edustandaard

Advies van bureau Edustandaard

Voor	Architectuurraad, Edustandaard
Van	Marcia van Oploo (Standaardisatie Expert)
Datum	27 juni 2017
Betreft	Advies van bureau Edustandaard voor in beheername van de afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v.2017 (afgekort Certificeringsschema v.2017)

Toelichting op het advies van bureau Edustandaard

*Dit onderdeel wordt **eerst** ingevuld door bureau Edustandaard.*

Bij de beoordeling van een ingediende standaard weegt het bureau Edustandaard een aantal kwaliteitsaspecten. De kwaliteitsaspecten vallen uiteen in vier categorieën:

- **Probleemgericht**: In hoeverre draagt de standaard bij aan een specifiek probleem en sluit deze aan bij de doelstellingen van de beheerorganisatie.
- **Implementeerbaar**: In hoeverre kan de standaard eenvoudig en correct geïmplementeerd worden.
- **Beheerbaar**: In hoeverre is de standaard efficiënt te beheren.
- **Beschikbaar**: In hoeverre is de standaard eenvoudig verkrijgbaar en bruikbaar.

Per aspect is een aantal criteria vastgelegd die verschillend worden gewogen. Er zijn drie wegingsfactoren:

- **Must**: Het belang van een criterium met importantie-oordeel *must* is extreem hoog, zodanig dat er nagenoeg geen redenen kunnen zijn om niet aan dit criterium te voldoen.
- **Should**: Het belang van het criterium met importantie-oordeel *should* is hoog. Ook al is het oordeel minder zwaar dan het oordeel *must*, toch wordt er veel waarde gehecht om te voldoen aan dit criterium. Echter mocht dit door omstandigheden niet gerealiseerd zijn, dan is dat niet per definitie een "disqualifier".
- **Could**: Het belang van een criterium met importantie-oordeel *could* is in feite een wens. Het is een advies dat past bij goede afspraken. Het is daarom wenselijk om dit advies ter harte te nemen en waar mogelijk op te volgen.

De beoordeling

1. Probleemgericht

1.1. MUST: Context: De afspraak moet een duidelijke contextbeschrijving bevatten evenals een omgevingsanalyse waarin referenties naar standaarden geplaatst worden. De afspraak moet daarbij aansluiten op de scope van Edustandaard: onderwijs- en onderzoektechnologische standaarden gericht op ict-gebruik in het Nederlandse onderwijs en onderzoek.

Gerelateerde vragen	2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11
Bureau Edustandaard	Het Certificeringsschema v.2017 betreft maatregelen voor ict-toepassingen die als (onderdeel van) een dienst worden aangeboden door organisaties binnen de onderwijssector. De afspraak is breed toepasbaar in alle sectoren van het onderwijs (po, vo, mbo en ho). De afspraak valt onder de katern informatiebeveiliging en privacy van ROSA en heeft samenhang met Privacyconvenant, normenkaders in het hoger onderwijs en normenkader informatiebeveiliging MBO. Het certificeringsschema is geïnspireerd op ISO27001 en ISO 27002. OORDEEL: VOLDOET
Reactie van indiener	

1.2. MUST: Oplossing: De afspraak moet een duidelijk omschreven doel hebben en daarbij een specifiek uitwisselingsprobleem oplossen waarvoor stakeholders benoemd zijn.

Gerelateerde vragen	2.5
Bureau Edustandaard	Het doel van het Certificeringsschema v.2017 is het specificeren van een baseline van maatregelen waaraan geleverde ict-diensten in de onderwijsketen moeten voldoen (1), het transparant maken van organisaties die hieraan voldoen (2) en zodoende een solide basisniveau van informatiebeveiliging en privacy binnen de onderwijsketen te bieden (3). Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy. OORDEEL: VOLDOET
Reactie van indiener	

1.3. MUST: Realistisch: De afspraak is ten minste in één relevante praktijksituatie succesvol toegepast.

Gerelateerde vragen	3.4
Bureau Edustandaard	Het Certificeringsschema v.2017 is in pilot-vorm getoetst en daarnaast door verschillende partijen beproefd. Feedback is meegenomen in de laatste versie van het schema. OORDEEL: VOLDOET
Reactie van indiener	

1.4. SHOULD: Flexibiliteit: De afspraak moet slechts die flexibiliteit bieden die noodzakelijk is voor het uitwisselingsproces. Vrije uitbreidingsmogelijkheden kunnen de interoperabiliteit schaden.

