edustandaard

# Aanmeldformulier

| | | |
|---|---|---|
| Voor | : | Bureau Edustandaard |
| Van | : | Jordy van den Elshout, namens de Werkgroep IBP |
| Datum | : | 24 mei 2022 |
| Betreft | : | Certificeringsschema informatiebeveiliging en privacy ROSA 2022 |

## Toelichting op de toepassing van dit aanmeldformulier

*Beheer of registratie*
Dit aanmeldformulier wordt gebruikt voor registratie of het in beheer laten nemen van een afspraak[1] 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 aanmeldformulier 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 v3.0 - 2022 | mei 2022 |

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

| titel en/of URL | auteur(s) | versienummer | status |
|---|---|---|---|
| Certificeringschema_Algemene beschrijving | Werkgroep IBP | 3.0 | Definitief |
| Certificeringschema_Proces | Werkgroep IBP | 3.0 | Definitief |
| Certificeringschema_Toetsingskader | Jordy van den Elshout, (namens de) Werkgroep IBP | 3.0 | Definitief |
| Certificeringschema_Toezicht | Werkgroep IBP | 3.0 | Definitief |

**2.** Beschrijf de afspraak:

**2.1.** Waar gaat de afspraak over?

| antwoord | verwijzing |
|---|---|
| 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.<br><br>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).<br><br>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. | 1.Certificeringsschema_algemene_beschrijving.docx<br>2.Certificeringsschema_proces.docx<br>5.Certificeringsschema_toezicht.docx |

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

| antwoord | verwijzing |
|---|---|
| Na de laatst vastgestelde versie in 2018 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. | Geen; signalen zowel per e-mail als mondeling. |

**2.3.** Wat is het doel?

| antwoord | verwijzing |
|---|---|
| Het doel van het Certificeringsschema is:<br>• Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy voor onderwijstoepassingen;<br>• Transparantie bieden over welke ICT-toepassingen voldoen aan deze baseline;<br>• Het creëren van een solide basisniveau van informatiebeveiliging voor alle geleverde ict-toepassingen in de onderwijsketen<br>• En, dit – bovengenoemde – zo gebruiksvriendelijk mogelijk te maken | 1.Certificeringsschema_algemene_beschrijving.docx, paragraaf 1.3 Doel. |

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

| antwoord | verwijzing |
|---|---|
| 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.<br><br>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.<br><br>Nieuwe toetreders op de markt zijn niet bekend met de baseline van beveiligingsmaatregelen waardoor nieuwe innovatieve producten het risico op beveiligingsincidenten mogelijk vergroten.<br><br>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 | |

**2.3.2.** Hoe urgent is de afspraak?

| Antwoord | verwijzing |
|---|---|
| Het is belangrijk om 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. Daarnaast is er een nieuwe versie van Privacy Convenant gepubliceerd, waarin verwezen wordt naar de nieuwe versie van deze afspraak. Het is van belang dat gebruiker van het Privacy Convenant deze goedgekeurde afspraak kunnen gebruiken. | |

**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. Tevens verwachten we op basis van de implementatie feedback en uitbreidingsvoorstellen van organisaties die ict-diensten leveren, onderwijsinstellingen en andere belanghebbenden. | |

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

| antwoord | verwijzing |
|---|---|
| De afspraak is 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 verwerkersovereenkomst gesloten worden, waarbij het certificeringsschema invulling geeft aan de eis om "passende technische en organisatorische maatregelen" te treffen op de ict-toepassing. | |

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

| antwoord | verwijzing |
|---|---|
| Het toepassingsbied is breed. Binnen de 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 daarmee maatregelen voor ict-toepassingen die binnen het onderwijs worden gebruikt. | 1.Certificeringsschema_algemene_beschrijving.docx |

**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.<br><br>**Onderwijsinstellingen**<br>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.<br>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. | ROSA Wiki (wikixl.nl) |

**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 | Basisniveau informatiebeveiliging en privacybescherming - ROSA Wiki (wikixl.nl) |

**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. | N.v.t. |

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

| antwoord | verwijzing |
|---|---|
| De afspraak heeft betrekking op alle gegevenssoorten. In de nieuwe versie zijn de vragen voor classificatie daar ook op aangescherpt, aangezien de eerdere focus (bijzondere) persoonsgegevens en leerresultaten zijn. Maar het gaat ook om andere soorten (gevoelige) gegevenssoorten, zoals examenvragen. | Certificeringschema_Toetsingskader.xlsx, tabblad Stap 2. |

