Advies van bureau Edustandaard

Voor	Standaardisatieraad, Edustandaard
Van	Elise Listenhouwer (Standaardisatie Expert)
Datum	15 februari 2018
Betreft	Advies van bureau Edustandaard over de update van de afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v.2018 (afgekort Certificeringsschema v.2018)

Toelichting op het advies van bureau Edustandaard

Het betreft een update van de afspraak en de focus ligt daarbij op de wijzigingen ten opzichte van de vorige versie, de adviezen van de beoordeling door bureau Edustandaard en de adviezen uit de architectuurscan.

De beoordeling

De wijzigingen ten opzichte van versie 2017
In de memo van Dirk Linden (20171212_Memo_wijzigingen_certificeringsschema.docx) staan de wijzigingen opgesomd. Hieruit komt naar voren dat er kleine wijzigingen zijn doorgevoerd om de afspraak actueel en beter toepasbaar te maken. In de werkgroep is een goede afspiegeling van de gebruikersgroep aanwezig waardoor aan te nemen is dat deze wijzigingen, net als de afspraak v.2017. breed geaccepteerd zijn.

De adviezen van de beoordeling door bureau Edustandaard
Namens bureau Edustandaard heeft Marcia van Oploo de beoordeling voor in beheer name uitgevoerd (Advies van bureau Edustandaard CS v.2017 dev.docx). In deze beoordeling zijn twee adviezen gegeven.

1. Voor het certificeringsschema is voor een andere vorm van doorontwikkeling gekozen: kortcyclisch. Dit houdt in dat er na elke werkgroepbijeenkomst (4 keer per jaar) een tussentijdse versie worden gepubliceerd naast de (jaarlijks) vastgestelde versie. Geadviseerd is om deze na een jaar te evalueren.

Er is geen officiële evaluatie gehouden, maar zowel de leden van de werkgroep als de leden van het tactisch overleg continuïteit en beveiliging vinden de huidige werkwijze prettig. Er is dus geen aanleiding om aan te nemen dat ze het anders in willen steken. Met betrekking tot versiegebruik en duidelijkheid zijn er wel verzoeken en antwoorden/oplossingen gekomen om het versiegebruik helder te houden. Tot nu toe lijken die te voldoen, want er zijn geen vragen/opmerkingen over versies en onduidelijkheid daarover.

2. Informatiebeveiliging wordt geborgd door een combinatie van techniek, proces en mens. Het Certificeringsschema bevat de technische maatregelen, het proces en de mens staan op de roadmap van v.2017. Geadviseerd is om het proces en de mens volgens roadmap uit te werken.

Omwille van de adoptie is er gekozen om in eerste instantie de technische maatregelen te 'doorontwikkelen' en te toetsen in de praktijk. Mens en proces zijn interessant vanuit informatiebeveiliging en privacy, maar de scope van het certificeringsschema is in eerste instantie beperkt. Wanneer het certificeringsschema in de huidige vorm

breed geaccepteerd en gebruikt wordt, kan er gekeken worden naar deze uitbreiding (in overleg met de ketenpartijen).

De adviezen van de architectuurscan voor het product
Voor het Certificeringsschema v.2017 is een architectuurscan uitgevoerd door Remco de Boer. In deze scan zijn een aantal adviezen gericht op het product gegeven.

1. Definieer het begrip “ict-toepassing”.

In §1.1 van “1. Certificeringsschema_algemene_beschrijving.docx” staat “Op verschillende manieren wordt gebruik gemaakt van ict-toepassingen voor onderwijskundige of onderwijsondersteunende producten en diensten. De aard en inhoud van deze ict-toepassingen kunnen onderling sterk verschillen, maar zij hebben als gemeenschappelijk kenmerk dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensbewerking cruciaal is.”

2. Beargumenteer waarom de BIV-definities en -classificaties in het certificeringsschema afwijken van die in het ROSA-katern IBP. Deze rationale kan mogelijk leiden tot aanpassing van het katern IBP. Het uitgangspunt zou moeten zijn in ieder geval gelijke definities en classificaties te hanteren.

De classificaties in het CS zijn aangepast naar laag, midden, hoog conform ROSA. De BIV-definities zijn afgeleid van de definities van NOREA.

3. Maak duidelijk hoe de maatregelen in het Certificeringsschema zich verhouden tot de doelen uit ISO 2700X, zoals die zijn beschreven in het ROSA-katern IBP.

In §2.2 van “1. Certificeringsschema_algemene_beschrijving” wordt deze verhouding uitgebreid beschreven.

4. Voeg maatregelen of richtlijnen toe aan het CS die aangeven dat gemonitord wordt in hoeverre aan de te nemen maatregelen wordt voldaan (en hoe dan) Bijvoorbeeld: hoe toon je aan (ook aan je ketenpartners) dat de gewenste RTO (recovery time objective) etc. daadwerkelijk is behaald.

