ROSA Architectuurscan/advies: Certificeringsschema 2017

edustandaard

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Remco de Boer
Versie	2e concept
Datum	14 juni 2017
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding	Inbeheername Certificeringsschema versie 2017
Betreft	Certificeringsschema Informatiebeveiliging en Privacy ROSA versie 2017
Brondocument(en)	Certificeringsschema algemene beschrijving v2.03 Certificeringsschema proces v2.03 Certifceringsschema classificatie v1.7 Certificeringsschema toetsingskader v0.9 Certificeringsschema toezicht v2.02
Begeleidende documenten	Aanmeldformulier *In beheername van Certificeringsschema Informatiebeveiliging en privacy ROSA door Edustandaard*

Inleiding

Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd. Niet alleen kan de indiener er zijn voordeel mee doen, ook kan ROSA ermee worden verrijkt. En tot slot stelt het andere ketenpartijen in staat om kennis te nemen van architectuurwijzigingen en het belang hiervan voor de eigen organisatie of achterban te bepalen (transparantie in de keten, informatiepositie).

Dit formulier bevat de uitkomst van een architectuurscan van het Certificeringsschema Informatiebeveiliging en privacy ROSA versie 2017 (hierna: het certificeringsschema). Het certificeringsschema is ter inbeheername aangeboden bij Edustandaard. Voor de Architectuurraad dient een uitgevoerde architectuurscan als basis voor haar advies aan de Standaardisatieraad. Voor de indiener biedt de scan concrete handvatten voor toepassing van ROSA, en

de mogelijkheid om lessen en ervaringen uit het project terug te koppelen aan ROSA. Een architectuurscan wordt in principe uitgevoerd met een hoge mate van betrokkenheid van vertegenwoordigers van de inbrenger. Deze wordt hierbij ondersteund door Bureau Edustandaard, de beheerder van ROSA. De inbrenger zou zich moeten herkennen in de uitkomsten.

Iedere architectuurscan begint met de vraag: welke onderdelen van ROSA zijn relevant voor het ingebrachte onderwerp, en indien relevant, op welke wijze? Vervolgens worden de vragen gesteld hoe het ingebrachte past op wat in ROSA is uitgewerkt, en of het project wellicht inzichten heeft die kunnen leiden tot verbetering of uitbreiding van ROSA. De antwoorden op deze vragen worden verwoord in termen van een advies richting zowel inbrenger, als richting ROSA zelf. De opzet van het advies is dat per onderdeel van ROSA uitspraken worden gedaan over:

1. Bevindingen uit project: *wat zegt het project zelf over het verband met ROSA van het ingebrachte onderwerp?*
2. Relatie met ROSA: *hoe verhoudt het ingebrachte zich tot ROSA[1]?*
3. Voorgesteld advies van de Architectuurraad aan het project: *tips, verbeterpunten, en ook bekrachtiging dat er goed werk is geleverd vanuit het perspectief van ROSA[2]*
   Adviezen in deze kolom zijn, gegroepeerd in 'PRODUCT' en 'CONTEXT'. De PRODUCT-adviezen bestrijken sec het ingediende 'product', d.w.z. het certificeringsschema. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van het certificeringsschema bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen het certificeringsschema toegepast gaat worden. Deze adviezen kunnen gericht zijn aan het project zelf, maar kunnen ook zijn gericht aan partijen die zich in die context bevinden, zoals de project(deel)groep die zich richt op de implementatie van de uiteindelijke certificeringsschema, maar ook (sector)organisaties die met de uiteindelijke implementatie te maken gaan krijgen.
4. **Voorgesteld advies voor de Architectuurraad voor plaatsing onderwerpen op de ROSA architectuur backlo**g: *wat kan ROSA doen om in het vervolg een betere ondersteuning te bieden aan dit project, en andere?*

Samenhang met andere formulieren:

- **Edustandaard aanmeldformulier**: in geval van een aanmelding of registratie, is er sprake van een Edustandaard aanmeldformulier[3]. In dit geval worden zowel het aanmeldformulier als de architectuurscan aan de Architectuurraad aangeboden. Het verband tussen de twee is dat het aanmeldformulier de bredere, ook niet-architecturele, context van het ingebrachte beschrijft. De architectuurscan gaat alleen, en dieper, in op de architectuuraspecten. Aangeraden wordt om de twee in samenhang te lezen, het aanmeldformulier eerst.[4]

[1] De verhouding tussen het ingediende en de ROSA wordt per onderdeel uitgedrukt in een 'level of conformance' ontleend aan TOGAF, zie de bijlage.

