Implementatieplan certificeringsschema informatiebeveiliging

Auteur(s) : Dirk Linden, Chris Zintel
Versienummer : Versie 0.9 09-06-2017

Edu-K

Inhoudsopgave

0 Documentgeschiedenis

0.1 Wijzigingen

Onderstaande tabel beschrijft de geschiedenis van dit document.

Versie	Datum	Omschrijving
0.1	4-5-2017	Eerste opzet
0.2	8-5-2017	Opzet implementatieplan voor tactisch overleg
0.5	31-5-2017	Input verwerkt uit tactisch overleg
0.9	9-6-2017	Input verwerkt uit tactisch overleg

0.2 Review

Dit document is ter review voorgelegd aan de onderstaande personen.

Naam	Functie	Versie	Datum
Dirk Linden	Kennisnet	0.1	4-5-2017
Tactisch overleg		0.2	8-5-2017
Dirk Linden	Kennisnet	0.4	31-5-2017
Tactisch overleg		0.5	1-6-2017

1 Inleiding

1.1 Probleemschets

Partijen in de educatieve keten werken samen aan een veilige betrouwbare keten. Hiervoor wordt de keten gestroomlijnd (standaard Distributie & toegang), wordt gewerkt met een ketenpseudoniem ten behoeve van dataminimalisatie (ECK iD), zijn er duidelijke afspraken over de omgang met leerlinggegevens (privacyconvenant en modelbewerkersovereenkomst) en worden afspraken gemaakt over de minimale maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van toepassingen en gegevens te garanderen (certificeringsschema).

Het certificeringsschema bevat een methodiek en een set aan maatregelen voor het niveau van informatiebeveiliging bij leveranciers van digitale diensten voor het onderwijs. Het geeft duidelijkheid over de minimale eisen en is een instrument dat inzichtelijk maakt in hoeverre partijen hieraan voldoen. Door het certificeringsschema te hanteren is er één werkwijze en één maatregelenset die zowel sectoroverstijgend als ketenoverstijgend toegepast kan worden in het onderwijsdomein. Dit levert efficiëntievoordelen op voor leveranciers, en maakt voor scholen op een eenduidige manier inzichtelijk of hun leveranciers ‘passende technische en organisatorische maatregelen’ hebben getroffen bij de omgang met leerlinggegevens en andere informatie.

In een digitaal tijdperk is het noodzakelijk dat het onderwijs de regie kan voeren over het gebruik van persoonsgegevens van leerlingen in de leermiddelenketen. De doelen van gebruik van het certificeringsschema binnen de educatieve keten zijn daarmee drieledig:

1. Verhoging van het algehele beveilingsniveau binnen de educatieve keten.
2. Schoolbesturen zijn in staat in control te zijn van de beveiligingsmaatregelen, in het bijzonder met betrekking tot leerlinggegevens.
3. Leveranciers in het onderwijs beschikken over een instrument om de genomen maatregelen inzichtelijk te maken.

1.2 Achtergrond en aanleiding

Verschillende ontwikkelingen en trajecten zijn relevant voor de implementatie van het certificeringsschema.

<u>Veilige en betrouwbare keten</u>
Binnen het publiek-private platform Edu-K werken brancheorganisaties van leveranciers en sectororganisaties van schoolbesturen samen aan een veilige en betrouwbare keten. Dit gebeurt onder andere door standaardisatie van distributie- en toegangsprocessen en het gebruik van een unieke identifier. Het privacyconvenant voor het primair en voortgezet onderwijs speelt hierin een centrale rol. De modelbewerkersovereenkomst bij het privacyconvenant bevat een bijlage met ‘technische en organisatorische maatregelen’ waarin leveranciers hun beschrijven van zij doen voor een veilige omgang met persoonsgegevens.

<u>Algemene verordening gegevensbescherming</u>
Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. Een belangrijk onderdeel van deze nieuwe wetgeving is de documentatieplicht. Dit houdt in dat organisaties met documenten moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen. Omdat het schoolbestuur als verantwoordelijke aan deze maatregelen moet voldoen, heeft zij deze informatie nodig van haar leveranciers.
Om te voldoen aan de AVG is meer nodig dan het toepassen van het privacyconvenant en het certificeringsschema. Beide geven hier wel duidelijk richting aan en het certificeringsschema is

een manier om de passende technische en organisatorische maatregelen inzichtelijk te maken voor leverancier en voor school. De AVG is een aanleiding om door middel van het certificeringsschema het niveau van informatiebeveiliging in de keten te verhogen, maar individuele partijen hebben een eigen verantwoordelijkheid om aan wetgeving te voldoen. Gebruik van de nummervoorziening wordt door alle Edu-K partijen als een wenselijke maatregel beschouwd, maar is niet verplicht om aan de AVG te voldoen.

