

Aanmeldformulier

Voor : Standaardisatieraad, Edustandaard
Van : Dirk Linden
Datum : 22 maart 2018
Betreft : Update Certificeringsschema informatiebeveiliging en privacy ROSA 2018

Toelichting op de toepassing van dit aanvraagformulier

Beheer of registratie

Dit aanvraagformulier wordt gebruikt voor registratie of het in beheer laten nemen van een afspraak¹ bij Edustandaard. Bij registratie ligt de ontwikkeling en besluitvorming (deels) buiten Edustandaard maar is er wel de intentie om het beheer in een later stadium over te dragen. Bij het in beheer nemen ligt de (door)ontwikkeling, het beheer en de besluitvorming binnen het platform Edustandaard.

Doel

Op basis van de antwoorden op de vragen in dit aanvraagformulier stelt bureau Edustandaard een advies op. Bij twijfel over de relevantie, het werkingsgebied of kwaliteit kan bureau Edustandaard besluiten een gesprek te voeren met de indiener. Het advies zal aan de indiener aangeboden worden voor een respons en vervolgens aan de Architectuurraad en de Standaardisatieraad worden voorgelegd.

Doelgroepen:

- **Bureau Edustandaard** beoordeelt op basis van deze vragenlijst in hoeverre aan de criteria is voldaan. Het bureau adviseert hierin de indiener en Standaardisatieraad.
- Een **werkgroep bij Edustandaard** zal de afspraak inhoudelijk bekijken en zal daarover een advies opstellen aan de Standaardisatieraad. Het is afhankelijk van de inhoud van de afspraak of en bij welke werkgroep deze wordt behandeld.
- De **Architectuurraad** bewaakt en beoordeelt de samenhang met de andere afspraken (architectuur) die in beheer of geregistreerd zijn bij Edustandaard en brengt hierover advies uit voor de Standaardisatieraad.
- De **Standaardisatieraad** zal op basis van de vragenlijst en de adviezen besluiten om de standaard al dan niet in beheer te nemen of te laten registreren bij Edustandaard.

Let op: Bij het beantwoorden van de vragen graag verwijzingen naar de documentatie opnemen. De antwoorden moeten terug te vinden zijn in de bijbehorende documentatie.

¹ Waar afspraak staat kan ook (informatie)model, begrippenset of architectuur gelezen worden.

De vragen

1. Om welke afspraak gaat het?

1.1. Wat is de naam en laatste wijzigingsdatum?

naam	datum
Certificeringsschema informatiebeveiliging en privacy ROSA (versie 2018)	maart 2018

1.2. Geef een overzicht van de bijbehorende documentatie, online en offline.

titel en/of URL	auteur(s)	versienummer	status
1. Certificeringsschema_algemene_beschrijving	Edustandaard werkgroep IBP	2.05	
2. Certificeringsschema_proces	Edustandaard werkgroep IBP	2.05	
3. Certificeringsschema_classificatie	Edustandaard werkgroep IBP	2.0	
4. Certificeringsschema_toetsingskader	Edustandaard werkgroep IBP	1.2	
5. Certificeringsschema_toezicht	Edustandaard werkgroep IBP	2.05	

2. Beschrijf de afspraak:
2.1. Waar gaat de afspraak over?

antwoord	verwijzing
<p>De afspraak is een gezamenlijk opgesteld 'normenkader', een baseline van maatregelen op het gebied van informatiebeveiliging voor organisaties die diensten – ondersteund door ict-toepassingen – leveren in de onderwijsketen.</p> <p>Op basis van een voorgeschreven werkwijze bepaalt een leverancier een beveiligingsniveau. Aan dit beveiligingsniveau zijn specifieke maatregelen gekoppeld die gelden als een baseline waaraan de leverancier dan moet voldoen (comply) of een beargumenteerde afwijking voor moet geven (explain).</p> <p>Er is een rapportageformat waardoor invullen en toetsen wordt vergemakkelijkt. Er zijn verschillende niveaus van toezicht gedefinieerd, van zelftoetsing tot externe audit. Daardoor hebben andere partijen inzicht in hoeveel vertrouwen gegeven kan worden aan de uitspraak van een leverancier dat deze aan het Certificeringsschema voldoet.</p>	<p>1.Certificeringsschema_algemene_beschrijving.docx 2.Certificeringsschema_proces.docx 5.Certificeringsschema_toezicht.docx</p>