**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 |
|---|---|---|---|
| De nieuwe structuur van de ISO 27002:2022, ter inspiratie voor de maatregelcategorieën | 2022 | 15 februari 2022 | https://www.iso.org/standard/75652.html |
| CIP: Secure Software Development (SSD) Beveiligingseisen voor (web)applicaties, ter inspiratie voor aanscherping maatregelen. | V3.0 | 20 Juli 2020 | https://www.cip-overheid.nl/media/1500/20200720-ssd-normen-v30.pdf |
| ISO 27001 en ISO 27002 zijn gebruikt ter inspiratie voor maatregelen in het toetsingskader | 2013/NL | 1 oktober 2013 | https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema-rosa-1/2.0/ |
| Voorgaande versies maakten gebruik van de “Cloud Control Matrix” van de Cloud Security Alliance. | V3.01 | 11 juli 2014 | https://cloudsecurityalliance.org/artifacts/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 aangeven door de verschillen te benoemen.)

| naam afspraak | raakpunten in overeenkomsten en/of verschillen | verwijzing |
|---|---|---|
| Toetsingskader informatiebeveiliging MBO | Sinds 2021 maakt MBO gebruik van het NBA Volwassenheidsmodel Informatiebeveiliging, kortweg het NBA-model. Dit model geeft richting aan de invulling van IB d.m.v. volwassenheidsniveau. Het Certificeringschema sluit daarop aan; het geeft nadere invulling van de beveiliging van toepassingen op basis van het BIV-niveau. | Netwerk IBP krijgt nieuw toetsingskader informatiebeveiliging - MBO Digitaal |
| HO normenkader | Idem als normenkader MBO; HO maakt ook gebruik van het NBA-Model. | Normenkader SURFaudit: audit je informatiebeveiliging \| SURF.nl |

**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 Standaard Edukoppeling. 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 |

**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:<br>Kennisnet (Dirk Linden, Jordy van den Elshout)<br>Surf (Bart Bosma)<br>MBO (Martijn Bijleveld)<br>OdinGroep (Jeroen Renard)<br>DUO (Erik Kwast)<br>GEU/MEVW (Paul Gilijns)<br>- Malmberg (Ellen de Kok, Ilja Kösters)<br>- BeatsnBits (Robin van Rootseler)<br>OCW (Oscar te Meer)<br><br>Daarnaast is er afstemming geweest met de werkgroep van het Privacyconvenant, welke breed is vertegenwoordigd.<br><br>Tevens regelmatig besproken en feedback opgehaald bij een Klankbordgroep Certificeringschema, waarin meerdere IBP-ers van schoolbesturen zijn vertegenwoordigd en georganiseerd is door de PO/VO-raad. | Webpagina van de Werkgroep: Informatiebeveiliging en privacy (IBP) - Edustandaard |

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

| antwoord | verwijzing |
|---|---|
| In het nieuwsbericht van het nieuwe Privacy Convenant, is ook verwezen naar de meest recente versie (3.0) van het Toetsingskader; om deze te gebruiken bij het herzien van de verwerkersovereenkomsten.<br><br>Op de website van Edustandaard worden de vastgestelde en meest recente documenten van de (concept) afspraak gepubliceerd. | Nieuws — Privacyconvenant onderwijs |

**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 van de voorgaande versie, in Edustandaard werkgroep informatiebeveiliging en Edu-K tactisch overleg continuïteit en beveiliging. De nieuwe versie 2022 is qua inhoud en vorm herzien, waarvan geen openbare notulen is gepubliceerd. Wijzigingen zijn – indien gewenst – wel inzichtelijk. | |

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

| antwoord | verwijzing |
|---|---|
| Nieuwsbericht: Nieuwe versie privacyconvenant en certificeringsschema klaar voor gebruik April 2022 | Nieuws — Privacyconvenant onderwijs |
| | |