Totstandkoming certificeringsschema

De methodiek en beveiligingsmaatregelen die gezamenlijk het certificeringsschema vormen, zijn publiek-privaat tot stand gekomen binnen Edustandaard. In een open en transparant proces hebben alle belanghebbende partijen mee kunnen praten over de inhoud hiervan. De standaardisatieraad toetst dit proces en de architectuurraad bewaakt de samenhang met ketenreferentiearchitectuur ROSA en andere afspraken. Binnen de werkgroep die het certificeringsschema heeft ontwikkeld zijn ook partijen uit het hoger onderwijs en de administratieve keten betrokken, zodat het certificeringsschema sector- en ketenoverstijgend toepasbaar is.

Relatie met ISO

ISO 27001 en 27002 geven zelf geen niveaus of baseline aan voor specifieke maatregelen. De zwaarte van de te nemen maatregelen is niet voorgeschreven. Dus zelfs als alle leveranciers ISO-gecertificeerd zijn, dan moeten onderwijsinstellingen nog de nodige vragen stellen. Wat is de scope van de certificering, wordt de toepassing die ik afneem wel gedekt door deze scope? Welke maatregelen acht de leverancier van toepassing voor deze dienst, wat is het Statement of Applicabilty? Welke risico's zijn er afgedekt en zijn de genomen maatregelen daarvoor wel afdoende?

Het certificeringsschema heeft een en ander in het toetsingskader expliciet gemaakt op basis van expertise en best practices in de markt. Hiermee is het een verbijzondering, een nadere invulling, van de ISO-normen, toegespitst op de situatie en gebruikte producten in het onderwijs. Leveranciers en onderwijsinstellingen hebben gezamenlijk overeenstemming over deze invulling. Bij het opstellen van het certificeringsschema zijn de voor onderwijstoepassingen algemeen geldende risicogebieden in kaart gebracht, dit zijn de aandachtsgebieden in het toetsingskader. Op basis van de relevante richtlijnen uit de ISO 27002:2013 norm zijn daarbij voor drie niveaus concrete maatregelen opgesteld. Deze concrete invulling maakt voor onderwijsinstellingen en ict-leverancier duidelijk aan welke eisen precies voldaan moet zijn. De uitwerking die het certificeringsschema biedt, levert daarmee eenduidigheid op voor zowel leveranciers als afnemende scholen.

1.3 Doel document

Het doel van het implementatieplan is het bieden van een routekaart en daarmee een sturingsinstrument voor de implementatie van het certificeringsschema in de educatieve keten in het po, vo en mbo.

1.4 Doelgroep

De doelgroep van dit ketenimplementatieplan zijn alle publieke en private partijen die betrokken zijn bij de implementatie van het certificeringsschema in de educatieve keten.

1.5 Bronnen

Bij het opstellen van dit Implementatieplan is in elk geval gebruik gemaakt van de volgende bronnen:

- Certificeringsschema versie 2017 (concept)
- Ketenimplementatieplan ECK iD PO

- Ketenimplementatieplan ECK iD VO/MBO
- Convenant Digitale onderwijsmiddelen en Privacy 2.0
- Memo Nummervoorziening Certificeringsschema (14-09-2016)
- Technische voorschriften nummervoorziening (05-04-2017)
- Verslagen tactische overleggen Continuïteit en beveiliging

2 Projectdefinitie

2.1 Opdracht

Het certificeringsschema biedt een eenduidige werkwijze voor het bepalen van de juiste beveiligingsmaatregelen, een baseline voor deze maatregelen en een aanpak om hierover te rapporteren. Een uniforme werkwijze binnen het hele onderwijsdomein biedt zekerheid voor leveranciers en de middelen voor scholen om meer in control te zijn over een veilige omgang met leerlinggegevens. Hiervoor dienen alle leveranciers in de leermiddelenketen in staat te zijn om hun technische en organisatorische maatregelen inzichtelijk te maken via bijlage 2 van de bewerkersovereenkomst.