2.2. Wat is de aanleiding geweest? (Bijv. wettelijke kaders, een projectdoelstelling of vanuit een bedrijfs- of ketenmissie.)

antwoord	verwijzing
<p>Na inbeheername in 2017 is vanuit de praktijk en de werkgroep IBP terugkoppeling gekomen ter verheldering, verbetering en ondersteuning van de implementatie. Ook zijn er voortschrijdende inzichten in relatie tot risicobeelden en de stand van de techniek.</p> <p>Deze terugkoppeling en voortschrijdende inzichten zijn gedurende het afgelopen jaar door de werkgroep IBP verwerkt in een nieuwe tussentijdse versie.</p>	<p>https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-2017/</p> <p>https://www.edustandaard.nl/standaard_bijeenkomsten/?edu_orderby=meta_value_num&edu_werkgroep%5B%5D=595</p>

2.3. Wat is het doel?

antwoord	verwijzing
Het doel van het Certificeringsschema is driedig: <ul style="list-style-type: none">• Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy;• Transparantie bieden over welke ICT-toepassingen voldoen aan deze baseline;• Het creëren van een solide basisniveau van informatiebeveiliging voor alle geleverde ict-toepassingen in de onderwijsketen.	1.Certificeringsschema_algemene_beschrijving.docx hoofdstuk 1, paragraaf 2

2.3.1. Wat gaat er fout als de afspraak niet geaccepteerd wordt door het veld?

antwoord	verwijzing
<p>Scholen komen dan met verschillende normenkaders waaraan organisaties die ict-diensten leveren getoetst gaan worden, wat de auditdruk vergroot. Voor elk normenkader zou dan namelijk een andere audit uitgevoerd moeten worden.</p> <p>Organisaties die ict-diensten leveren worden niet expliciet getoetst op een breed gedragen normenkader in de onderwijssector, waardoor niet inzichtelijk wordt welke leveranciers informatiebeveiliging wel op orde hebben, en welke leveranciers informatiebeveiliging niet op orde hebben. Dit leidt mogelijk tot een onvoldoende niveau van informatiebeveiliging, willekeur en geen transparantie.</p> <p>Nieuwe toetreders op de markt zijn niet bekend met de baseline van beveiligingsmaatregelen waardoor nieuwe innovatieve producten het risico op beveiligingsincidenten mogelijk vergroten.</p> <p>Voor informatiebeveiliging in de keten wordt de kans gemist om het momentum te gebruiken wat nu bij leveranciers ontstaat. Deze willen het goede voorbeeld geven door het Certificeringsschema te gaan gebruiken, zodat scholen op hun beurt ook kunnen werken aan maatregelen bij de scholen zelf.</p>	

2.3.2. Hoe urgent is de afspraak?

antwoord	verwijzing
Het is belangrijk om jaarlijks een update uit te brengen om voortschrijdende inzichten en actuele risico's te kunnen verwerken in maatregelen. De goedkeuring van een nieuwe versie door de architectuur- en standaardisatieraad draagt bij aan de acceptatie in de onderwijsketen.	

2.3.3. Biedt de afspraak een volledige oplossing voor het beoogde doel en de beoogde doelgroep?

antwoord	verwijzing
De afspraak biedt een oplossing om de genomen technische maatregelen te toetsen. De roadmap bevat onder andere een uitbreiding voor maatregelen op het gebied van organisatie en proces. Tevens verwachten we op basis van de implementatie feedback en uitbreidingsvoorstellen van organisaties die ict-diensten leveren, onderwijsinstellingen en andere belanghebbenden.	6.Certificeringsschema_roadmap.xlsx

