemen te beschermen

Op basis van bovengenoemd inzicht in de informatiestromen en bijbehorende veiligheidsrisico's van een school kunnen schoolbesturen passende, technische en organisatorische maatregelen nemen. Op deze manier kunnen besturen beter bepalen hoe ze hun scholen kunnen beschermen tegen dreigingen en zo de continuïteit van het onderwijs kunnen borgen en de veiligheid van persoonsgegevens beschermen.

5. Schoolbesturen zijn op de hoogte van dreigingen en nemen op basis hiervan de juiste maatregelen

Het is van groot belang dat schoolbesturen hun dreigingsdetectie en de reactie hierop op orde krijgen. Ondanks preventieve, beschermende maatregelen zijn er nog steeds veel cyberdreigingen in het onderwijs. Het is dus belangrijk dat ieder schoolbestuur waakzaam is en continu kan monitoren en bijsturen. Hierdoor kunnen dreigingen effectief en efficiënt worden afgewend en wordt de kans dat een dreiging ook daadwerkelijk een incident wordt, verkleind.

6. Schoolbesturen reageren adequaat op beveiligingsincidenten en herstellen snel

Bij een incident is het noodzakelijk dat het onderwijsproces daar zo min mogelijk onder lijdt en eventuele schade tot een minimum beperkt wordt. Daarom moeten schoolbesturen in staat zijn snel te reageren en snel te herstellen naar de normale, gewenste situatie. Vanwege het belang van onderwijs in de (lokale) samenleving moeten scholen zich hierop ontwikkelen.

10 https://www.nist.gov/cybersecurity

3

Inspanningen en activiteiten

Om de strategische doelen zoals benoemd in hoofdstuk 2 te behalen, ondernemen we vanuit het programma diverse activiteiten. Hiermee helpen we schoolbesturen de stappen te zetten die helpen de beoogde veranderingen te realiseren. Hoe we dit voor ons zien is uitgewerkt op de volgende pagina.

VAN STRATEGISCHE NAAR OPERATIONELE DOELEN

Om de strategische doelen SMART te maken hebben we deze vertaald in operationele doelen. Deze hebben betrekking op de processen in de organisatie die op orde moeten zijn. Ze zijn geformuleerd als meetbare normen. De operationalisatie maakten wij samen met IBP'ers van schoolbesturen. Zo hebben we geborgd dat de doelen zijn toegesneden op de situatie in het funderend onderwijs. Voor het voldoen aan de normen stellen we een realistisch groeipad op. De basis voor dit groeipad is zowel de realistische verwachting van het tempo dat schoolbesturen kunnen volgen als de financiële middelen die beschikbaar komen om hen hier effectief in te kunnen ondersteunen.

Verantwoording operationele doelen

De strategische doelen zijn vertaald in tien operationele doelen. Deze operationele doelen zijn gebaseerd op het Toetsingskader Informatiebeveiliging van de Nederlandse Beroepsorganisatie van Accountants (ook wel het NBA-kader genoemd). Wij nemen dit kader als basis omdat het breed gebruikt wordt in Nederland. Ook het mbo, hbo en wo gebruiken het als basis voor het toetsen van hun beveiligingsmaatregelen. Het NBA-kader is voor informatiebeveiliging dekkend, wat betekent dat het gebruikt kan worden om beveiliging over de hele breedte te toetsen. Een kanttekening hierbij is dat privacy (nog) geen onderdeel uitmaakt van dit kader.

Voor het funderend onderwijs (FO) wordt het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (IBP FO) ontwikkeld. Om onnodige diversiteit in de onderwijssector te voorkomen, om het lerend vermogen van sectoren en organisaties te stimuleren en om schoolbesturen te ondersteunen die in meerder sectoren actief zijn, nemen wij de normen van het hoger onderwijs en mbo als uitgangspunt voor het Normenkader IBP FO. Daarin worden zowel privacy als informatiebeveiliging opgenomen.