De opdracht voor de implementatie van het certificeringsschema luidt als volgt:
Zorg ervoor dat alle ketenpartijen in het po, vo en mbo op 25 mei 2018 conform het certificeringsschema hun beveiligingsmaatregelen inzichtelijk kunnen maken en op het gewenste niveau kunnen brengen, zodat scholen en leveranciers aan de verplichtingen van de AVG kunnen voldoen.[1]

2.2 Doelstelling implementatie certificeringsschema

Een gezamenlijke ambitie om te komen tot een veilige en betrouwbare keten, vergt een gezamenlijke aanpak. De implementatie van het certificeringsschema an sich is geen ketenvraagstuk. Iedere partij kan zelf de passende beveiligingsmaatregelen treffen. Echter, de keten is zo sterk als de zwakste schakel. Daarom is samenwerking op ketenniveau nodig voor ontwikkeling van de sector (het op orde brengen / verhoging van het algehele beveiligingsniveau) en voor acceptatie van het certificeringsschema als de te hanteren standaard. Wanneer ketenpartners gezamenlijk achter deze ambitie staan, kunnen zij niet alleen van elkaar leren om dit te bereiken, maar kunnen zij elkaar ook aanspreken wanneer de gestelde ambitie niet gehaald wordt.

Het primaire doel van implementatie van het certificeringsschema is verhoging van het beveiligingsniveau in de educatieve keten. Het gezamenlijk optrekken in Edu-K-verband heeft vier belangrijke doelen:

1. Verhoging van het niveau van informatiebeveiliging in de educatieve keten, zodat er minder incidenten optreden en er minder risico is op (reputatie)schade.
2. Gezamenlijk leren en collegiale ondersteuning bij implementatie van werkwijze en beveiligingsmaatregelen door leveranciers.
3. Acceptatie van het certificeringsschema door leveranciers in de educatieve keten en door schoolbesturen.
4. Ondersteuning en ontzorging van schoolbesturen om per 25 mei 2018 te kunnen voldoen aan de AVG.

2.3 Begrenzing / scope

- Doelstelling van dit implementatietraject betreft het gebruik van het certificeringsschema door alle partijen in de educatieve keten. Dit betekent dat dat implementatie in andere processen (OSO-uitwisseling, gegevenslevering aan DUO of Onderwijsinspectie, etc.) buiten scope van dit project is. Het certificeringsschema kan in deze processen wel worden toegepast.

[1] De doelstelling is zo geformuleerd dat individuele partijen zelf verantwoordelijk zijn om de gewenste beveiligingsmaatregelen, maar dat ze hierin worden ondersteund. Het is echter de ambitie van alle partijen om het beveiligingsniveau bij alle ketenpartijen te verhogen, en zij spannen zich in om dit te bevorderen.

- De implementatie van de beveiligingsvoorschriften bij de nummervoorziening die overeenkomen met het certificeringsschema, zijn buiten scope van dit project en worden ondersteund door het programma implementatie ECK iD.
- Implementatie van het certificeringsschema richt zich op leveranciers in de sectoren primair en voortgezet onderwijs en het middelbaar beroepsonderwijs.
- Ervaring opdoen met het certificeringschema en het inbrengen van lessons learned in het standaardisatieproces zijn onderdeel van de implementatie. Aanpassing van het certificeringsschema is geen onderdeel van dit project. Dit is belegd bij Edustandaard.
- Binnen de Aanpak IBP bieden de PO-Raad en VO-raad ondersteuning aan scholen om het beveiligingsniveau te verhogen. Op deze manier stellen de raden schoolbesturen in staat om aan de AVG te voldoen en om hun beveiligingsmaatregelen op een voldoende niveau te brengen. De mbo-sector heeft hiervoor de Toolbox IBP en Regiegroep IBP. Vanuit de sectorraden wordt de verbinding gelegd tussen deze activiteiten en de ondersteuning/producten/communicatie die onderdeel uitmaken van in het implementatieplan.
- Het doel van dit implementatietraject is dat *alle* leveranciers gebruik kunnen maken van het certificeringsschema. Voor een praktische afbakening wordt dit geoperationaliseerd als ‘alle partijen die het privacyconvenant hebben ondertekend’. Het tactisch overleg Privacy spant zich in voor vergroting van het aantal aangesloten partijen. Voor het mbo bestaat er geen convenant. Dit creëert een extra uitdaging voor het betrekken van partijen en het borgen van afspraken. Hiervoor wordt gebruik gemaakt van de contacten binnen het programma implementatie ECK iD.