2.4. Wat is het werkingsgebied? (Bijv. onderwijssectoren, organisaties.)

antwoord	verwijzing
De afspraak is van toepassing binnen de onderwijssector. Binnen deze sector bieden verschillende organisaties diensten aan, welke ondersteund worden door een ict-toepassing (bijvoorbeeld administratie van uitgifte van fysieke leermiddelen) of zijn zelf een ict-toepassing zijn (bijvoorbeeld digitaal leermateriaal). Het certificeringsschema betreft maatregelen voor deze ict-toepassingen.	1.Certificeringsschema_algemene_beschrijving.docx hoofdstuk 1

2.5. Wat is het toepassingsgebied? (Bijv. administratieve domein, onderzoek, leermiddelendomein.)

antwoord	verwijzing
De afspraak breed toepasbaar in alle sectoren van het onderwijs (po, vo, mbo en ho). De afspraak wordt door het Privacyconvenant als geldige invulling genoemd voor het beveiligen van digitale leermiddelen en leerlingadministratiesystemen in het po, vo en mbo. Voor elke ict-dienst moet een bewerkersovereenkomst gesloten worden, waarbij het certificeringsschema invulling geeft aan de eis om "passende technische en organisatorische maatregelen" te treffen op de ict-toepassing.	1.Certificeringsschema_algemene_beschrijving.docx hoofdstuk 1

2.6. Wie is de doelgroep? (Bijv. DUO, onderwijsinstellingen, LAS-systemen, uitgevers.)

antwoord	verwijzing
Organisaties die ict-diensten leveren in de onderwijsketen: deze kunnen per toepassing door een eenduidig normenkader aantonen dat ze informatiebeveiliging op orde hebben en transparant maken op welke wijze ze dit doen. Onderwijsinstellingen: onderwijsinstellingen kunnen eenvoudiger eisen stellen op het gebied van informatiebeveiliging en eenvoudiger (laten) toetsen of een ict-leverancier informatiebeveiliging op orde heeft.	1.Certificeringsschema_algemene_beschrijving.docx hoofdstuk 1, paragraaf 3

2.6.1. Bestaat de afspraak uit verschillende delen die zich op verschillende doelgroepen richten en zo ja, welke?

antwoord	verwijzing
Nee. De afspraak bestaat wel uit verschillende onderdelen maar is geheel gericht op de organisaties die door middel van het certificeringsschema willen aantonen dat ze de informatiebeveiliging van een specifieke ict-toepassing op orde hebben. Binnen deze documentatie wordt de organisatie geholpen om zelf andere doelgroepen (bijvoorbeeld auditors) te bedienen.	Alle documentatie

3. Hoe past de afspraak in het grotere geheel?

3.1. Aan welke referentiearchitectuur is de afspraak gekoppeld?

antwoord	verwijzing
De afspraak valt onder de katern informatiebeveiliging en privacy van de ROSA.	http://www.wikixl.nl/wiki/rosa

3.2. Welke architectuurprincipes zijn gerelateerd aan de afspraak? (Geef bij voorkeur aan hoe die relatie ligt.)

antwoord	verwijzing
De afspraak geeft praktische invulling aan het principe "basisniveau informatiebeveiliging en privacy" doordat de afspraak een baseline (lees: basisniveau) vastlegt van concrete maatregelen op dit gebied.	http://www.wikixl.nl/wiki/rosa

3.3. Op welke (keten)processen heeft de afspraak betrekking? (Bijv. in- en uitschrijfprocessen tussen instellingen.)

antwoord	verwijzing
De afspraak betreft geen uitwisselingsstandaard maar een standaard voor de beveiliging van een ict-toepassing. Daarmee heeft het certificeringsschema geen betrekking op een specifiek (keten)proces.	http://www.wikixl.nl/wiki/rosa

3.4. Op welke gegevenssoorten heeft de afspraak betrekking? (Bijv. persoonsgegevens, leermateriaal, metadata, leerresultaten.)

antwoord	verwijzing
De afspraak heeft in principe betrekking op alle gegevenssoorten. De classificatie stelt in het bijzonder vragen over (bijzondere) persoonsgegevens en leerresultaten omdat deze een hoger vertrouwelijkheids-/integriteitsniveau vereisen dan overige gegevenssoorten die niet door de AVG of andere wetgeving een hogere beveiliging vereisen.	2.Certificeringsschema_proces.docx

3.5. In welk formaat worden de data beschikbaar gesteld? (Bijv. in XML, Turtle (LOD), JSON, CSV.)

antwoord	verwijzing
Niet van toepassing.	