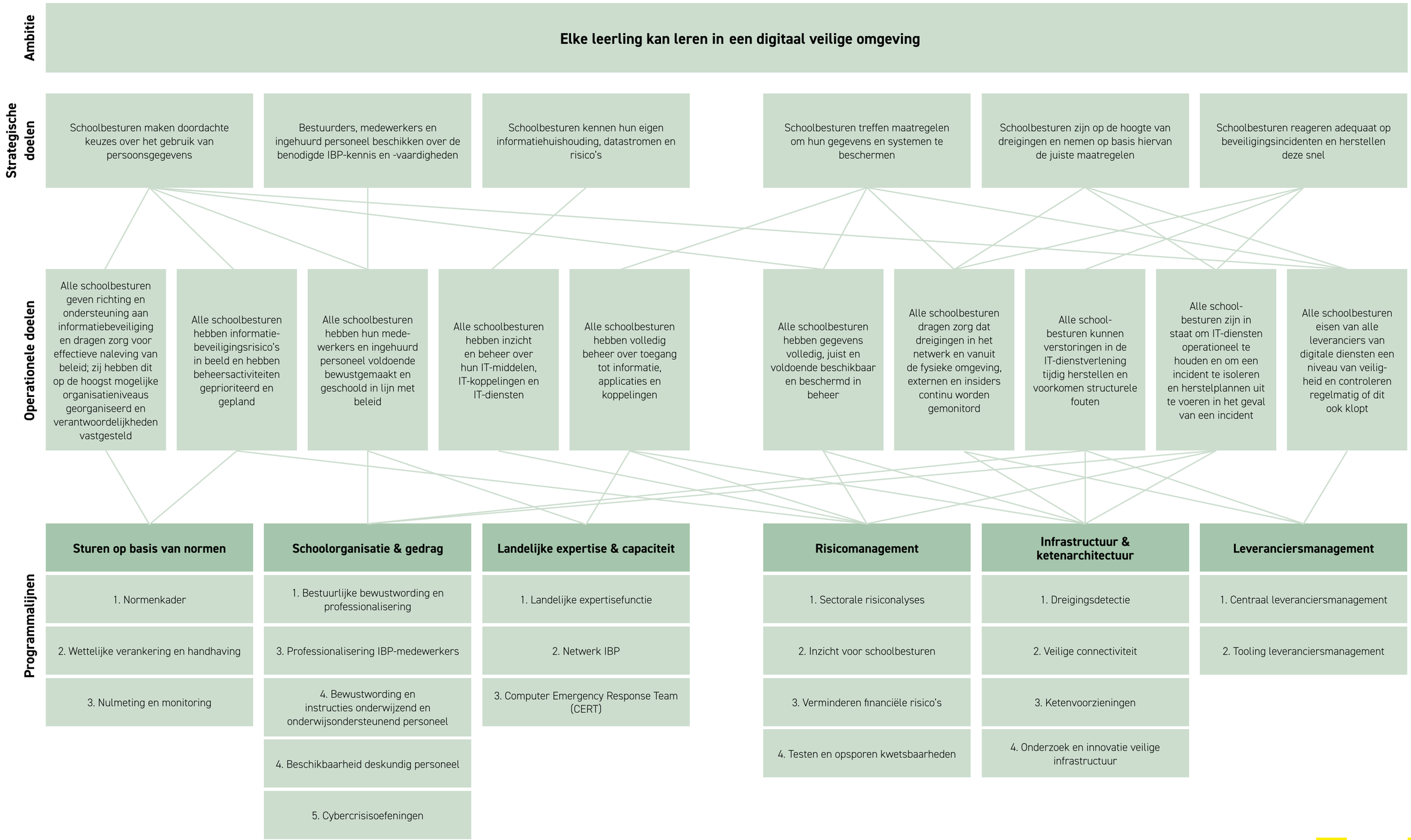
Fasering

Naast oplevering van het normenkader wordt in 2023 ook gewerkt aan een voorstel voor een groeipad. Het groeipad beschrijft op welk moment aan welke normen moet worden voldaan. Dit maakt concreter welke veranderingen in de schoolorganisatie op welk moment moeten worden doorgevoerd. Niet alles hoeft in één keer. We nemen 31 december 2027 als einddatum van het programma: dat is het moment waarop we ernaar streven dat de operationele doelen van het programma zijn behaald en alle schoolbesturen hun digitale veiligheid duurzaam op orde hebben.

Monitoring

Om te bepalen of de strategische programmadoelen zijn behaald, moet gemonitord worden op de operationele doelen. In 2023 start het proces van nulmeting en monitoring. Het succes van het programma in termen van outcome wordt gedefinieerd op basis van deze metingen: hebben schoolbesturen de maatregelen getroffen die nodig zijn voor digitaal veilig onderwijs? Het succes in termen van output wordt gedefinieerd aan de hand van de concrete activiteiten in de faseplannen. Het succesvol uitvoeren en opleveren van de inspanningen die hierin beschreven staan bepalen of de uitvoering van het programma goed functioneert. Wanneer activiteiten volgens plan worden uitgevoerd, maar de operationele en strategische doelen onvoldoende worden behaald is dit aanleiding tot bijsturing binnen het programma. In de monitoring zullen jaarlijks die elementen worden uitgelicht die aansluiten bij de onderdelen van het groeipad die op dat moment opportuun zijn.

Figuur 1: Doel-inspanningen-netwerk programma Digitaal Veilig Onderwijs (DVO)



OPERATIONELE DOELEN

Bestuur en organisatie

Alle schoolbesturen geven richting en ondersteuning aan informatiebeveiliging en privacy en dragen zorg voor effectieve naleving van beleid; zij hebben dit op de hoogst mogelijke organisatieniveaus georganiseerd.
Met dit doel wordt geborgd dat informatiebeveiliging en privacy niet alleen zijn belegd bij de jurist of de ICT-afdeling. De structurele bestuurlijke aandacht voor dit thema wordt geborgd. Dit doel zorgt voor een organisatie(structuur) die de hele onderwijsinstelling in staat stelt informatiebeveiliging en privacy goed te organiseren.

Risico's

Alle schoolbesturen hebben informatiebeveiligings- en privacyrisico's in beeld en hebben beheersactiviteiten geprioriteerd en gepland.
Als schoolbesturen de juiste informatiebeveiligings- en privacymaatregelen willen nemen, moeten zij inzicht hebben in de risico's die de organisatie loopt. Ook moeten zij zicht hebben op welke activiteiten nog nodig zijn om hun eigen organisatie digitaal veilig te maken en zij moeten een planning maken voor de uitvoering daarvan.

Personeel

Alle schoolbesturen hebben structureel voldoende capaciteit voor informatiebeveiliging en privacy en dragen continu zorg dat (ingehuurde) medewerkers blijvend bewust en geschoold zijn in lijn met het beleid.
Een goede organisatie en uitvoering van IBP-maatregelen begint bij voldoende capaciteit om deze uit te kunnen voeren. Naast capaciteit moet het personeel dat werkzaam is in de scholen over de kennis en vaardigheden beschikken om hun functie goed uit te kunnen voeren. Voor leraren en onderwijsondersteunend personeel betekent dit dat ze weten wat ze moeten doen om beveiligings- en privacyrisico's te beperken.

Omgaan met configuraties en wijzigingen

Alle schoolbesturen hebben inzicht in en beheer over hun IT-middelen, IT-koppelingen en IT-diensten.
Om in control te zijn, dus om risico's te kennen en om te weten welke maatregelen genomen zijn of nog moeten worden genomen, is inzicht nodig. Welke software en hardware gebruiken we, van welke leveranciers nemen we die af, hoe zien gegevensuitwisselingen tussen systemen eruit en op welke manier hebben we afspraken gemaakt met leveranciers over het nemen van de juiste beveiligings- en privacymaatregelen. Zonder inzicht is het onmogelijk te bepalen of een bestuur de juiste maatregelen heeft genomen.

Omgaan met gegevens

Alle schoolbesturen hebben gegevens volledig, juist en voldoende beschikbaar en beschermd in beheer.
Het schoolbestuur moet ervoor zorgen dat ze controle hebben over de (persoons)gegevens waarvoor ze verantwoordelijk zijn. Dat betekent onder andere gegevens niet langer in bezit hebben dan nodig en het nemen van de juiste beveiligingsmaatregelen op basis van een classificatie van deze gegevens.

Identiteiten en toegangsbeheer

Alle schoolbesturen hebben volledig beheer over de toegang tot informatie, applicaties en koppelingen.
Om fouten en problemen te voorkomen, moet goed beheerd worden welke personen toegang hebben tot data of systemen. Ook moeten rechten goed worden toegekend, zodat alleen personen die dat mogen gegevens of systemen kunnen aanpassen.