2.4 Resultaten en producten

a) Ervaring opdoen met grotere en kleinere leveranciers
b) Bepaling van gevraagde ondersteuning en inrichting hiervan door tactisch overleg (voor zowel leveranciers als scholen)
c) Input leveren ten behoeve van aanpassing van het certificeringsschema
d) Opstellen van communicatieplan en opzetten van communicatie over certificeringsschema (mede i.r.t. andere activiteiten Edu-K en positionering t.o.v. andere normenkaders)
e) Opstellen van informatieproducten voor scholen (bijv. infographic, factsheet, checklist; i.r.t. de Aanpak IBP)
f) Onderzoek naar invulling ketenverantwoordelijkheid
g) Communicatie naar leveranciers over certificeringsschema (door brancheorganisaties, gecoördineerd vanuit Edu-K)
h) Communicatie naar scholen over certificeringsschema (door sectorraden, gecoördineerd vanuit Edu-K)
i) Zelfbeoordeling door individuele leveranciers (gecoördineerd door brancheorganisatie)
j) Opstellen van brancheoverstijgende heat-map op welke onderdelen van het certificeringsschema de meeste inspanningen moeten worden gericht t.b.v. eventueel extra ondersteuning
k) Opzetten van ondersteuning (op basis van behoefte leveranciers en aandachtspunten heatmap)
l) Verkenning verankering van certificeringsschema in privacyconvenant en/of modelbewerkersovereenkomst
m) Leveranciers zijn in staat om een rapportage conform certificeringsschema naar scholen te sturen wanneer de school daarom gevraagd
n) Leveranciers nemen benodigde maatregelen om te voldoen aan de minimale eisen uit het certificeringsschema
o) Ondersteuning vanuit Edu-K door bijv. groepen/overleggen op operationeel niveau voor individuele leveranciers en door inrichting van een ‘vraagbaak’ voor afstemming, beantwoording van vragen en uitwisseling van ervaringen en lessons learned

p) Het maken van publiek-private afspraken over (externe) toetsing van naleving van het certificeringsschema

2.5 Uitgangspunten

Uitgangspunten zijn:

- Kunnen voldoen aan de AVG per 25 mei 2018 is leidend voor het implementatietraject. Het certificeringsschema alleen is hier niet voldoende voor, maar biedt in combinatie met het privacyconvenant een belangrijke handreiking. Iedere leverancier en ieder schoolbestuur is individueel verantwoordelijk voor het voldoen aan de AVG.
- De ondersteuning vanuit Edu-K bestaat primair uit het faciliteren van communicatie, kennisdeling en inbreng van expertise.
- Voor het primair en voortgezet onderwijs zijn het privacyconvenant en de modelbewekers-overeenkomst natuurlijke landingsplaatsen voor verankering van het certificeringsschema.
- Voor de implementatie van het certificeringsschema wordt op operationeel niveau zoveel mogelijk aangesloten bij de reeds bestaande groepen en overleggen.
- De implementatie van het certificeringsschema wordt zoveel mogelijk in samenhang ingevuld met het programma implementatie ECK iD. De betekenis hiervan voor de twee implementatiegroepen is uiteengezet in de figuur in paragraaf 4.3. Het is nadrukkelijk niet de bedoeling dat partijen die het ECK iD gaan gebruiken per schooljaar 2018/2019 wachten met de implementatie van het certificeringsschema.
- Gestreefd wordt naar het optimaal benutten en inzichtelijk maken van de verschillende trajecten rondom ECK iD, privacy en beveiliging.
- De PO-Raad, VO-raad en MBO Raad maken zich sterk voor het toepassen van de Aanpak IBP (po/vo) en de Toolbox IBP (mbo) om privacy en informatiebeveiliging in de sector op het gewenste niveau te brengen en zo te voldoen aan de AVG;
- Edu-K is opdrachtgever van het project; het tactisch overleg is opdrachtnemer.