Gerelateerde vragen	Het Certificeringsschema v.2017 kent een vrijheidsgraad in de toetsvorm: een self-assessment, interne audit, een peer review of een externe audit. De gekozen toetsvorm is van invloed op de onafhankelijkheid van de rapportage. In de auditverklaring wordt expliciet welke vorm is gekozen, de weging hiervan is aan de afnemende onderwijsinstelling. Bij twijfel kan extra informatie worden opgevraagd. Verder bevat het Certificeringsschema v.2017 nu technische maatregelen. Informatiebeveiliging wordt geborgd door een combinatie van techniek, proces en mens. Deze laatste twee zijn voorzien in de roadmap.
Bureau Edustandaard	OORDEEL: VOLDOET / VOORZIEN IN DE ROADMAP
Reactie van indiener	

1.5. SHOULD: Acceptatie: Er moet draagvlak zijn voor de afspraak, wat betekent dat potentiële gebruikers de afspraak realistisch en bruikbaar moeten vinden en ondersteunen (draagvlak).

Gerelateerde vragen	3.1, 3.2, 3.3
Bureau Edustandaard	Van alle werkgroepleden is een expliciete goedkeuring ontvangen. Dit betreft van bijna alle leden een schriftelijke goedkeuring op de versie die in maart 2017 is voorgelegd. Op 27 juni is de versie die is gewijzigd naar aanleiding van commentaar door Edustandaard aan de werkgroep voorgelegd, hiermee hebben alle leden mondeling ingestemd. OORDEEL: VOLDOET
Reactie van indiener	

2. Implementeerbaar

2.1. MUST: Begrijpelijk, Eenduidig, Scoping: De afspraak moet eenduidig en compleet zijn, in voldoende detail uitgewerkt, de reikwijdte afdekken met betrekking tot het te bereiken doel en duidelijk omschreven zijn. Aan de hand van de documenten rond de afspraak moet het eenvoudig zijn om een implementatie uit te voeren die interoperabel is met andere implementaties. De afspraak mag maar op één manier (eenduidig) te interpreteren zijn. De afspraak mag dus geen onduidelijke, vage beschrijvingen bevatten, maar dient juist structuur en duidelijke beschrijvingen te bevatten, toegelicht met voorbeelden. Daarnaast moet de mate van detail aansluiten bij de scope van de afspraak.

Gerelateerde vragen	4.1, 4.2, 4.3
Bureau Edustandaard	Het Certificeringsschema v.2017 bestaat uit een pakket van documenten, waarin naast een algemene beschrijving ook een proces- en toetsbeschrijving zijn opgenomen. Naast het Certificeringsschema v.2017 zelf is ook een tool opgenomen waarmee de classificatie van een ict-toepassing is te bepalen. Alle documenten zijn gedetailleerd en zorgvuldig uitgewerkt. OORDEEL: VOLDOET
Reactie van indiener	

2.2. MUST: Techniek: De afspraak is beschikbaar via marktconforme technieken en technieken die aansluiten bij de doelgroep, zoals XML. De technische uitdrukking (binding) voegt geen informatie toe die niet in modellen en beschrijvingen van de afspraak staan. De technische uitdrukking is gerealiseerd

op basis van de modellen en beschrijvingen van de afspraak en is daarmee een 1-op-1- afspiegeling van deze modellen en beschrijvingen.

Gerelateerde vragen	2.11
Bureau Edustandaard	Het Certificeringsschema v.2017 bestaat uit documenten in Word en Excel. Mogelijk komt de classificatietool op termijn beschikbaar als webformulier als het schema verder is doorontwikkeld. Dit zijn allemaal toegankelijke formats. Een technische beschrijving is voor het Certificeringsschema v.2017 niet van toepassing. OORDEEL: VOLDOET
Reactie van indiener	

2.3. SHOULD: Afhankelijk: Afhankelijkheid met andere standaarden is mogelijk, maar dient doordacht te zijn. Dit kan van invloed zijn op bijvoorbeeld de reikwijdte van de afspraak. Relaties met andere standaarden en mogelijke invloed daarvan op de reikwijdte van de afspraak, dienen op zijn minst omschreven te zijn. Daarbij geldt de basisregel dat bestaande open standaarden zoveel mogelijk worden hergebruikt, maar dat er wel kritisch naar de kwaliteit van die standaarden wordt gekeken.