Digitale en fysieke beveiliging

Alle schoolbesturen dragen zorg dat dreigingen in het netwerk en vanuit de fysieke omgeving, externen en insiders continu worden gemonitord.
Het startpunt is het nemen van de juiste (technische) beveiligingsmaatregelen om te zorgen dat kwaadwillende personen systemen niet van buitenaf kunnen binnendringen. Om te weten dat geen misbruik wordt gemaakt van toegekende toegangsrechten, moeten schoolbesturen te allen tijde monitoren en vastleggen wie toegang heeft gehad en wie aanpassingen heeft gedaan in systemen. Door dit goed te monitoren kunnen zij ook aanvallen van buitenaf detecteren. Ook zijn er processen nodig voor het tijdig installeren van beveiligingsupdates. Daarnaast is het zaak de fysieke locaties en apparatuur te beveiligen om kwaadwillende personen minder kans te geven om toegang te krijgen tot systemen.

Omgaan met incidenten en problemen

Alle schoolbesturen kunnen verstoringen in de IT-dienstverlening tijdig herstellen. Ze voorkomen structurele fouten.
Om systemen goed te beschermen en om snel te kunnen reageren op problemen moeten er procedures en draaiboeken zijn, zodat duidelijk is wat te doen en wie waarvoor verantwoordelijk is. Ook zijn heldere afspraken nodig over hoe wijzigingen in ICT zo snel mogelijk worden doorgevoerd.

IT-operatie en onderwijscontinuïteit

Alle schoolbesturen zijn in staat om IT-diensten operationeel te houden en om een incident te isoleren en herstelplannen uit te voeren in het geval van een incident.
Om te zorgen dat het primaire proces ook digitaal altijd doorgang kan vinden, moeten schoolbesturen niet alleen beveiligingsmaatregelen treffen, maar ook maatregelen om snel te herstellen. Hierbij gaat het onder andere over het maken van back-ups en het op orde hebben van herstelplannen.

Leveranciersmanagement

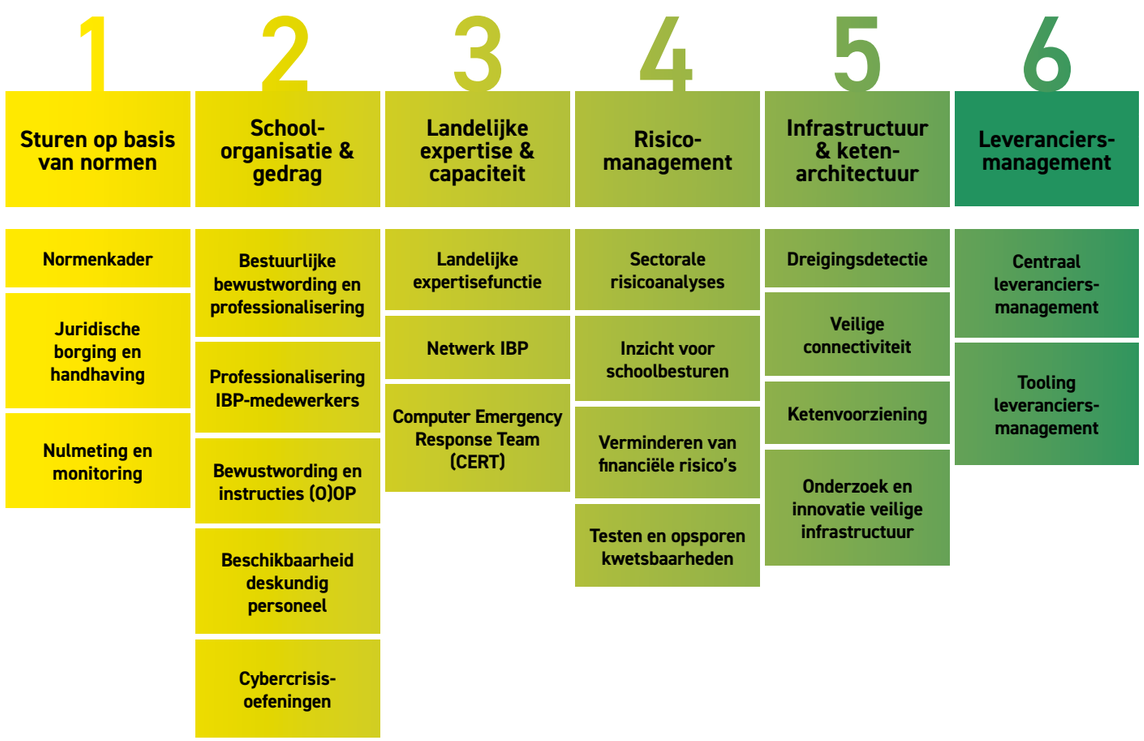
Alle schoolbesturen eisen van alle leveranciers van digitale diensten een niveau van privacy en veiligheid en controleren regelmatig of dit ook klopt.
Schoolbesturen maken veel gebruik van digitale diensten van leveranciers. Veelal betreft dit systemen in de cloud. Het is zaak goede afspraken te maken met leveranciers over de persoonsgegevens die zij verwerken en hoe zij die beveiligen. Ook moeten deze afspraken regelmatig worden gecontroleerd zodat zeker is dat deze afspraken niet slechts een papieren werkelijkheid zijn.

ZES PROGRAMMALIJNEN

Om aan al deze normen te voldoen, helpen we schoolbesturen met ondersteuningsaanbod. Soms in de vorm van kennis en voorbeelddocumenten waar ze zelf mee aan de slag moeten. Soms door zaken uit handen te nemen, door bijvoorbeeld gezamenlijk leveranciersmanagement of door schoolbesturen actief te waarschuwen bij dreigingen. Deze ondersteuning wordt bepaald door het normenkader. Bewustwording bij besturen zorgt ervoor dat schoolbesturen daadwerkelijk aan de slag gaan met digitale veiligheid en gebruikmaken van het ondersteuningsaanbod.

Om het programma goed te kunnen organiseren en besturen, hebben wij zes programmalijnen gedefinieerd. Deze lijnen relateren aan de operationele doelen, maar zijn opgesteld vanuit de logica van het kunnen organiseren van het programma. Dus op basis van wat er moet worden gemaakt, georganiseerd, etc. om schoolbestuurders, schoolleiders en IBP'ers te helpen om aan de operationele doelen te kunnen voldoen. Onderstaand model geeft hiervan een schematische weergave.

Figuur 2: De zes programmalijnen in beeld



Sturen op basis van normen

Voor de veranderstrategie van het programma is het van belang dat schoolbesturen goed weten welke verantwoordelijkheid ze hebben op het gebied van IBP en wat ze moeten doen om die in te vullen. Het Normenkader IBP Funderend Onderwijs vormt daarmee de inhoudelijke ruggengraat van zowel de verantwoordelijkheid van besturen, als die van het programma Digitaal Veilig Onderwijs (DVO).