[2] Dit is een concept advies, de uitkomsten worden eerst door de Architectuurraad besproken.

[3] Een ROSA architectuurscan speelt naar verwachting niet in alle gevallen een rol in een aanmelding bij Edustandaard. Dit proces moet nog geformaliseerd worden.

[4] Op dit moment is er nog sprake van enige overlap tussen de twee formulieren. Deze wordt binnenkort geadresseerd, maar is niet bezwaarlijk voor het begrijpen van beide formulieren.

ROSA Architectuurscan/advies: Certificeringsschema

ROSA-onderdeel	Bevindingen uit project: Certificeringsschema	Relatie met ROSA (blauw: ROSA, geel: Certificeringsschema)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkings-gebied	Onderwijsdomein - het certificeringsschema is van toepassing op het gehele onderwijsdomein. Implementatie vindt op dit moment voornamelijk plaats in de sectoren po, vo, mbo. Daarnaast is het certificeringsschema onlosmakelijk verbonden aan implementaties van de Edukoppeling Transactiestandaard.	**Fully conformant** - het werkingsgebied van het Certificeringsschema valt volledig samen met het ROSA werkingsgebied.	-	-
Toepassings-gebied	Alle ict-toepassingen in het onderwijsdomein Het begrip “ict-toepassing” is belangrijk voor de duiding van de scope van het certificeringsschema, maar is binnen het certificeringsschema niet nader gedefinieerd.	**Compliant** - het certificeringsschema bestrijkt alle ict-toepassingen (in ROSA-termen: Voorzieningen) in het onderwijsdomein. Het certificeringsschema is gericht op ict-toepassingen, en niet op (certificering van) organisaties of processen.	**PRODUCT:** Definieer het begrip “ict-toepassing” **CONTEXT:** -	Overweeg het ROSA-begrip “voorziening” te vervangen door het begrip “ict-toepassing” - Binnen het certificeringsschema is bewust gekozen voor gebruik van het begrip “ict-toepassing” in plaats van “voorziening”. De herkenbaarheid van het begrip “ict-toepassing” blijkt namelijk groter. De strekking van beide begrippen is gelijkaardig.
Thema: **Bovensectorale samenwerking**	(niet getoetst ihkv quickscan)	**Onbepaald**	-	
Thema: **Informatie-beveiliging en privacy (IBP)**	***Algemeen*** Het certificeringsschema (CS) hanteert in het toetsingskader (iets) andere definities voor BIV dan het ROSA-katern IBP Het aspect ‘Controleerbaarheid’ is niet (apart) opgenomen in het toetsingskader CS. De rapportage, beschreven in het procesdocument, geeft invulling aan controleerbaarheid.	**Compliant** - Het certificeringsschema dekt (bewust) niet alles, maar beperkt zich tot ict-toepassingen. Hoewel gehanteerde BIV-definities en classificaties afwijken van die in het ROSA-katern IBP is de essentie van deze definities en classificaties gelijk.	**PRODUCT:** ***Algemeen*** 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.	Besteed bij het ontwerpkader Incident Response aandacht aan de zgn. PDRC-cyclus (preventie, detectie, repressie, correctie).Incident Response begint bij het gestructureerd kunnen herkennen en vervolgens reageren op incidenten Overweeg - Overnemen/vervangen definities BIV