Gerelateerde vragen	2.11
Bureau Edustandaard	Het Certificeringsschema v.2017 kent geen afhankelijkheid van andere standaarden. Het is geïnspireerd op ISO 27002 en ISO 27002, maar er is geen een-op-een relatie hiertussen. Verder komen de beveiligingsniveaus overeen met het Normenkader informatiebeveiliging MBO, maar deze kent niet de concrete technische maatregelen en niveaus uit het Certificeringsschema v.2017. OORDEEL: VOLDOET
Reactie van indiener	

2.4. SHOULD: Begrijpelijk, Eenduidig, Scoping: De afspraak moet bij voorkeur een informatiemodel bevatten ten behoeve van de begrijpelijkheid, de eenduidigheid en scoping.

Gerelateerde vragen	2.8
Bureau Edustandaard	Het Certificeringsschema v.2017 heeft betrekking op alle informatie-objecten die in systemen van ict-leveranciers worden bewerkt. Deze informatie-objecten vallen onder de scope van het Certificeringsschema v.2017, maar maken er geen deel vanuit. Een informatiemodel is daarom niet aan de orde. Het onderdeel ter audit betreft ‘ict-toepassing’, waarvan in het Certificeringsschema v.2017 geen expliciete definitie is opgenomen. Dit zou de scoping en de eenduidigheid van de afspraak sterk ten goede komen. OORDEEL: VOLDOET
Reactie van indiener	

2.5. COULD: Begrijpelijk, Eenduidig: De afspraak heeft indien mogelijk een binding ten behoeve van de begrijpelijkheid en de eenduidigheid.

Gerelateerde vragen	
Bureau Edustandaard	Het Certificeringsschema v.2017 kent geen informatiemodel (zie vraag 2.4), een binding is daarom ook niet aan de orde. OORDEEL: VOLDOET
Reactie van indiener	

2.6. COULD: Eenduidig: De afspraak heeft indien mogelijk een (XSD) schema ten behoeve van de eenduidigheid.

Gerelateerde vragen	1.2
Bureau Edustandaard	Het Certificeringsschema v.2017 bestaat uit begeleidende documenten waarin de principes en werkwijzen uitgebreid zijn toegelicht. Gezien de scope van het Certificeringsschema v.2017 is een XSD-schema niet aan de orde. OORDEEL: VOLDOET
Reactie van indiener	

3. Beheerbaar

3.1. MUST: Beheerd: Het beheer wordt zonder voorbehoud overgedragen aan EduStandaard.

Gerelateerde vragen	5.1
Bureau Edustandaard	Onderhoud en doorontwikkeling van het Certificeringsschema v.2017 is belegd bij de ES werkgroep IBP. Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van het Certificeringsschema v.2017 besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de ES werkgroep IBP en relevante ketensamenwerkingen zoals Edu-K. OORDEEL: VOLDOET
Reactie van indiener	

3.2. MUST: Beheerprocedure: Wijzigingen worden doorgevoerd op basis van de wijzigingsprocedure van EduStandaard.

Gerelateerde vragen	5.2
Bureau Edustandaard	De leden van de ES werkgroep IBP zijn momenteel het loket en dienen issues aan voor de roadmap. Op korte termijn komt een mailadres beschikbaar waar niet-direct-betrokken partijen vragen en issues kunnen indienen. OORDEEL: VOLDOET
Reactie van indiener	

3.3. SHOULD: Wijzigingen: De afspraak moet voldoende stabiel zijn. Bij voorkeur wordt het aantal versies beperkt tot dat wat noodzakelijk is. Wijzigingen op de afspraak die niet door EduStandaard zijn uitgevoerd worden beschouwd als een nieuwe afspraak.

Gerelateerde vragen	5.2, 5.3, 6.2, 6.3
Bureau Edustandaard	Om adequaat te kunnen inspringen op nieuwe dreigingen is tijdens de Standaardisatieraad van 10 november 2016 besproken om kortcyclisch te werken. De werkgroep verwerkt gedurende het jaar nieuwe inzichten in het schema. Slechts eenmaal per jaar doorloopt het schema de gehele standaardisatiekolom en vindt bekrachtiging door de Standaardisatieraad plaats. De status van de tussenversies is adviserend, alleen de formeel vastgestelde versie door Edustandaard geldt als baseline waar partijen aan gehouden kunnen worden. OORDEEL: ONDERBOUWDE AFWIJKING
Reactie van indiener	

3.4. SHOULD: Versiebeheer: Een historisch overzicht van versies in het verleden en daarnaast een roadmap van geplande versies in de toekomst is gewenst.