Het sturen op basis van normen is in de eerste plaats van belang op het niveau van het individuele schoolbestuur: weet ik waaraan ik moet voldoen om mijn leerlingen te kunnen laten leren in een digitaal veilige omgeving? Een duidelijke, voor het onderwijsbestuur passende en toepasbare set normen is daar het vertrekpunt voor.

Een juridische borging van deze normen geeft schoolbesturen de expliciete plicht om de digitale veiligheid van het onderwijs serieus te nemen. Het nemen van maatregelen voor naleving (variërend van een oproep aan accountants en interne toezichthouders tot handhaving in combinatie met wettelijke maatregelen) geeft de overheid de handvatten om digitale veiligheid voor élke leerling te borgen.

Een nulmeting en regelmatige monitoring laten zien waar het schoolbestuur staat en zijn daarmee een belangrijk vertrekpunt voor het opstellen van een verbeterplan en het bepalen van de juiste acties om de veiligheid te vergroten.

Om tot een verstandig en haalbaar groeipad te komen voor de hele sector en stapsgewijs de passende ondersteuningsactiviteiten in het programma te bepalen, is ook op sectoraal niveau inzicht nodig in de stand van zaken binnen schoolbesturen. Monitoring biedt ook hiervoor de juiste inzichten.

In de programmalijn *Sturen op basis van* normen zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het realiseren, beheren en de doorontwikkeling van de set normen, een toetsingskader en voorbeeldmaatregelen en het opstellen van een stappenplan waarin staat beschreven wanneer aan welke normen moet worden voldaan: het zogenaamde groeipad;
2. De wettelijke verankering van de set normen en het naleven/handhaven hiervan;
3. Het uitvoeren van een nulmeting en herhaalde metingen (monitoring) om de vorderingen van het digitaal veilig maken van onderwijsinstellingen op basis van het groeipad te volgen en waar nodig bij te sturen op bestuurs-, programma- en beleidsniveau.

Schoolorganisatie en gedrag

Uiteindelijk beoogt het programma een gedragsverandering binnen schoolbesturen. Schoolbestuurders moeten zich hiervoor bewust zijn van het belang van privacy en digitale veiligheid, weten welke verantwoordelijkheden zij hebben en actie ondernemen om hun organisatie digitaal veilig te laten zijn (kennis, houding, gedrag). Hiervan afgeleid is het ook belangrijk dat schoolleiders hun rol en verantwoordelijkheid kennen in deze verandering.

Een van die verantwoordelijkheden betreft de inzet van personeel met kennis van informatiebeveiliging en privacy. Aangezien er krapte op de arbeidsmarkt is en de markt voor gespecialiseerd securitypersoneel in het bijzonder krap is, is een gemeenschappelijke aanpak nodig. Immers: er is al weinig vis in de vijver en als scholen elkaar ook nog gaan beconcurreren, krimpen de kansen op succes voor de sector als geheel. Voor kleinere schoolbesturen is het bovendien zeer moeilijk om een aantrekkelijke werkgever te zijn voor dergelijk gespecialiseerd werk.

Daarnaast is het belangrijk dat het aanwezige personeel over de juiste kennis en vaardigheden beschikt. Dit begint bij het IBP-personeel dat zorg draagt voor de uitvoering van het IBP-beleid: privacy officers, security officers, ICT'ers, functionarissen gegevensbescherming en CISO's.

Maar ook voor het overige onderwijzend en ondersteunend personeel moet duidelijk zijn wat er van hen wordt verwacht om te zorgen voor een digitaal veilige omgeving voor alle leerlingen.

Tot slot is het van belang dat elke onderwijsorganisatie regelmatig test hoe goed zij kunnen handelen in het geval van een incident. Want hoe goed scholen alle processen en techniek ook inregelen, de kans bestaat altijd dat het een keer misgaat. Op basis van de lessen uit dergelijke oefeningen kunnen processen binnen het schoolbestuur worden verbeterd.

In de programmalijn *Schoolorganisatie* en gedrag zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het investeren in de bewustwording en activering van onderwijsbestuurders zodat zij de juiste activiteiten in hun onderwijsinstellingen starten om aan het normenkader te voldoen;
2. Activiteiten om de beschikbaarheid van deskundig personeel voor onderwijsbesturen te bevorderen;
3. Een aanpak voor de scholing van IBP-medewerkers van schoolbesturen
4. Investeren in de bewustwording en het kennisniveau van onderwijzend en onderwijsondersteunend personeel
5. Het uitvoeren van cybercrisisoefeningen

Landelijke expertise en capaciteit

Een stevige landelijke organisatie is nodig om te zorgen dat schoolbesturen niet allemaal voor zichzelf het wiel uit hoeven te vinden. Het ontwikkelen en duurzaam borgen van IBP-kennis die specifiek is toegespitst op het primair en voortgezet onderwijs helpt IBP'ers van onderwijsinstellingen om hun werkzaamheden goed uit te voeren. Een landelijk en sectorbreed expertisecentrum duidt nieuwe ontwikkelingen, ontwikkelt voorbeelddocumenten en stappenplannen en deelt kennis met de sector. Het biedt ook een stabiele basis voor het uitvoeren van diverse andere programma-activiteiten.

De landelijke expertisefunctie wordt versterkt door de samenwerking met schoolbesturen door het Netwerk IBP te benutten om kennis en informatie te delen.

Naast het ondersteunende werk van een expertiseorganisatie is ook het monitoren en duiden van concrete dreigingen vitaal voor onderwijsinstellingen. Dit betreft zowel de advisering van onderwijsinstellingen bij het nemen van de juiste maatregelen bij een dreiging, als het coördineren richting (software)leveranciers en andere ketenpartijen om adequaat (en waar mogelijk preventief) op dreigingen te reageren. Deze werkzaamheden worden uitgevoerd door een Computer Emergency en Response Team (CERT). Het CERT heeft ook een belangrijke rol bij eerste hulp bij digitale veiligheidsincidenten: het concreet helpen van een onderwijsinstelling (of het organiseren van deze hulp) om een incident zo snel en adequaat mogelijk op te lossen en te herstellen.

In de programmalijn *Landelijke expertise en capaciteit* zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het beschikken over een landelijke expertisefunctie die onder andere zorgt voor duiding van ontwikkelingen, adviseren van schoolbesturen en het opstellen van voorbeelddocumenten;
2. Beheer en versterking van het Netwerk IBP waarin IBP-professionals van onderwijsbesturen samenwerken en kennisdelen;
3. Een sectoraal Computer Emergency en Response Team (CERT) voor verspreiding van kennis over dreigingen en risico's en ondersteuning voor schoolbesturen bij incidenten.