	Het ROSA-katern IBP beschrijft risicoanalyse vanuit (keten)processen, het CS vanuit voorziening/ICT-toepassing. In de procesbeschrijving van het CS lopen teksten over het proces van toepassing van CS en het (keten)proces waarbinnen de desbetreffende ict-toepassing wordt gebruikt wat door elkaar. Noodzakelijkerwijs wordt de ict-toepassing als vertrekpunt genomen, maar wel beschouwd in zijn context (waaronder het ketenproces en de eisen die dat proces stelt). BIV-classificatie in CS (Basis/Standaard/Hoog) wijkt af van ROSA katern IBP (L/M/H) --- ***Principes en ontwerpkaders*** "Harmonisatie van de te nemen maatregelen" (ROSA) - naast het certificeringsschema bestaan er normenkaders specifiek voor ho (SURF) en mbo (taskforce IBP). Zij zijn alle geïnspireerd op ISO 2700X. Het certificeringsschema is een eerste onderwijsnormenkader waarin operationale maatregelen zijn vastgesteld. Een eerdere versie van het certificeringsschema was gebaseerd op de Cloud Control Matrix van de CSA, en stond daarmee verder af van de andere (ISO-gebaseerde) onderwijsnormenkaders. "Ketenpartijen conformeren aan CvIB" (ROSA) - het CS is gebaseerd op ISO 27002. Een mapping van CS-maatregelen op doelstellingen uit ISO 2700X ontbreekt. "Sectorbrede frameworks" (ROSA) - CS is hier een invulling van "Incident response" (ROSA) - Het CS toetsingskader besteed geen expliciete		***Ketenpartijen Conformeren aan CvIB*** 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. ***Incident response*** 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 - Bijeenroepen WG en besluitvorming - Actieve communicatie nieuwe maatregelen aan gebruikers van het certificeringsschema (leverancier, instellingen, organisaties aangesloten op Edukoppeling) - Termijn voor opstellen nieuwe auditverklaring? (cf. Auditverklaring punt 3, nu alleen voor ingrijpende wijzigingen IN DE DIENST zelf) ***Voldoende meet- en controlepunten*** 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. ***Voorkom ongewenste traceerbaarheid***	- Overnemen/vervangen BIV-classificatie (vereist uitleg waarom afgeweken is) De Term CvIB wordt niet breed herkend. Vervang dit door een expliciete verwijzing naar ISO 2700X.

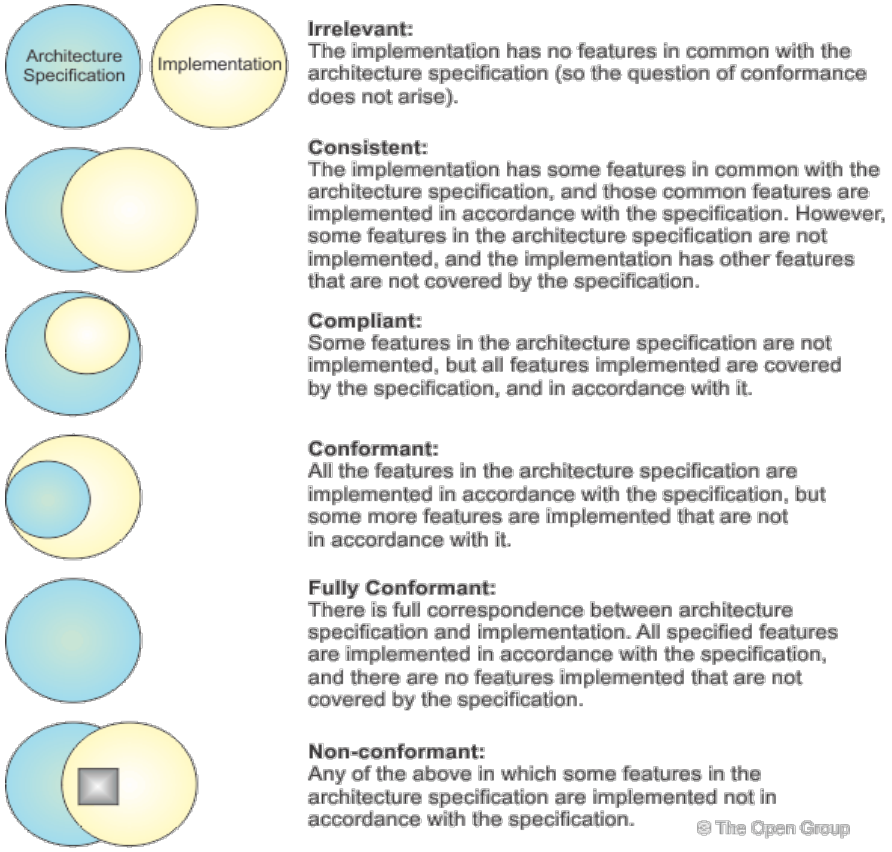
	aandacht aan de organisatie van Incident Response (*). Het beschreven proces rondom nieuw te nemen maatregelen (buiten het reguliere standaardisatieproces om) biedt de mogelijkheid om 'kortcyclisch' te werken. "Juiste gegevens op het juiste moment op de juiste plaats" (ROSA) - dit ontwerpkader heeft een bredere scope dan individuele voorzieningen / ICT-toepassingen. Wordt door CS tot op zekere hoogte invulling aan gegeven via B-maatregelen. "Continuiteit vd dienstverlening" (ROSA) - is een aparte kolom (business continuity) in het CS toetsingskader. "Duidelijke eisen en verwachtingen" (ROSA) - CS geeft invulling aan eisen en verwachtingen op een specifiek toepassingsgebied (nl. ICT-toepassingen) "Voldoende meet- en controlepunten" (ROSA) - hoewel het toetsingskaders enige gekwantificeerde kenmerken beschrijft (voor B, niet voor IV) wordt aan de monitoring van de mate waarin aan die kenmerken en/of maatregelen wordt voldaan geen aandacht besteed. "Afspraken over te realiseren ambitieniveaus" (ROSA) - dit is duidelijk aanwezig in het Toezicht-deel (niveaus van toezicht) en het Toetsingskader (niveaus van maatregelen) van het CS "Transparantie over maatregelen" (ROSA) - het CS maakt de te nemen maatregelen transparant, de auditverklaring de genomen maatregelen. "Valideer persoonsgebonden gegevens" (ROSA) - dit ontwerpkader kent vooral een		Overweeg - mede vanwege het belang van dit kader voor (minderjarige) onderwijsvolgers - maatregelen (ook) expliciet in het toetsingskader op te nemen, wellicht in een aparte kolom. ***Proactief technisch beheer*** 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. ***Technieken voor veilig programmeren*** Overweeg een kolom toe te voegen voor maatregelen t.a.v. veilig programmeren. ***Niet langer bewaren dan strikt noodzakelijk*** 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. **CONTEXT:** Het certificeringsschema dekt (bewust) niet alles, maar beperkt zich tot ict-toepassingen. Organisatorische (proces)maatregelen blijven noodzakelijk.	