2.6 Implementatie-uitdagingen

Uitdagingen zijn:

- Het certificeringsschema moet door scholen, leveranciers en accountants van scholen worden geaccepteerd als dé standaard voor de minimale gegevensbescherming in het onderwijsdomein.
- Schoolbesturen moeten op termijn het voldoen aan het certificeringsschema gaan verwachten van al hun leveranciers van digitale producten.
- Schoolbesturen benoemen bij inkooptrajecten het certificeringsschema als de te hanteren norm voor, maar verlangen van leveranciers niet eerder dan 25 mei 208 dat zij voldoen aan deze norm.
- Wanneer het certificeringsschema succesvol is geïmplementeerd door alle leveranciers, is dit een duidelijke verbetering van de beveiliging in de keten. Maar ook scholen moeten hun beveiliging goed op orde hebben en op dit moment is dat in veel gevallen nog niet zo.
- Voor kleine partijen kan implementatie van het certificeringsschema een grote impact hebben. Enerzijds moet er aandacht voor zijn dat ook kleinere partijen met het certificeringsschema kunnen werken, anderzijds mag van iedere partij verwacht worden dat zij aan een minimale set beveiligingseisen voldoen.
- Voor het po en vo kan het certificeringsschema worden verankerd in het privacyconvenant. In het mbo is een dergelijk convenant er (nog) niet. Hiermee ontbreekt een logische plek voor deze verankering.
- Het certificeringsschema kent een belangrijke relatie met de implementatie van het ECK iD. De samenhang tussen beide projecten biedt kansen voor leveranciers om beide implementaties tegelijk op te pakken, maar biedt risico's wanneer leveranciers moeten

prioriteren. Voor de communicatie over het certificeringsschema is het tevens van belang deze samenhang inzichtelijk te maken.

2.7 Relatie met andere projecten

Het project heeft relaties met de volgende projecten en activiteiten:

- Implementatie ECK iD (Edu-K)
- Privacyconvenant en modelbewerkersovereenkomst po/vo (en herziening daarvan) (Edu-K)
- Ontwikkeling en beheer certificeringsschema (Edustandaard)
- Aanpak IBP (PO-Raad en VO-raad)
- Regiegroep IBP / Toolbox IBP (saMBO-ICT)

3 Gewenste situatie

3.1 Werking en gebruik certificeringsschema in de keten

Gebruik van het certificeringsschema moet zowel voor schoolbesturen als leveranciers gemak en efficiëntie bieden bij het voldoen aan de verplichtingen van de inwerkingtreding van de AVG per 25 mei 2018. De classificatie en rapportage uit het certificeringsschema bieden voor leveranciers een duidelijk inzicht in of zij ‘passende technische en organisatorische maatregelen’ ten aanzien van persoonsgegevens hebben getroffen. De rapportage stelt hen in staat dit ook aan hun klanten te communiceren. Wanneer alle vragende partijen in de onderwijsmarkt vragen om een rapportage conform het certificeringsschema, en daarnaast niet meer en niet minder verwachten dan de minimale beveiligingseisen die het certificeringsschema voorschrijft, biedt dit een duidelijk voordeel voor de aanbodzijde van de markt.

Voor de vraagzijde van de markt maakt een eenduidige wijze van rapporteren het eenvoudiger om te kunnen beoordelen of er ‘passende technische en organisatorische maatregelen’ zijn getroffen. Wanneer er op basis van een classificatie een duidelijke set aan voorschriften is, waar een leverancier slechts beargumenteerd van af kan wijken, is relatief eenvoudig te controleren of de school hiermee akkoord moet gaan of aanvullende maatregelen mag verwachten. Immers, wanneer een leverancier bij alle vakjes een vinkje heeft staan, kan de school erop vertrouwen dat deze zijn zaken goed heeft geregeld.
Breed gebruik van het certificeringsschema heeft tevens als voordeel dat er een gemeenschappelijk kader is op basis waarvan in de toekomst mogelijk audits kunnen worden uitgevoerd die voor het hele onderwijs beschikbaar zijn.

3.2 Usecases certificeringsschema (op hoofdlijnen)

1. Ik wil als leverancier weten welke beveiligingsmaateregelen ik moet treffen, zodat ik aan de in de markt geldende standaard (en de wensen van mijn klant) kan voldoen.
2. Ik wil als leverancier op een eenduidige manier kunnen rapporteren, zodat ik aan mijn klanten kan laten zien dat ik ‘passende technische en organisatorische maatregelen’ heb getroffen.
3. Ik wil als schoolbestuur een helder overzicht van de getroffen beveiligingsmaatregelen door mijn leverancier ontvangen, zodat ik deze ‘eenvoudig’ kan beoordelen en in control kan zijn zoals de AVG voorschrijft.
4. Ik wil als schoolbestuur (gezamenlijk of zelfstandig) externe audits uit kunnen laten voeren op mijn leveranciers, zodat duidelijk is dat een leverancier daadwerkelijk het gewenste beveiligingsniveau biedt.