Risicomanagement

Het weerbaar zijn tegen cyberdreigingen gaat over risicomanagement: welke risico's zijn er en welke zijn we bereid te accepteren. Schoolbesturen lijken in heel veel opzichten op elkaar, zeker wat betreft digitale omgevingen. Dat betekent dat het mogelijk is om een groot deel van het in kaart brengen van risico's voor privacy en digitale veiligheid landelijk uit te voeren. De nulmeting en monitoring vanuit het programma dragen hieraan bij. Niet alleen zijn schoolbesturen hiermee geholpen, het biedt ook inzichten voor aanpassingen van het normenkader of de landelijke ondersteuning voor besturen.

Inzicht in het eigen ICT-landschap en datahuishouding vormt de basis voor goed risicomanagement bij schoolbesturen. Weten wat je in huis hebt, helpt bij het weten wat je moet beschermen, en hoe. Naast inzicht in wat een bestuur in huis heeft, is ook inzicht nodig in de veiligheid en robuustheid van de schoolomgeving door regelmatig te scannen en testen op kwetsbaarheden. Het programma stelt besturen in staat dit te organiseren.

Wanneer er toch een keer een incident is, kan dit gepaard gaan met hoge kosten voor het schoolbestuur. Kosten voor het niet kunnen geven van onderwijs of aanpassingen daarin, kosten voor reactie en herstel, denk hierbij aan het opnieuw opbouwen van systemen en herstellen van data. Schoolbesturen moeten op een doelmatige manier in staat zijn om deze kosten te dragen. Het programma onderzoekt of hiervoor collectieve verzekeringen of een calamiteitenfonds zijn of kunnen worden georganiseerd.

In de programmalijn *Risicomanagement* zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het uitvoeren van sectorale risicoanalyses en publiceren van o.a. een sectoraal cyberdreigingsbeeld;
2. Het activeren en ondersteunen van schoolbesturen bij het zicht krijgen op de eigen situatie en risico's;
3. Ondersteuning voor schoolbesturen bij het in kaart brengen van de kwetsbaarheden in de eigen systemen en het testen van deze systemen;
4. Het verminderen van de financiële risico's voor schoolbesturen bij een beveiligingsincident door middel van verzekeringen of een calamiteitenfonds

Infrastructuur en ketenarchitectuur

Naast gedrag en goed ingerichte processen vormt de digitale infrastructuur van een schoolbestuur een belangrijk onderdeel van digitale veiligheid. De fysieke (connectiviteits)infrastructuur is belangrijk voor de continuïteit van het onderwijs, maar is ook kwetsbaar. Een robuuste infrastructuur voor alle scholen (met onder meer bescherming tegen DDoS-aanvallen en filtering van malafide domeinen) ontzorgt scholen en borgt de veiligheid en continuïteit van hun onderwijs. Daarnaast moeten scholen gewaarschuwd worden door specifieke dreigingen voor hun systemen te detecteren en direct te handelen. Waar een CERT algemene dreigingen detecteert, is het ook nodig dreigingen op het niveau van één specifieke laptop of gebruiker waar te nemen.

Ook ketenvoorzieningen waarmee gegevens tussen organisaties worden uitgewisseld spelen een belangrijke rol in het standaard veiliger maken van de digitale onderwijsomgeving. Door met standaarden en voorzieningen de ketens voor de uitwisseling van persoonsgegevens in te richten volgens de principes van privacy en security by design, worden – zowel voor scholen als leveranciers – de veiligheid verhoogd en de beheerlasten verlaagd. Omdat cybersecurity en techniek steeds veranderen zijn doorlopend onderzoek en innovatie nodig om scholen en leerlingen zo goed mogelijk te beschermen.

In de programmalijn *Architectuur en techniek* zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het realiseren van een passende oplossing voor dreigingsdetectie voor schoolbesturen door middel van het faciliteren van een Security Operations Center (SOC);
2. Het realiseren van oplossingen voor veilige connectiviteit (waaronder veilig internet en veilige wifi);
3. Landelijke ketenvoorzieningen die onder andere veilige gegevensuitwisseling en toegang tot gegevens en systemen mogelijk maken (o.a. standaarden, bestaande voorzieningen zoals OSO, Entree Federatie en nieuw te ontwikkelen centrale of collectieve diensten en voorzieningen);
4. Doorlopende onderzoeken, analyse en innovatie om de landelijke en lokale infrastructurele voorzieningen op de beste manier te organiseren voor het funderend onderwijs.

Leveranciersmanagement

Een belangrijk deel van het digitale schoolleven van leerlingen speelt zich af in systemen: de leerlingadministratie, leermiddelen, dashboards, etc. Daarom moeten scholen goede afspraken maken met de leveranciers hiervan over hoe zij omgaan met persoonsgegevens en de beveiliging van deze systemen. Daarnaast moeten scholen onderzoek doen naar de risico's die verwerking van deze persoonsgegevens met zich meebrengen (een DPIA), en moeten zij controleren of een leverancier zich daadwerkelijk aan de afspraken houdt. Hierin loont het voor scholen om samen op te trekken: vanuit een doelmatigheidsperspectief, maar ook om gezamenlijk een vuist te kunnen maken tegen grote leveranciers en beter afspraken af te dwingen. Deze landelijke activiteiten worden voor scholen ontsloten op een manier die hen helpt om aan hun eigen (wettelijke) verplichtingen te voldoen.

In de programmalijn *Leveranciersmanagement* zijn de belangrijkste activiteiten gedurende de totale looptijd van het programma:

1. Het inrichten en uitvoeren van centraal leveranciersmanagement door onder andere inzicht in IBP-eigenschappen van producten, het hanteren van inkoopvoorwaarden, uitvoeren van DPIA's en DTIA's, toetsing van verwerkersovereenkomsten en het uitvoeren van audits;
2. Tooling die het voor schoolbesturen eenvoudiger maakt om hun eigen leveranciers- en risicomanagement vorm te geven (o.a. beheer verwerkersovereenkomsten en uitvoering DPIA's).

Met deze programmalijnen en globale activiteiten is er zicht op wat gedaan wordt vanuit het programma. Sommige onderdelen zijn hierbij al vrij duidelijk (bijvoorbeeld het normenkader), andere onderdelen worden in de komende tijd nog verder uitgewerkt om gericht te kunnen plannen en begroten (bijvoorbeeld ketenvoorzieningen).