3.6. Welke regels zijn vastgelegd over wie de data mag inwinnen, opslaan, wijzigen, beschikbaar stellen, inzien en/of vernietigen?

antwoord	verwijzing
Niet van toepassing.	

3.7. Welke relatie hebben de begrippen in de afspraak met andere begrippen in het onderwijs?

3.7.1. Welke begrippen zijn te relateren aan KOI of zouden dat moeten kunnen?

begrip uit de afspraak	relatie	KOI-begrip uit <KOI-versie>
Niet van toepassing.		

3.7.2. Welke begrippen zijn vergelijkbaar met begrippen uit andere bronnen binnen het onderwijsveld?

begrip uit de afspraak	relatie	begrip uit andere onderwijsveldbron
Niet van toepassing.		

3.7.3. Welke begrippen zijn gerelateerd aan begrippen buiten het onderwijsveld?

begrip uit de afspraak	relatie	begrip buiten het onderwijsveld
Niet van toepassing.		

3.7.4. In welk formaat worden de begrippen beschikbaar gesteld?

antwoord	verwijzing
Niet van toepassing.	

3.8. Op welke manier is de informatiebeveiliging vormgegeven?

antwoord	verwijzing
Het Certificeringsschema stelt hierover kaders aan ict-toepassingen.	

3.9. Op welke manier is privacy gewaarborgd?

antwoord	verwijzing
Het Certificeringsschema stelt hierover kaders aan ict-toepassingen.	

3.10. Op welke manier komen identificatie, authenticatie en autorisatie aan de orde?

antwoord	verwijzing
Niet van toepassing.	

3.11. Op welke services, voorzieningen en/of infrastructuur heeft de afspraak betrekking? (Bijv. Edukoppeling, Edurep, ENTREE-federatie, Metaplus, BME, Linked Open Data-API.)

antwoord	verwijzing
Het certificeringsschema kan voor alle ict-toepassingen worden ingezet om de beveiligingsmaatregelen te toetsen. Het maakt geen onderdeel uit, maar is een aanvulling op de beveiliging van ict-toepassingen die mogelijk met Edukoppeling aan elkaar zijn gekoppeld.	

3.12. Wat is de samenhang van deze afspraak met andere afspraken en standaarden?

3.12.1. Is de afspraak gebaseerd op (inter)nationale standaarden en zo ja, welke?

naam standaard	versie	datum	verwijzing
ISO 27001 en ISO 27002 zijn gebruikt ter inspiratie voor maatregelen in het toetsingskader	2013/NL	1 oktober 2013	https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-nl.htm
Voorgaande versies maakten gebruik van de "Cloud Control Matrix" van de Cloud Security Alliance. Voor backwards compatibility zijn in deze versie verwijzingen hiernaar opgenomen.	v3.01	11 juli 2014	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

3.12.2. Welke afspraken en standaarden zijn gerelateerd met deze afspraak en waar raken ze elkaar? (Bijv. afspraken en standaarden zowel binnen als buiten het onderwijs, zowel binnen als buiten Nederland. Bijv. welke principes komen overeen; zijn er services die ook binnen andere afspraken een rol spelen? Nota bene: Samenhang kan ook worden aangegeven door de verschillen te benoemen.)

naam afspraak	raakpunten in overeenkomsten en/of verschillen	verwijzing
Normenkader informatiebeveiliging MBO	Beveiligingsniveaus komen overeen. Verskil is dat het Certificeringsschema concrete technische maatregelen en niveaus toekent.	