4 Aanpak, fasering en planning

4.1 Aanpak

Het gezamenlijk optrekken in Edu-K-verband heeft vier belangrijke doelen:

- Verhoging van het niveau van informatiebeveiliging in de educatieve keten verhogen, zodat er minder incidenten optreden en er minder risico is op (reputatie)schade.
- Gezamenlijk leren en collegiale ondersteuning bij implementatie van werkwijze en beveiligingsmaatregelen bij leveranciers.
- Acceptatie van het certificeringsschema door leveranciers in de educatieve keten en door schoolbesturen.
- Ondersteuning en ontzorging van schoolbesturen om per 25 mei 2018 te kunnen voldoen aan de AVG.

Voor de implementatie van het certificeringsschema in de leermiddelenketen hanteren we een ketenaanpak, waarbij publieke en private ketenpartners samenwerken om tot een succesvolle implementatie te komen. Enerzijds is sprake van een 'centraal' ketenimplementatieplan waar alle publieke en private partijen zich aan committeren. Anderzijds hebben individuele ketenpartners hun eigen verantwoordelijkheid voor de implementatie en het gebruik van het certificeringsschema in hun eigen systemen en processen. Deze implementaties door individuele ketenpartners vinden uiteraard wel plaats binnen de kaders en tijdslijnen die op centraal niveau in ketenverband met elkaar worden afgesproken. Individuele ketenpartners kunnen elkaar hier ook op aanspreken. Op bestuurlijk niveau geeft het Edu-K platform sturing aan het implementatieprogramma. Op tactisch niveau vindt in het tactisch overleg Continuïteit en beveiliging afstemming plaats tussen de ketenpartners.

Gezien de potentieel grote impact die deze implementatie kan hebben op leveranciers en de relatie met het implementatieprogramma ECK iD, kiezen we voor een aanpak die start met het opdoen van praktijkervaringen en een checklist voor alle leveranciers en werken we langs de lijn van de beveiligingseisen bij de nummervoorziening toe naar een algehele implementatie.

4.2 Fasering

In lijn met de hiervoor geschetste aanpak kiezen we voor de volgende fasering:

1. Kwartiermaken
2. Communicatie en zelfbeoordeling
3. Implementatie beveiligingsmaatregelen bij ECK iD BUITEN SCOPE
4. Rapportage conform certificeringsschema beschikbaar voor scholen
5. Implementatie beveiligingsmaatregelen certificeringsschema *Mijlpaal:*
6. Afspraken externe toetsing beveiligingsmaatregelen

1. Kwartiermaken

In deze fase vinden de voorbereidingen plaats om het certificeringsschema breed te introduceren bij leveranciers in het educatieve domein. De nadruk ligt op het opdoen van ervaringen met (de documentatie bij) certificeringsschema door verschillende (grotere en kleinere) leveranciers. Op basis van deze ervaringen kunnen nog aanpassingen aan het certificeringsschema zelf worden gedaan en wordt verder uitgewerkt welke behoefte er is aan ondersteuning bij de implementatie. Het is wenselijk om dit met één á twee leveranciers per branche te doen. Hierbij rekening houdend met de activiteiten die al in verschillende branches zijn uitgevoerd (pilots VDOD, traject KBb-E).
Tevens wordt in de kwartiermakersfase gewerkt aan een goede positionering van het certificeringsschema. Dit betreft in het bijzonder de relatie met andere normen en kaders. In deze

fase worden ook gesprekken gevoerd door leden van het tactisch overleg met vertegenwoordigers van accountants en auditors over de manier waarop zij een bijdrage kunnen leveren aan de positionering van het certificeringsschema. Daarbij komt dat leveranciers aan scholen diverse andere partijen inhuren en sub-bewerkers inschakelen. Ook in deze keten moet de veiligheid en betrouwbaarheid worden geborgd. Onderzoek naar de wijze waarop deze keten-verantwoordelijkheid kan worden ingevuld is eveneens onderdeel van de kwartiermakersfase. Ook communicatie richting scholen is een belangrijk onderdeel van deze fase. Extra aandacht en producten zijn nodig, dit geldt ook voor toepassing van het certificeringsschema door scholen wanneer zij zelf applicaties beheren.