4

Fasering

Het programma Digitaal Veilig Onderwijs (DVO) wordt gefaseerd opgebouwd in periodes van een jaar. Iedere faseperiode eindigt met besluitvorming over de afgelopen fase en de start van de volgende periode. Elk jaar rond de zomer kijken we terug en vooruit naar activiteiten en doen we eventuele aanpassingen aan de koers voor het volgende jaar. Met de financieringssystematiek via de Voorjaarsnota[11] bouwen we rond de jaarwisseling ook een moment in om het lopende faseplan bij te stellen.

In de planning van activiteiten en middelen zetten we als eerste in op de middelen die de grootste impact hebben op het verminderen van mogelijke risico's voor de informatiebeveiliging en privacy binnen het funderend onderwijs. De verwachting is dan ook dat de activiteiten aan het begin van het programma een snelle groei van de verbetering zullen laten zien. In de jaren daarna komen activiteiten op het programma die een minder grote impact hebben op het verminderen van risico's, maar nog steeds van belang zijn en aandacht nodig hebben. Ook verandering in dreigingen, techniek en maatschappij hebben impact op de te nemen maatregelen en het herijken van het programma.

PROGRAMMA-ACTIVITEITEN

We onderscheiden in het programma Digitaal Veilig Onderwijs (DVO) vier typen activiteiten:

1. Onderzoeken van vraagstukken en oplossingen
Binnen het programma Digitaal Veilig Onderwijs (DVO) definieert het normenkader voor een belangrijk deel de benodigde activiteiten voor schoolbesturen. Het normenkader is bij de ontwikkeling van dit programmaplan nog in ontwikkeling. Zodra het kader is vastgesteld kunnen ook de verschillen tussen de huidige en gewenste situatie worden vastgesteld. Hier zijn diverse onderzoeken voor nodig. De uitkomsten van deze onderzoeken bepalen in grote mate de benodigde typen activiteiten die we moeten ontwikkelen en borgen. De verwachting is dat de onderzoeken voornamelijk bij de start van het programma een dominant onderdeel zijn en naar mate de tijd vordert slechts een klein deel van de activiteiten zullen betreffen. Soms is de probleemanalyse voldoende helder, dan wordt onderzoek gedaan naar de beste wijze van het oplossen van de problematiek: hoe kunnen we schoolbesturen het beste ondersteunen?

2. Ontwikkelen van nieuwe ondersteuningsactiviteiten
Het programma Digitaal Veilig Onderwijs (DVO) onderneemt een breed scala aan activiteiten die tezamen bijdragen aan het realiseren van de strategische doelen. De activiteiten variëren van het ontwikkelen van kennisproducten tot aan gezamenlijke ontwikkeling of aanbesteding van producten en diensten. De precieze scope van activiteiten worden gaandeweg het programma steeds meer bekend. Het is de verwachting dat het programma in de periode 2023 en 2024 veel energie in de activiteiten gaat steken. Daarna zullen activiteiten meer structurele vormen aannemen en hebben inspanningen vooral betrekking op de goede uitvoering van de dienstverlening.

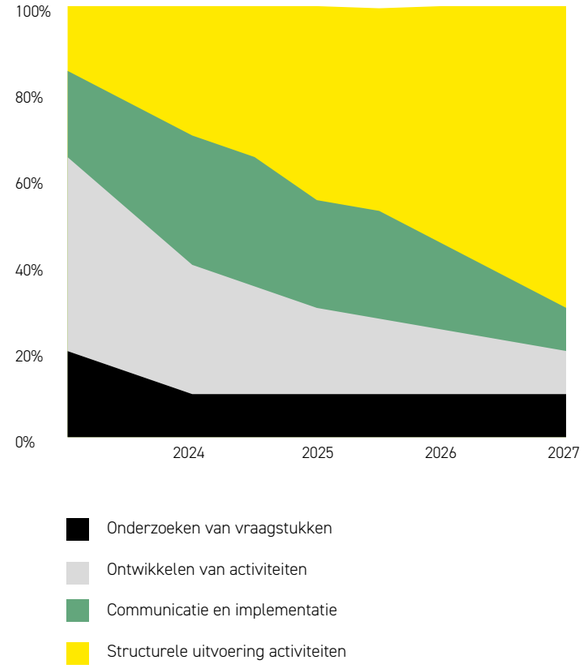
11 https://www.tweedekamer.nl/zo_werkt_de_kamer/van_prinsjesdag_tot_verantwoordingsdag/voorjaarsnota

3. Communicatie en implementatie
Het programma heeft een complexe opdracht om verandering bij zo'n 1.300 autonome en zeer diverse schoolbesturen te bewerkstelligen. Het is hierbij essentieel om goed in contact te zijn met de schoolbesturen en te zorgen dat we de ondersteuningsbehoefte goed invullen, onder andere door hen te betrekken bij de ontwikkeling hiervan. Communicatie heeft vanaf het begin van het programma veel aandacht. Communicatie richt zich op het helder en eenduidig informeren over het programma en de daarbij behorende verwachtingen van de schoolbesturen. Communicatie is daarnaast het fundament onder het participatieproces waarin we bestuurders en IBP'ers betrekken bij het tot stand komen van activiteiten en middelen.

4. Structurele activiteiten
Het programma bouwt in samenhang aan veel activiteiten. Voor iedere activiteit kijken we of, en zo ja op welke manier, een nieuwe activiteit structureel moet worden uitgevoerd. De verwachting is dat dit voor veel activiteiten geldt. Daarom is het van belang om vanaf de start van het programma activiteiten zoveel mogelijk in de bestaande organisatiestructuren van de uitvoerende partijen te beleggen.

Schematisch ziet de activiteitenverdeling zoals deze nu is ingeschat er als volgt uit.

Figuur 3: Schematische weergave van de verandering van het type activiteiten in het programma



5

Communicatie

DOELEN EN SUBDOELEN VOOR COMMUNICATIE

De programma-ambitie vertalen we voor communicatie naar het volgende doel:

- Schoolbestuurders voelen zich verantwoordelijk voor de digitale veiligheid van hun schoolorganisatie en worden geactiveerd hiernaar te handelen.

Subdoelen hierbij zijn:

- Schoolbestuurders, schoolleiders en IBP'ers zijn **op de hoogte** van de mogelijke dreigingen op het gebied van cybersecurity en privacy.
- Schoolbestuurders, schoolleiders en IBP'ers kennen de **urgentie** om aan de slag te gaan met digitale veiligheid en privacy.
- Schoolbesturen, schoolleiders en IBP'ers kennen hun eigen rol in het digitaal veilig maken van hun eigen schoolomgeving, weten hoe zij - stap voor stap - moeten **handelen** en dat ze daarbij geholpen worden door het programma.