HO normenkader	Idem als normenkader MBO (welke is gebaseerd op het HO normenkader)	
----------------	---	--

3.13. Zijn er nog andere zaken die randvoorwaardelijk zijn en waar de afspraak betrekking op heeft en zo ja, welke?

antwoord	verwijzing
Een afspraak die gerelateerd is aan het Certificeringsschema is de Edukoppeling transactiestandaard. Deze heeft een verwijzing naar het Certificeringsschema. Zie ook antwoord 3.11. Verder is er samenhang met ROSA, Privacyconvenant en normenkaders in het mbo en hoger onderwijs, zoals beschreven bij 3.12.2.	Certificeringsschema.docx hoofdstuk 1 paragraaf 4. http://www.edustandaard.nl/afspraken-en-architectuur/beheerde-afspraken/edukoppeling/

4. Is de afspraak breed geaccepteerd door de doelgroep?

4.1. Welke partijen en welke personen waren betrokken bij de ontwikkeling?

antwoord	verwijzing
Ja Leden IBP werkgroep: Kennisnet (Job Vos, Axel Eissens, Dirk Linden) DUO (Ad van Etten) VDOD, Educus (Herrie Abbink) KBb-e, van Dijk (Paul Arnold, Marten Bakker) OCW (Oscar ter Meer) SURF (Alf Moens) GEU, ThiemeMeulenhof (Rob van der Staaij, Rimmer Hylkema) MBO (Ludo Cuijpers) Tevens regelmatig besproken en feedback opgehaald in Tactisch Overleg Continuïteit en Beveiliging daarin zijn de volgende branches vertegenwoordigd: Distributeurs KBb-E Uitgevers GEU VDOD OCW PO-raad VO-raad MBO-raad (agendalid)	Zie notulen https://www.edustandaard.nl/standaard_bijeenkomsten/?edu_orderby=meta_value_num&edu_werkgroep%5B%5D=595

4.2. Wie zijn op welke manieren ingelicht over de afspraak? (Bijv. bijeenkomsten, seminars, FAQ's op websites, fora, papers.)

antwoord	verwijzing
Via Edustandaard werkgroep IBP en Edu-K tactisch overleg continuïteit en beveiliging: GEU (René Montenarie, Jannes Hessels) KBb-E (Herman van der Vegte, Paul Arnold, Albert Jagt) VDOD (Ernst-jan Heuseveldt) Thieme Meulenhoff (Rob van der Staaij) OCW (Oscar ter Meer) PO-Raad (Maurits Huigsloot) VO-raad (Anna Serraris, Anne Goris) Op de website van Edustandaard worden de vastgestelde en meest recente documenten van de (concept) afspraak gepubliceerd.	Notulen werkgroep IBP Notulen TO C&B www.edustandaard.nl https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-2017/

4.3. Zijn er openbare verslagen en/of besluitenlijsten van bijeenkomsten die aantonen dat de afspraak breed is geaccepteerd en zo ja, welke?

antwoord	verwijzing
Ja, in Edustandaard werkgroep informatiebeveiliging en Edu-K tactisch overleg continuïteit en beveiliging.	Notulen werkgroep IBP Notulen TO C&B

4.4. Zijn er toepassingsvoorbeelden waarin de afspraak is gebruikt en zo ja, welke?

antwoord	verwijzing
Rapport KPMG	Notulen werkgroep IBP 31 januari 2017
Verskillende toepassingen door branchegenoten werkgroepleden	Notulen werkgroep IBP 22 november 2017
Leden van de GEU	Notulen Edu-K tactisch overleg continuïteit en beveiliging 20 augustus 2017

5. Hoe ziet de implementatie of toepassing van de afspraak eruit?

5.1. Is er een implementatiehandleiding en/of andere implementatieondersteuning beschikbaar en zo ja, welke?

antwoord	verwijzing
Ja, de hele documentatieset voorziet in alle nodige aspecten van de implementatie. Tevens voorziet Edu-K in een implementatieplan voor het in gebruik nemen van het certificeringsschema an sich.	Edu-K vergaderstuk 2017-08-30 Bijlage 2 Implementatieplan Certificeringsschema