In het document “5. Certificeringsschema_toezicht.docx” worden verschillende manieren beschreven hoe het toezicht eruit kan zien. Het is aan de organisaties zelf om dit te toetsen, bijvoorbeeld een school die een leverancier van een ICT-toepassing hierover bevraagt. Het CS faciliteert hierin door categorieën te beschrijven die ketenbreed gelden waardoor eenvoudiger te toetsen is of een organisatie voldoet.

5. Overweeg maatregelen toe te voegen mbt incident response (detectie + opvolging). Overweeg maatregelen te koppelen aan fasen in PDRC-cyclus. Definieer communicatielijnen en proces bij (acute) dreigingen en gewijzigde dreigingsbeelden die nopen tot nieuwe/aanvullende maatregelen.

Het CS is een baseline *voor beveiligingsmaatregelen en deze beperken zich niet tot wat er in het CS staat. (Actute) dreigingen vereisen sneller ingrijpen dan waar een standaard toe in staat is. Maatregelen kunnen uiteindelijk toegevoegd worden aan de CS, maar de CS zal nooit leidend kunnen zijn wanneer nieuwe (actute) dreigingen zich aandoen. De continuïteit en stabiliteit van een standaard en de doorlooptijd van de implementatie passen hier ook niet bij.*

6. Overweeg - mede vanwege het belang van het kader “Voorkom ongewenste traceerbaarheid en vindbaarheid” voor (minderjarige) onderwijsvolgers - maatregelen (ook) expliciet in het toetsingskader op te nemen, wellicht in een aparte kolom. Zie bijvoorbeeld ook de (aanvullende) ‘maatregelen om vermenging van gegevens te voorkomen’ die op de auditverklaring staan.

Het CS bevat sinds de eerste indiening al een palet aan maatregelen die bijdragen aan het voorkomen van de ongewenste traceerbaarheid en vindbaarheid voor minderjarige onderwijsvolgers. Een deel van die maatregelen valt onder vertrouwelijkheid onder verschillende kolommen. De beperking van productieomgeving tot alleen productieomgevingen en het goed inrichten van logische, fysieke en netwerktoegang zijn voorbeelden van waar deze maatregelen zijn te vinden. Aanvullend: het CS is een baseline/minimum aan maatregelen. Het ontslaat niet een leverancier van de verplichting of verantwoordelijkheid om daar waar nodig aanvullende maatregelen te treffen.

7. Werk het bedoelde 'eigenaarschap' uit in termen van de relevante zeggenschap(pen): welke zeggenschappen maken dat partijen die die zeggenschap hebben, betrokken dienen te worden bij de uitvoering van het in het certificeringsschema beschreven proces?

In het document "2. Certificeringsschema_proces.docx" waar 'eigenaar van de data' wordt genoemd, staat deze gedefinieerd als "dit is vaak een proceseigenaar en vaak iemand uit de 'business'. Deze heeft een groot belang bij de bewerkte data." Het gaat hier niet om de zeggenschappen over de data zoals beschreven in ROSA, maar om een rol in het certificeringsproces naast de eigenaar van de ict-toepassing, inhoudelijk specialisten en een procesbegeleider.

8. Edukoppeling maakt gebruik van het certificeringsschema, en heeft als werkingsgebied het hele onderwijsdomein. Het ho maakt gebruik van een ander normenkader. Hoe verhoudt het certificeringsschema zich tot het ho normenkader? (Kan worden opgenomen in paragraaf 1.5 Algemene beschrijving)

In §2.2 van "1. Certificeringsschema_algemene_beschrijving" wordt de verhouding tot ISO 27001 uitgebreid beschreven. Het normenkader voor het ho is een andere beschrijving van ISO 27001. Hoe het certificeringsschema zich verhoudt tot het ho-normenkader is daarmee ook impliciet beschreven.

9. Er bestaat geen geformaliseerde relatie tussen de twee werkgroepen IBP en Edukoppeling. Er is nu bilateraal afgestemd of de nieuwe versie van het certificeringsschema voldoet voor Edukoppeling. Overweeg om dit overleg structureel via de werkgroepen te laten verlopen.

Over de formele afstemmingsprocedure lijkt het nuttig om vóór elke jaarlijkse indiening een conceptversie te sturen naar de werkgroep Edukoppeling, zodat deze hierop feedback kan geven. Aangezien beide werkgroepen de wens hebben dat de standaarden interoperabel zijn, is de verwachting dat issues in het reguliere proces worden opgepakt en 'standaardisatie' niet in de weg staan.