In deze fase worden de volgende activiteiten uitgevoerd:

a) Ervaring opdoen met grotere en kleinere leveranciers
b) Bepaling van gevraagde ondersteuning en inrichting hiervan door tactisch overleg (voor zowel leveranciers als scholen)
c) Input leveren ten behoeve van aanpassing van het certificeringsschema
d) Opstellen van communicatieplan en opzetten van communicatie over certificeringsschema (mede i.r.t. andere activiteiten Edu-K en positionering t.o.v. andere normenkaders)
e) Opstellen van informatieproducten voor scholen (bijv. infographic, factsheet, checklist; i.r.t. de Aanpak IBP)
f) Onderzoek naar invulling ketenverantwoordelijkheid

2. Communicatie en zelfbeoordeling

In deze fase start de daadwerkelijke communicatie naar leveranciers over het certificeringsschema. Brancheorganisaties nemen hun leden hierin mee en ondersteunen hen om ervoor te zorgen dat alle leden hun eigen beveiligingsmaatregelen beoordelen op basis van het certificeringsschema. Deze zelfboordeling wijst voor leverancier uit welke inspanningen zij nog moeten doen aan het gewenste beveiligingsniveau te voldoen.
Parallel hieraan moet ook duidelijk richting scholen worden gecommuniceerd op welke wijze het certificeringsschema hen helpt om aan de AVG te voldoen, en worden scholen door de sectorraden geïnformeerd over de minimaal te nemen maatregelen om hun eigen beveiliging op orde te hebben conform de AVG.

In deze fase worden de volgende activiteiten uitgevoerd:

g) Communicatie naar leveranciers over certificeringsschema (door brancheorganisaties, gecoördineerd vanuit Edu-K)
h) Communicatie naar scholen over certificeringsschema (door sectorraden, gecoördineerd vanuit Edu-K)
i) Zelfbeoordeling door individuele leveranciers (gecoördineerd door brancheorganisatie)
j) Opstellen van branche-overstijgende heat-map op welke onderdelen van het certificeringsschema de meeste inspanningen moeten worden gericht t.b.v. eventueel extra ondersteuning
k) Opzetten van ondersteuning op basis van behoefte leveranciers en aandachtspunten heatmap (kennisdeling/vraagbaak; hierbij zoveel mogelijk aansluiten bij projectgroepen ECK)
l) Verkenning verankering van certificeringsschema in privacyconvenant en/of modelbewerkersovereenkomst

BUITEN SCOPE

3. Implementatie beveiligingsmaatregelen bij ECK iD

Partijen die per september 2018 gaan werken met het ECK iD, zullen conform planning van het programma implementatie ECK iD de nodige beveiligingsmaatregelen treffen. Hier is een duidelijke synergie. De ondersteuning die hiervoor nodig is zal worden geleverd door het programma implementatie ECK iD. Partijen die per september 2019 het ECK iD gaan gebruiken, zullen deze maatregelen in 2019 implementeren.

In deze fase worden *binnen het programma implementatie ECK iD* de volgende activiteiten uitgevoerd:

x) Implementatie onderdelen uit het certificeringsschema die overeenkomen met de technische voorschriften bij de nummervoorziening door leveranciers

4. Rapportage beschikbaar voor scholen

Op 25 mei 2018, wanneer de AVG van kracht gaat, kunnen alle leveranciers hun rapportage over technische en organisatorische maatregelen beschikbaar maken voor hun klanten.

In deze fase worden de volgende activiteiten uitgevoerd:

m) Leveranciers zijn in staat om een rapportage conform certificeringsschema naar scholen te sturen wanneer de school daarom gevraagd

5. Implementatie beveiligingsmaatregelen certificeringsschema

Op basis van de zelfevaluatie weten leveranciers welke beveiligingsmaatregelen ze hebben getroffen en van welke maatregelen scholen van hen verwachten op basis van publiek-private afspraken. Deze maatregelen worden door de leveranciers genomen.

In deze fase worden de volgende activiteiten uitgevoerd:

n) Ondersteuning vanuit Edu-K door bijv. groepen/overleggen op operationeel niveau voor individuele leveranciers en door inrichting van een 'vraagbaak' voor afstemming, beantwoording van vragen en uitwisseling van ervaringen en lessons learned