- 5.2. Is er een tool beschikbaar om implementatie van (delen van) de afspraak op correct gebruik te toetsen zo ja, welke? Zo nee, voor welke delen zou dit wel denkbaar zijn? (Graag aanvullen met een korte schets welke technieken daarvoor gebruikt kunnen worden.)

antwoord	verwijzing
Nee. Er is een format voor een rapportage. Deze kan een organisatie zelf gebruiken of door een derde laten uitvoeren om compliance aan te tonen. Deze rapportage kan een klant opvragen en zelf inschatten op waarde.	Certificeringsschema_toezicht.docx

- 5.3. Wat is de globale inschatting voor wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor de implementatie?

antwoord	verwijzing
In de procesbeschrijving staat beschreven welke stappen nodig zijn en wat de bijbehorende inspanning is. Deze is afhankelijk van de hoeveelheid betrokken personen en loopt uiteen van 34 tot 50 uur per ict-toepassing. Wanneer een organisatie meerdere ict-diensten of meermaals dezelfde ict-toepassing toetst wordt deze inspanning naar verwachting bij elk vervolg kleiner.	Certificeringsschema_proces.docx

6. Hoe zijn het beheer en de doorontwikkeling geregeld?

- 6.1. Onder welke samenstelling gaat het beheer vallen? (Bijv. onder een bestaande werkgroep of een nieuw op te richten werkgroep of is er de wens om het beheer bij een werkgroep van Edustandaard te beleggen.)

antwoord	verwijzing
<p>Onderhoud en doorontwikkeling van het certificeringsschema is belegd bij de werkgroep IBP.</p> <p>Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van het certificeringsschema besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep IBP en relevante ketensamenwerkingen zoals Edu-K.</p> <p>De specifieke inhoud van het schema en het toetsingskader worden geëvalueerd door de Edustandaard werkgroep IBP. In eerste instantie wordt uitgegaan van een evaluatiefrequentie van tweemaal per jaar. Hiertoe wordt input verzameld vanuit Edu-K en individuele organisaties die het certificeringsschema gebruiken.</p> <p>Aanpassingen aan het toetsingskader, bijvoorbeeld wegens optreden van nieuwe risico's of bijstelling van de maatregelen, worden direct gepubliceerd. Hiermee wordt een uitzondering gemaakt op het gebruikelijke standaardisatie proces. Jaarlijks wordt de standaard als geheel, dus toetsingskader en de overige onderdelen van het certificeringsschema, opnieuw formeel vastgesteld.</p> <p>Vanwege het bijzondere karakter van het certificeringsschema is tijdens de standaardisatieraad van 10-11-2016 het volgende besproken:</p> <p>Aangepaste werkwijze voor Certificeringsschema, kortcyclisch werken. <i>In de huidige praktijk van Edustandaard gaat er enige tijd overheen voor een voorstel dat in de werkgroep is behandeld, uiteindelijk door de standaardisatieraad is bekrachtigd. Dat is doorgaans geen groot probleem aangezien er afstemming rondom implementatie van de afspraak ook de nodige tijd vraagt.</i></p> <p><i>Voor het certificeringsschema is de situatie iets anders omdat in dit schema een baseline van maatregelen bevat waarmee gangbare informatiebeveiligingsrisico's bestreden kunnen worden. Als er nieuwe dreigingen worden signaleerd willen we daar in het certificeringsschema zo snel mogelijk passende maatregelen opnemen en publiceren. Proces wat we daarbij voorstellen is dat de werkgroep gedurende het jaar nieuwe inzichten verwerkt in het schema. Slechts een keer per jaar zal het schema de gehele standaardisatiekolom doorlopen en door de standaardisatieraad worden bekrachtigd. De, door de werkgroep vastgestelde, tusserversies gelden daarbij vooral als advies aan de keten. Alleen de formeel door de standaardisatieraad vastgestelde versie kan geldt als formele baseline waar partijen ook aan gehouden kunnen worden. Waarbij natuurlijk wel wordt geadviseerd om de laatste inzichten ook over te nemen. Maar een eenmaal doorlopen certificering</i></p>	<p>Certificeringsschema.docx</p> <p>Bijlage 8. Terugtrekking Certificeringsschema v1.1 en aangepaste werkwijze</p>