10. "Proactief technisch beheer" (ROSA) - dit komt in het CS terug onder B: patchen en updates van firmware en software zijn ingeregeld en worden periodiek uitgevoerd. In het CS wordt dit beheer niet gerelateerd aan aan I en V. Beheer heeft naast beschikbaarheids- ook integriteits- en vertrouwelijkheidsimpact. Denk bijvoorbeeld aan security advisories vanuit bijvoorbeeld het NCSC, die vaak juist de I en V-aspecten belichten. Neem daarom de desbetreffende maatregelen ook bij I en V op, en leg vast dat bij verschillende vereiste niveaus in B,I,V steeds de zwaarste maatregelen (behorend bij het hoogste vereiste niveau) worden gehanteerd.

Er is bewust voor gekozen om de maatregelen maar eenmaal op te nemen in het CS om het beheer van de standaard en de implememtatie te vergemakkelijken. Tussen BIV zitten grijze gebieden omdat maatregelen altijd een groter effect hebben of nauw met elkaar samenhangen (bijvoorbeeld RPO/RTO). Er is gekozen om de maatregelen te plaatsen waar deze het grootste effect op heeft. In de praktijk blijkt dat het eigenlijk niet voorkomt dat door een verschil in vereiste niveau een maatregel gemist wordt. Daarbij gaat het met het CS om de basismaatregelen en zijn binnen een organisatie meestal nog veel andersoortige maatregelen nodig/mogelijk.

Met opmerkingen [AE1]: Ik snap de vraag nu helemaal niet meer eigenlijk, maar heb een antwoord geformuleerd naar beste eer en geweten.

11. “Technieken voor veilig programmeren” (ROSA) - komen niet expliciet terug in het CS. Overweeg een kolom toe te voegen voor maatregelen t.a.v. veilig programmeren.

Dit is een goede suggestie. Deze heeft vorm gekregen in RFC 25, die in de bijeenkomst van de Edustandaard werkgroep IBP op 19 februari 2018 wordt behandeld.

12. “Niet langer bewaren dan strikt noodzakelijk” - Heeft een duidelijk procesaspect, maar de ict-toepassing moet het wel *mogelijk* maken dat oude data wordt vernietigd. De kolom ‘levenscyclus’ besteedt wel aandacht aan bewaartermijnen, maar niet aan doelbinding. Neem in deze kolom ook maatregelen op die bewerkstelligen dat data waarvoor niet langer een doelbinding bestaat vernietigd kan worden.

Goede suggestie. In het CS kan worden opgenomen dat er voldaan moet worden aan de wettelijke bewaartermijnen. Het is een lastig gebied waarbij voorkomen moet worden dat er eisen gesteld worden aan de interface van een ict-toepassing. Het is aan de leverancier hoe *deze aan de eisen en maatregelen in het CS gaat voldoen.*
Voor wat betreft de doelbindingen pretendeert het CS niet om volledig te zijn. Het opsommen van mogelijke doelbindingen is oneindig. Het CS is daarbij een baseline/minimum aan maatregelen. Het ontslaat niet een leverancier van de verplichting of verantwoordelijkheid om daar waar nodig aanvullende maatregelen te treffen. In het bijzonder is het CS een afspraak over technische maatregelen voor de ict-toepassing. Informatiebeveiliging en privacy worden alleen passend beschermd door een samenspel van maatregelen op het gebied van mens (bijvoorbeeld bewustzijn), proces (bijvoorbeeld procedures en richtlijnen) en techniek (bijvoorbeeld het CS). Het gebruik van het CS alleen is niet voldoende, want niet alles is in techniek af te vangen. Een medewerker die gegevens verwerkt (met behulp van de toepassing) moet bewust zijn van toegestane en noodzakelijke handelingen. Dat kan deels worden ingevuld/gestuurd/ondersteund met richtlijnen en procedures. Het CS heeftop dit moment niet de ambitie om maatregelen op het gebied van mens en proces te beschrijven.

Het advies

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[1]	Goed
Adviseur(s)	Elise Lustenhouwer (Standaardisatie Expert)

Overige constateringen:

De roadmap die bij versie 2017 aanwezig was, is niet volldeig uitgevoerd. Voornamelijk de ‘mens en proces’-uitbreiding heeft geen doorgang gevonden. De implementatie van de huidige ‘techniek’ heeft al veel voeten in de aarde gehad en de tijd is nog niet rijp voor uitbreiding. Op dit moment is er geen roadmap, maar wordt er gewerkt aan de hand van RFC’s. Een logische (want vaak voorkomende) manier van werken voor een stabiele standaard.

Onderbouwing advies:

De adviezen uit de 2017-versie van het Certificeringsschema zijn opgepakt of anders is de keuze onderbouwd. De wijzigingen in de 2018-versie zijn minor en geven geen aanleiding voor nieuwe adviezen.

[1] 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