**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. | Alle documenten |

**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 |
|---|---|
| Ja, het Excelbestand Certificeringschema_Toezicht.xsls is een tool waarmee de<br>a) De BIV-niveau bepaald kan worden op basis van beantwoorden van vragen<br>b) De maatregelen gepresenteerd worden op basis van BIV en ruimte is opgenomen om testresultaten bij te houden<br>c) Rapportagevorm automatisch wordt opgemaakt, om te gebruiken voor verantwoording.<br><br>Voor implementatie van de maatregelen wordt waar mogelijk en beschikbaar, gerefereerd aan hulpinformatie. | 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 40 tot 60 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 |
|---|---|
| Onderhoud en doorontwikkeling van het certificeringsschema is belegd bij de werkgroep IBP.<br>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.<br><br>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 eenmaal per jaar. Hiertoe wordt | Certificeringsschema.docx |

| | |
|---|---|
| input verzameld vanuit Edu-K en individuele organisaties die het certificeringsschema gebruiken. | |

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

| antwoord | verwijzing |
|---|---|
| Vragen en verbeteringen kunnen gestuurd worden naar info@edustandaard.nl. Deze worden dan in behandeling genomen en indien nodig, een item op de lijst met verbetering opgenomen. | |

**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 |
|---|---|
| | |

**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 | |
| 1.1 | Het normenkader is aangepast naar aanleiding van de resultaten uit de risicoanalyse.<br>Het normenkader is uitgebreid met nadere vragen voor de normen en de mapping met ISO 27001:2013 (conform het werk van de CSA) | Certificeringsschema informatiebeveiliging en privacy ROSA - Certificeringsschema informatiebeveiliging en privacy ROSA 1.1 - 2015 - Edustandaard - Edustandaard |
| 2.0 | Overzicht belangrijkste wijzigingen:<br>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.<br>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 | Certificeringsschema informatiebeveiliging en privacy ROSA - Certificeringsschema informatiebeveiliging en privacy ROSA 2017 - Edustandaard - Edustandaard |

| | | |
|---|---|---|
| | is. In dat geval zal de auditor voor deze control rapporteren dat deze niet van toepassing is en waarom.<br>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.<br>4. Besturingsmodel van certificeringsschema – de taken, rollen en verantwoordelijkheden met betrekking tot het eigenaarschap (Edustandaard), beheer (werkgroep informatiebeveiliging) en toezichthoudende rol (Kennisnet) van het certificeringsschema zijn vastgesteld en geoperationaliseerd.<br>5. Tekst van de verklaring voor de leverancier – de verklaring die de leveranciers dienen te verstrekken is geactualiseerd.<br>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. | |
| 2017 | 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 toetsen<br>2. Herziening van de hele documentatieset om het proces beter te begeleiden | |
| 2017/2018 | Verwerking terugkoppeling en voortschrijdende inzichten | Alle documentatie<br>20171212_memo_wijzigingen_certificeringsschema |
| 2022 | Het Toetsingskader is grondig herzien en functioneel uitgebreid. Qua vorm zijn de vragen voor classificatie nu onderdeel van het Toetsingskader, zodat op basis daarvan direct de juiste maatregelen worden getoond. Ook wordt de rapportagevorm automatisch opgemaakt. Qua inhoud zijn de vragen en maatregelen verduidelijkt. De maatregelen zijn in sommige gevallen ook aangescherpt. Onder andere om a) aan te sluiten bij de huidige stand van techniek en het huidige dreigingsbeeld, zoals voor de back-upinrichting en minimaal 2FA voor beheertoegang; en b) om preciezer te zijn in verantwoordelijkheden van de leverancier (de verwerker). Op basis hiervan zijn de begeleidende teksten zoals de ‘Algemene beschrijving’, ‘Proces’ en ‘Toezicht’ bijgewerkt. | Toetsingskader versie 3.0 |

**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 |
|---|---|
| De afspraak wordt reeds breed gebruikt binnen de leermiddelenketen, middels het privacy convenant. Ook wordt het door de schoolbesturen gebruikt ter toetsing van onderwijs toepassen, echter is niet bekend hoe breed.<br><br>Wel is tijdens de architectuurraad besproken of de standaard breder gebruikt moet worden binnen de onderwijssector, wat ook een bespreekpunt is voor de standaardisatieraad. Met name om toetsing ervan te kunnen bevorderen. | |

**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. | |