<p><i>zal zijn geldigheid niet verliezen door de tussentijdse toevoegingen.</i></p> <p>In de praktijk betekent dit dat een organisatie elk jaar de toetsing moet uitvoeren. Ook betekent dit dat ernstige bedreigingen gedurende het jaar nooit dwingend zijn op te lossen. Afnemers zijn zelf verantwoordelijk om de juiste controlevragen te stellen en maatregelen ten aanzien van de meest recente bedreigingen zijn daar een goed voorbeeld van.</p> <p>Een goedgekeurde versie van het certificeringsschema krijgt het jaartal als versienummer. Daaronder hangen specifieke versies van de onderliggende documentatie. Deze documenten worden gedurende het jaar bijgewerkt en het eigen versienummer wordt daarbij opgehoogd. Het certificeringsschema wordt als geheel elk jaar ingediend ter goedkeuring en bij goedkeuring wordt het jaartal als versienummer opgehoogd.</p>	
---	--

6.2. Hoe is de doorontwikkeling geregeld? (Bijv. is er een loket voor het beantwoorden van vragen en indienen van wijzigingen?)

antwoord	verwijzing
<p>Op dit moment zijn de leden van de werkgroep het loket. Zij dienen issues aan voor de roadmap. Bedoeling is om hier op korte termijn ook een mailadres voor open te stellen zodat ook niet-direct-betrokken partijen vragen en issues in kunnen dienen.</p>	<p>Alle documentatie</p>

6.3. Wat is de globale inschatting van wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor het beheer en doorontwikkeling van de afspraak?

antwoord	verwijzing
<p>Vier dagen per jaar, dagdeel voor de werkgroep + voorbereiding aangenomen dat er minder dan vijf tussenversies zijn. De verwachting is dat gedurende 2017 en 2018 meer tussenversies komen waarbij de werkgroep twee tot vier dagen extra besteedt per jaar.</p> <p>Kennisnet besteedt tijd aan procesbegeleiding en expertise vanuit haar gebruikelijke rol.</p>	

7. Hoe ziet de geschiedenis en toekomst van de afspraak eruit?

7.1. Wanneer zijn deze en alle voorgaande versies uitgebracht? Geef kort de belangrijkste verschillen aan tussen de versies.

versie	wijzigingen	verwijzing
1.0	Eerste versie	http://www.sionderwijs.nl/fileadmin/contentelementen/kennisnet/SI_Onderwijs/Certificatieschema_Edukoppeling_en_SA_AS_01.pdf
1.1	<p>Het normenkader is aangepast naar aanleiding van de resultaten uit de risicoanalyse.</p> <p>Het normenkader is uitgebreid met nadere vragen voor de normen en de mapping met ISO 27001:2013 (conform het werk van de CSA)</p>	https://www.edustandaard.nl/standaarden/afspraken/afsprak/certificeringsschema-rosa-1/1.1/