Gerelateerde vragen	6.1, 6.2
Bureau Edustandaard	Het aanmeldformulier bevat een uitgebreid overzicht van alle voorgaande versies en de wijzigingen die zijn doorgevoerd. Het Certificeringsschema v.2017 beschikt over een roadmap met daarin een overzicht van geagendeerde issues. OORDEEL: VOLDOET
Reactie van indiener	

3.5. COULD: Efficiënt en effectief beheerbaar: Het is wenselijk dat het beheer van een afspraak efficiënt kan worden vormgegeven; hiervoor is een modelgebaseerde opzet van een afspraak essentieel. Een goede afspraak heeft in principe weinig versies nodig. Anderzijds is het essentieel dat er nieuwe versies kunnen komen indien noodzakelijk. Net zoals voor “minimale flexibiliteit” (zie probleemgericht) geldt ook hier een zo beperkt mogelijke hoeveelheid versies.

Gerelateerde vragen	5.1, 5.2, 5.3, 6.1, 6.2, 6.3
Bureau Edustandaard	Vanwege het bijzondere karakter van het Certificeringsschema v.2017 is besloten en bekrachtigd om kortcyclisch te werken, waarbij met tussentijdse versies is in te springen op nieuwe dreigingen. Om het voor alle partijen efficiënt en effectief beheerbaar te houden wordt niet vaker dan eenmaal per jaar het standaardisatieproces te doorlopen (zie ook vraag 3.3). Het is raadzaam een heldere versionering toe te passen, zodat een ieder van het versienummer de status kan aflezen. Edustandaard adviseert daarom omwille van de duidelijkheid om alle versienummers eens per jaar gelijk te trekken, en tussenversies achter de punt te updaten[1] OORDEEL: ONDERBOUWDE AFWIJKING
Reactie van indiener	

4. Beschikbaar

4.1. MUST: Publicatie: Het eigendom wordt zonder voorbehoud overgedragen aan EduStandaard. Hierdoor kan de afspraak vrij worden verkregen en gekopieerd.

Gerelateerde vragen	7.2
Bureau Edustandaard	Het Certificeringsschema v.2017 is vrij beschikbaar. Bij de afspraak zijn bestaande normen ter inspiratie gebruikt, maar hiervan zijn geen teksten of indelingen in het Certificeringsschema v.2017 overgenomen. OORDEEL: VOLDOET
Reactie van indiener	

[1] Dat zou bijvoorbeeld betekenen dat voor de versie van 2017 alle onderliggende documenten nummer 3.0 krijgen, en gedurende het jaar versies 3.1, 3.2 enz verschijnen. Per volgende gestandaardiseerde versie van 2018 kunnen alle documenten dan een upgrade naar 4.0 krijgen. Uiteraard is ook een andere nummering mogelijk, bv 17.0 voor de documenten van 2017.

4.2. MUST: Eigendom: Het intellectuele eigendom - m.b.t. mogelijk aanwezige patenten - van (delen van) de afspraak is onherroepelijk ter beschikking gesteld op een royalty-free basis.

Gerelateerde vragen	7.1
Bureau Edustandaard	Op het Certificeringsschema v.2017 zijn geen copyright of voorwaarden van toepassing. OORDEEL: VOLDOET
Reactie van indiener	

4.3. SHOULD: Vindbaar: De afspraak moet vindbaar zijn en bekend zijn bij de doelgroep.

Gerelateerde vragen	1.2, 3.1, 3.2, 3.3
Bureau Edustandaard	Bij de ontwikkeling van het Certificeringsschema v.2017 zijn de verschillende stakeholders ruim vertegenwoordigd. Publicatie van het Certificeringsschema v.2017 op de website van Edustandaard heeft plaatsgevonden, waardoor het voor niet-direct-betrokken partijen vindbaar is. OORDEEL: VOLDOET
Reactie van indiener	

Het advies

Aan de hand van deze criteria kan men een gefundeerd beeld krijgen van de kwaliteit van de afspraak. Uiteraard wordt hierin het onderscheid in importantie-oordeel (MUST, SHOULD, COULD) meegenomen. De criteria worden ieder voor zich in ogenschouw genomen, waarna een oordeel wordt gevormd op de set van criteria binnen een hoofdcategorie.

Aangezien elke afspraak uniek is en elke standaardisatieomgeving uniek is, dienen experts deze beoordeling in te vullen met gevoel voor context en pragmatiek.