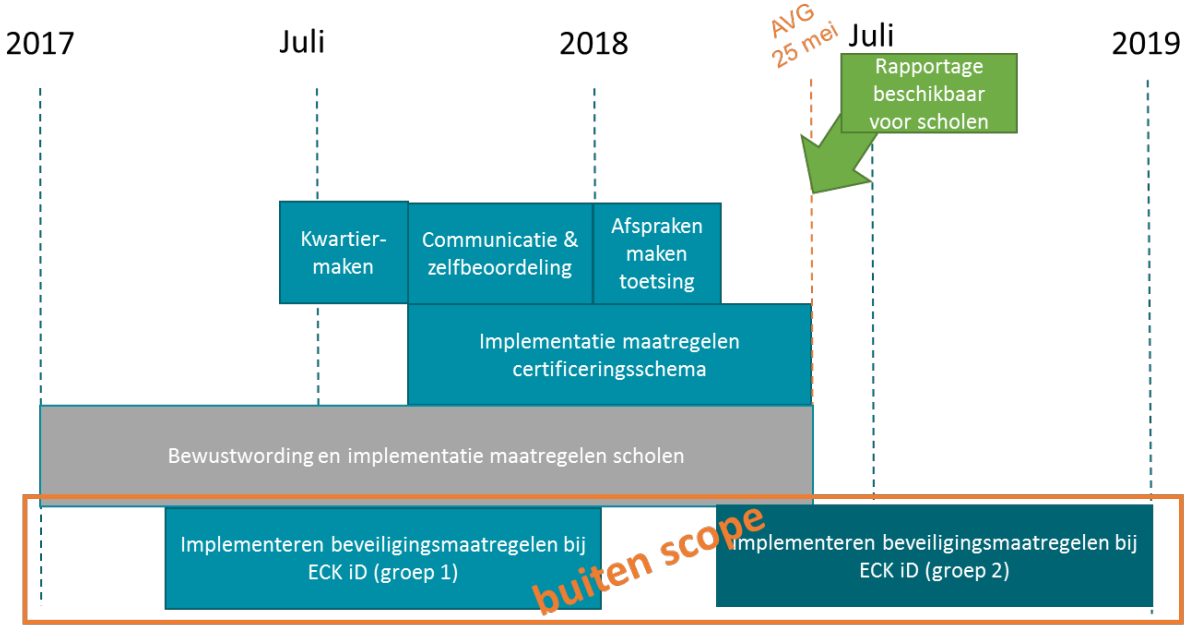
6. Afspraken (externe) toetsing certificeringsschema

Na invoering van de AVG is het gewenst dat getoetst kan worden of de beveiligingsniveaus ook daadwerkelijk worden gerealiseerd. Formeel kunnen scholen dit nu al vragen van hun leveranciers, maar door hier publiek-privaat afspraken over te maken ontstaat hier potentieel een efficiëntievoordeel en kunnen scholen worden ontzorgd. De zelfrapportage is hier een voorbeeld van maar ook andere vormen van toetsing zijn mogelijk.

In deze fase worden de volgende activiteiten uitgevoerd:

o) Het maken van publiek-private afspraken over (externe) toetsing van naleving van het certificeringsschema

4.3 Planning



5 Organisatie

5.1 Opdrachtgever

De opdrachtgever van het project implementatie certificeringsschema is Edu-K.

Binnen Edu-K wordt:
- Het implementatieplan certificeringsschema vastgesteld;
- Input gegeven op de samenhang tussen realisatie, implementatie en het bestuurlijke traject;
- Besluiten genomen over de wijze van implementatie;
- Verantwoording afgelegd over de voortgang.

5.2 Opdrachtnemer

Tactisch overleg Continuïteit en beveiliging.

5.3 Projectorganisatie

Gezien de 'lichte' vorm van het project zoals is beschreven in dit plan, zal de projectorganisatie ook op een lichte manier worden ingericht. Het gehele tactisch overleg zal de verantwoordelijkheid dragen voor de voortgang van de daadwerkelijke implementatie en dus werk moeten verrichten. Veel activiteiten, zoals het onder de aandacht brengen van de activiteiten en het ertoe bewegen dat leveranciers aan de slag gaan met bijvoorbeeld de zelfevaluatie, zal door de brancheorganisaties zelf ingevuld moeten worden. Vanuit Kennisnet kunnen de randvoorwaarden hiervoor worden ingevuld. Verder zijn de volgende rollen gedefinieerd:
- Inspanningsleiders & coördinerende functie: vertegenwoordigers branche- en sectororganisaties in tactisch overleg Continuïteit en beveiliging
- Expert informatiebeveiliging en certificeringsschema: Axel Eissens / Dirk Linden (Kennisnet)
- Implementatieondersteuning: n.t.b. (Kennisnet)
- Coördinatie communicatie: implementatieondersteuner + secretaris TO