DOELGROEPEN

Zoals de subdoelen voor communicatie al laten zien, richt de communicatie van het programma zich primair op **schoolbestuurders, schoolleiders en IBP'ers** (of medewerkers in scholen met een vergelijkbare functie).

Er zijn ook secundaire doelgroepen te benoemen. Deze doelgroepen hebben invloed op de primaire doelgroepen en worden daarom meegenomen in onze aanpak. Deze secundaire doelgroepen zijn:

- **Beïnvloeders** van de primaire doelgroepen (mensen die vanuit een belang, invloed of relatie, invloed hebben op de primaire doelgroep, zoals de onderwijsinspectie, raden van toezicht, vakbonden, politiek, Ouders & Onderwijs, etc.
- **Overige werknemers van schoolbesturen** bijvoorbeeld de ICT'er, Informatiemanager, leerkracht, HR-medewerker, etc. Zij hebben straks allemaal een rol/deeltaak bij de implementatie van digitaal veilig werken.
- **De programma-organisatie** en de partnerorganisaties: Kennisnet, SIVON, het ministerie van OCW, PO-Raad en VO-raad. Weten wie wat doet en waarom dat belangrijk is in het kader van het programma, helpt het goed samenwerken en daarnaast om bovenstaande doelgroepen zoveel mogelijk te faciliteren.

In de communicatie staat de activatie van schoolbestuurders, schoolleiders en IBP'ers centraal. Dit doen we onder andere door zo dicht mogelijk aan te sluiten bij de beleefwereld, belangen en bestaande kanalen van de doelgroepen. Voor de uitwerking betekent dit dat we werken vanuit een campagnematige aanpak met een herkenbare stijl, zoveel mogelijk gebruik maken van bestaande kanalen, herkenbaar taalgebruik, duidelijk handelingsperspectief en inzicht in rollen en taken van de betrokkenen (schoolbestuurders, schoolleiders en IBP'ers).

Figuur 6: Message house Programma Digitaal Veilig Onderwijs

Schoolbestuurders en IBP'ers voelen zich verantwoordelijk voor een digitaal veilige schoolorganisatie en handelen hiernaar.

Bewustwording

Schoolbestuurders, schoolleiders en IBP'ers kennen de urgentie van én weten dat zij verantwoordelijk zijn voor een digitaal veilige schoolorganisatie.

Bewijsvoering:

- Er zijn dagelijks cyber security incidenten, het gaat vaak mis of bijna mis en dat heeft grote gevolgen voor een deels kwetsbare doelgroep.
- De minister voor onderwijs onderschrijft de urgentie van digitaal veilig onderwijs en heeft daarom een programma geïnitieerd.
- Schoolbestuurders, schoolleiders en IBP'ers weten dat ze verantwoordelijk zijn voor een digitaal veilige schoolorganisatie en hoe ze hier invulling aan kunnen (gaan) geven.

Normen en wetgeving

De normen waaraan een digitaal veilige schoolorganisatie moet voldoen, zijn opgesteld in samenwerking met de sector en verankerd in de wet.

Bewijsvoering:

- De sector vraagt om heldere normen.
- Onder begeleiding van de partijen binnen het programma is met vertegenwoordigers van de sector gesproken om te komen tot een passende set normen.
- Digitale veiligheid verandert continu. Om de normen passend te houden, kan de sector hierop blijvend reageren.
- De set normen duidt waaraan schoolorganisaties moeten voldoen.
- Deze normen worden verankerd in doelmatige wet- en regelgeving.

Toetsingskader, maatregelen en ondersteuning

Schoolbestuurders, schoolleiders en IBP'ers weten dat én hoe ze de hulp kunnen vragen die nodig is om een digitaal veilige schoolorganisatie te realiseren, te behouden en op de juiste manier te handelen als er onverhoopt een onveilige situatie ontstaat.

Bewijsvoering:

- Er is een toetsingskader opgesteld zodat schoolbestuurders en IBP'ers weten waar de schoolorganisatie nu staat.
- Er zijn voorbeeldmaatregelen opgesteld die helpen om aan de normen te gaan voldoen.
- Binnen de sector worden krachten gebundeld.
- Kennisnet, SIVON, PO-Raad en VO-raad bieden, in opdracht van en in samenwerking met OCW, ondersteuning om de maatregelen uit te voeren en te helpen als het onverhoopt toch mis gaat.

Programmasturing en PMO

De opdrachtgever van het programma is het ministerie van OCW. Zij neemt haar besluiten in samenspraak met het overige partners in het programma: PO-Raad, VO-raad, SIVON en Kennisnet. Al deze partijen hebben eveneens uitvoeringsverantwoordelijkheid in het programma.

Rollen van de deelnemers

- Het ministerie van OCW heeft de rol van opdrachtgever en is voor vrijwel alle activiteiten financier.
- De PO-Raad en VO-raad hebben de rol om de sector te vertegenwoordigen en vanuit deze rol de opdrachtgever de adviseren, en bij te dragen aan draagvlak onder hun leden. Ook dragen zij bij aan bewustwording en professionalisering van bestuurders en schoolleiders.
- Kennisnet heeft de rol om te adviseren vanuit haar expertrol op privacy en informatiebeveiliging in het onderwijs en aangrenzende thema's en vanuit haar rol als sector-/ketenarchitect. Ook ontwikkelt en beheert Kennisnet dienstverlening voor de hele sector funderend onderwijs.
- SIVON heeft de rol om de opdrachtgever te adviseren vanuit in het bijzonder de tussenpositie die SIVON inneemt tussen marktpartijen en schoolbesturen, en de vertaling die zij kan maken tussen behoefte van het onderwijs en concrete dienstverlening.
- Alle deelnemers in het programma hebben de rol van uitvoerder en adviseren ook vanuit deze hoedanigheid.

UITVOERING

De verantwoordelijkheid voor de uitvoering van de programma-activiteiten ligt bij de lijnorganisaties. De uitvoerende partij is aanspreekbaar op de uitvoering van de eigen activiteiten. Elk project kent een projectleider of verantwoordelijke. Deze is verantwoordelijk voor het opleveren van de projectresultaten of de uitvoering van de activiteit. De projectleiders worden aangestuurd vanuit de lijnorganisatie. De projectleider stemt af met de programmaorganisatie over de wijze waarop het project vordert en bijdraagt aan de programmadoelen. De programmaorganisatie is immers verantwoordelijk voor de inhoudelijke samenhang en coördinatie van de uitvoering van de activiteiten. Bij problemen in de uitvoering heeft het programmateam een signalerende rol in het programma. In dat geval spreekt de programmamanager eerst de projectleider aan en zoekt naar een oplossing. Indien nodig escaleert de programmamanager naar de manager/directeur van de verantwoordelijke organisatie. Indien dit niet tot een oplossing leidt, escaleert de programmamanager de situatie naar de opdrachtgever.