Het advies kent de volgende variaties:

1. **Goed**: Betekent een ruime voldoende. Een goede uitgangsituatie voor een onderwijsafspraak.
2. **Voldoende, met aandachtspunten**: Betekent dat de beoordeelde situatie als voldoende wordt ervaren, maar dat de situatie nog verbeterd kan worden door een aantal aandachtspunten op te pakken.
3. **Voldoende, mits de volgende punten aangepakt worden**: Betekent dat de situatie bijna voldoende is, maar dat er nog een paar pijnpunten zijn die veranderd moeten worden, wil de situatie echt voldoende zijn. Echter de pijnpunten zijn dusdanig beperkt van aard dat, indien de indiener bereid is deze pijnpunten op te lossen, het oordeel een voldoende status krijgt.
4. **Onvoldoende, kijk vooral naar de volgende punten**: Betekent een onvoldoende beoordeling doordat de pijnpunten te belangrijk zijn. Dit is een verschil met het oordeel "voldoende, mits", doordat de pijnpunten in dit geval zwaarder wegen of dat het totaal aan pijnpunten groter is.
5. **Onvoldoende**: Een onvoldoende betekent dat er meerdere zwaarwegende punten zijn waardoor deze afspraak als kwalitatief onvoldoende wordt bestempeld. Aangezien de situatie te ver afwijkt van de gewenste situatie wordt geen analyse opgesteld rond de pijnpunten.

Totaaloordeel standaard:

Advies[2]	Voldoende, met aandachtspunten
Adviseur(s)	Marcia van Oploo (Standaardisatie Expert)

Overige constateringen:
(Beschrijving van andere opmerkelijke zaken die tijdens de analyse naar voren kwamen).

Onderbouwing advies:
(Een onderbouwing van het advies; de aandachtspunten dienen hier nauwkeurig omschreven te worden).

Het Certificeringsschema v.2017 informatiebeveiliging en privacy ROSA v.2017 (CS v.2017) is een afspraak die een gedetailleerde uitwerking kent. De begeleidende documenten schetsen de context en het beheerproces van de afspraak, waarbij de focus op structurele feedback op de afspraak positief opvalt. De classificatietool is bedoeld als een praktisch hulpmiddel waarmee leveranciers hun audit kunnen (laten) uitvoeren, en onderwijsinstellingen desgewenst transparantie biedt. De vorm (Excel-formulier) kan professioneler, maar voldoet voor de fase waarin het Certificeringsschema v.2017 zich bevindt. Het toetsingskader is met zorg tot stand gekomen en met consultatie van een brede groep stakeholders. Al met al beoordelen wij de afspraak als voldoende, met aandachtspunten.
Om adequaat in te kunnen springen op nieuwe dreigingen is gekozen om de doorontwikkeling van het Certificeringsschema v.2017 kortcyclisch te laten plaatsvinden. Tussentijdse versies bieden advies over de laatste informatiebeveiliging en privacy-inzichten, de eenmaal per jaar formeel vastgestelde versie door Edustandaard geldt als baseline waar partijen aan gehouden kunnen worden[3]. Deze werkwijze wijkt af van de standaard processen van Edustandaard, maar is gezien het afwijkende karakter van het Certificeringsschema v.2017 te verdedigen. Het aandachtspunt hierbij is wel om in praktijk te ervaren hoe het kortcyclisch werken voldoet voor alle partijen. Is voor leveranciers helder waar zij aan moeten voldoen, en voor onderwijsinstellingen waarop zij kunnen toetsen? En wat is de status van de tussentijdse versies in de praktijk, worden ze überhaupt opgepakt of worden ze misschien zelfs leidend? De antwoorden hierop kunnen aanleiding geven om het standaardisatieproces anders in te steken. Om deze reden stellen wij voor in de roadmap van het Certificeringsschema v.2017 een evaluatie op te nemen om de kortcyclisch werkwijze na het eerste jaar te toetsen en de werkwijze indien nodig aan de bevindingen aan te passen.

[2] De volgende classificatie gebruiken: 1. Goed; 2. Voldoende, met aandachtspunten; 3. Voldoende, mits de volgende punten aangepakt worden; 4. Onvoldoende, kijk vooral naar de volgende punten; 5. Onvoldoende
[3] Edustandaard adviseert omwille van de duidelijkheid alle versienummers van de onderliggende documenten eens per jaar gelijk te trekken, en tussenversies achter de punt te updaten. Voor Certificeringsschema 2017 zou dit voorr alle documenten bv 17.0 kunnen zijn, met tussendocumenten 17.1, 17.2 enz.