2.0 concept	<p>Overzicht belangrijkste wijzigingen:</p> <ol style="list-style-type: none">1. Scope van het certificeringsschema – de scope is niet meer alleen cloud-gerelateerde dienstverlening, maar ICT-dienstverlening in het algemeen. Dit betekent dat niet alleen leveranciers van cloud oplossingen binnen het onderwijs aan de certificeringsvraag moeten voldoen, maar dat dit geldt voor alle ICT-leveranciers binnen het PO, VO en MBO.2. Aanpassing normenkader – Doordat de scope van de certificering is verbreed, is het cloud-specifieke normenkader verlaten. Het normenkader voor certificering is nu gebaseerd op de wereldwijde en ook in Nederland breed geaccepteerde ISO 27002 standaard. Met dit normenkader is het mogelijk om van alle vormen van ICT-dienstverlening de betrouwbaarheid vast te stellen. De specifieke interpretaties voor cloud-dienstverlening zijn in het normenkader overigens behouden. Het normenkader ISO 27002:2013 is in principe in zijn geheel van toepassing. Tijdens een beoordeling kan de auditor besluiten dat een van de normen niet van toepassing is. In dat geval zal de auditor voor deze control rapporteren dat deze niet van toepassing is en waarom.3. Wijze van certificering – de certificering vindt plaats op basis van een verklaring van het management, waarbij de kwaliteit van de onderlinge maatregelen is vastgesteld aan de hand van een externe audit. Een zelfverklaring is niet langer afdoende.4. Besturingsmodel van certificeringsschema – de taken, rollen en verantwoordelijkheden met betrekking tot het eigenaarschap (Edustandaard), beheer (werkgroep informatiebeveiliging) en toezichhoudende rol (Kennisnet) van het certificeringsschema zijn vastgesteld en geoperationaliseerd.5. Tekst van de verklaring voor de leverancier – de verklaring die de leveranciers dienen te verstrekken is geactualiseerd. <p>Toevoeging van een auditprotocol – als bijlage van het schema is een auditprotocol toegevoegd. Dit protocol moet het mogelijk maken dat de externe audits op een consistente en hoogwaardige manier worden uitgevoerd.</p>	<p>https://www.edustandaard.nl/standaarden/afspraken/afspraken/certificeringsschema-rosa-1/2.0/</p>
2017	<ol style="list-style-type: none">1. Herziening van het toetsingskader: er is gekozen voor een baseline van technische maatregelen op basis van niveaus van beveiligingsaspecten om de praktischer te kunnen toetsen2. Herziening van de hele documentatieset om het proces beter te begeleiden	Alle documentatie

	3. Wijze van toezicht: er is gekozen om het toezicht in eerste instantie vrij te laten, maar er worden wel verschillende toetsvormen gedefinieerd die inzicht geven in de betrouwbaarheid van de toetsing	
2017/2018	Verwerking terugkoppeling en voortschrijdende inzichten	Alle documentatie 20171212_memo_wijzigingen _certificeringsschema

7.2. Wat is de roadmap m.b.t. de doorontwikkeling van de afspraak?

antwoord	verwijzing
De werkgroep hanteert sinds 2017 een nieuwe werkwijze waarbij RFC's worden ingediend en per bijeenkomst worden behandeld en (eventueel) gewijzigd worden goedgekeurd. Er zijn geen verdere grote ontwikkelingen gepland.	

7.3. Wat is de roadmap m.b.t. de implementatie van de afspraak?

antwoord	verwijzing
Nu het certificeringsschema is vastgesteld zal het ook gebruikt gaan worden als onderdeel van het privacy-convenant om passende organisatorische en technische maatregelen aan te tonen. Sommige organisaties gebruiken het al. In mei 2018 wordt de AVG van kracht. Deze wet verplicht dat organisaties "passende en adequate technische en organisatorische maatregelen" aan kunnen tonen. In het TO C&B is voorgesteld om het certificeringsschema daarvoor te gebruiken.	Besluit van Edu-K Tactisch Overleg Continuïteit en Beveiliging

8. Welke copyrights en andere voorwaarden zijn van toepassing op de afspraak?

8.1. Kan het intellectuele eigendom - m.b.t. mogelijk aanwezige patenten - van de afspraak onherroepelijk op een royalty-free basis aan Edustandaard ter beschikking worden gesteld?

antwoord	verwijzing
Er zijn nog geen copyrights of voorwaarden van toepassing op de afspraak. Er is een RFC in behandeling om CC BY 4.0 te gebruiken als copyright.	

8.2. Is het voor een ieder mogelijk om de afspraak (inclusief alle bijbehorende documentatie) te kopiëren, beschikbaar te stellen en te (her)gebruiken om niet?

antwoord	verwijzing
Ja. Bij de afspraak zijn wel bestaande normen ter inspiratie gebruikt, maar er bevinden zich geen teksten of indeling van deze normen in het certificeringsschema zelf.	