PROGRAMMAORGANISATIE

De programmamanagementorganisatie (PMO) zorgt voor overzicht en samenhang tussen de activiteiten en het behalen van de programmadoelen. Daarvoor zorgt zij voor inhoudelijke coördinatie tussen de inspanningen op basis van de bijdrage aan de programmadoelen. Ook stelt de PMO de opdrachtgever op basis van begrotingen, planningen, risico-inventarisaties, rapportages, onderzoeken en analyses in staat om bij te sturen om de doelen te behalen.

De PMO draagt zorg voor de vergaderagenda's en -stukken in de programma-governance. Ook regie op het omgevingsmanagement behoort de verantwoordelijkheden van de PMO, waarbij de programmamanager ook voor externe partijen een aanspreekpunt is. Voor zowel de interne als externe omgeving is de PMO verantwoordelijk voor de communicatiestrategie en -coördinatie alsook de uitvoering van diverse programmacommunicatie-activiteiten van het programma.

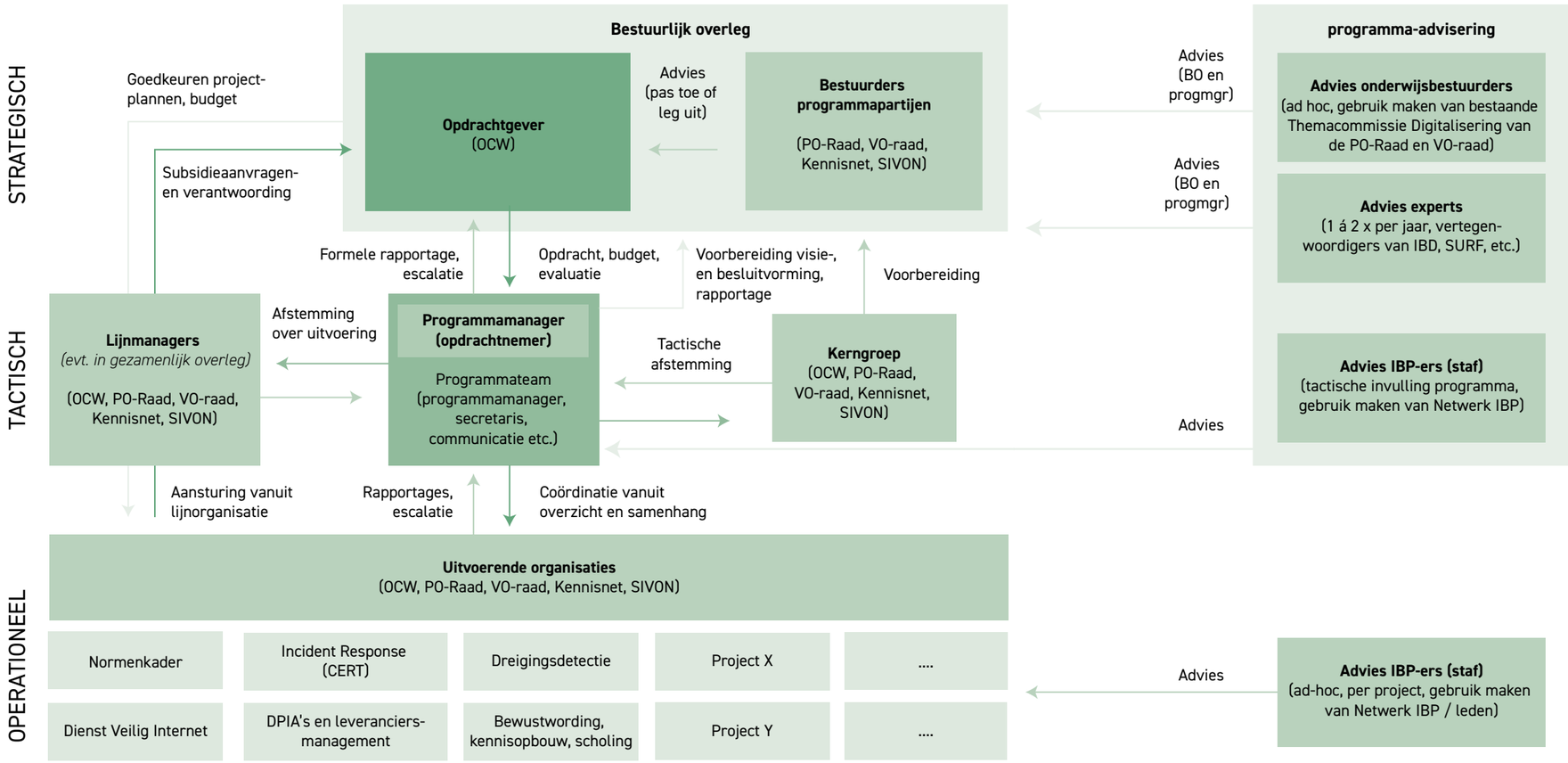
De PMO is tevens verantwoordelijk voor het beheer van de onderzoeksagenda en stuurt zelf ook diverse onderzoeken op deze agenda aan.

ADVIES VANUIT HET ONDERWIJSVELD

Om goed aan te sluiten bij de behoeftes van het onderwijsveld en de situatie in de praktijk, wordt er regelmatig advies ingewonnen bij zowel onderwijsbestuurders als uitvoerend IBP'ers van schoolbesturen. Deze laatste groep is verenigd in het Netwerk IBP po/vo. Ook wordt regelmatig advies ingewonnen bij expertise- en uitvoeringsorganisaties die een gelijksoortige opdracht hebben voor andere publieke sectoren.

De governance en sturing van het programma is weergegeven in Figuur 7. In Figuur 8 zijn ook de adviserende groepen ingetekend.

Figuur 7: Strategische sturing en uitvoering



Figuur 8: Advisering door doelgroep en experts

7

Middelen

Voor het behalen van de programmadoelen is vanaf 2023 structureel 6 miljoen per jaar beschikbaar. Deze middelen worden door het ministerie van OCW beschikbaar gesteld. Jaarlijks wordt een faseplan opgesteld met concrete activiteiten op basis waarvan de middelen worden toegedeeld aan activiteiten en organisaties.