	procesaspect, het CS gaat over voorzieningen c.q. Ict-toepassingen. “Voorkom ongewenste traceerbaarheid en vindbaarheid” (ROSA) - dit ontwerpkader heeft procesaspecten, maar gaat ook over de organisatie van data binnen de toepassing. Zie bijvoorbeeld ook de (aanvullende) ‘maatregelen om vermenging van gegevens te voorkomen’ die op de auditverklaring staan. “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. “Technieken voor veilig programmeren” (ROSA) - komen niet expliciet terug in het CS. “Voorkom onrechtmatige toegang” (ROSA) - komt in het CS terug via I/V maatregelen “Handelingen zijn herleidbaar” (ROSA) - komt terug in de kolommen logging en onweerlegbaarheid in BIV “Niet langer bewaren dan strikt noodzakelijk” - Heeft een duidelijk procesaspect, maar de ict-toepassing moet het wel *mogelijk* maken dat oude data wordt vernietigd. “Voorkom aantasting van integriteit” (ROSA) - komt in het CS terug in de I-maatregelen			
Thema: **IAA**	(niet getoetst ihkv quickscan)	**Onbepaald**	-	-
Thema: **Gegevens-**	(niet getoetst ihkv quickscan)	**Onbepaald**	-	-

uitwisseling in de keten				
Keten-processen	Het certificeringsschema kan gebruikt worden voor een ict-toepassing die als bouwsteen dient voor één of meer ketenprocessen. Het certificeringschema valt binnen de ketenfunctie Informatielevering en (indirect) mogelijk alle andere ketenfuncties, wanneer daar sprake is van informatielevering middels systemen binnen scope van het CS.	 **Fully conformant** - het certificeringsschema is binnen elk ketenproces toe te passen.	-	-
Zeggen-schappen en gegevens-soorten	Het certificeringsschema heeft betrekking op alle soorten gegevens die bewerkt worden door de desbetreffende ict-toepassing. In de procesbeschrijving van het certificeringsschema wordt, waar het gaat over de te betrekken partijen, gesproken over “de eigenaar van de data”.	 **Nonconformant** - Eigenaarschap van gegevens is zowel juridisch als inhoudelijk lastig te duiden. Een formeel (juridisch) eigenaarschap van gegevens bestaat niet, omdat in formele zin eigenaarschap altijd over stoffelijke zaken gaat, en gegevens dat niet zijn. Bovendien zullen vanuit verschillende rollen verschillende partijen 'iets' met gegevens moeten doen - een absoluut eigenaarschap is dus, los van de juridische context, uitgesloten. In ROSA wordt daarom uitgegaan van zeggenschappen die partijen kunnen hebben over gegevens.	**PRODUCT:** 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? **CONTEXT:**	
Bouwstenen en voorzieningen	Het certificeringsschema kan gebruikt worden voor een ict-toepassing die als bouwsteen dient voor één of meer ketenprocessen.	 **Fully conformant** - het certificeringsschema kan voor alle ict-toepassingen worden ingezet om de beveiligingsmaatregelen te toetsen.	-	-
Architecturele randvoor-waarden	Edukoppeling maakt gebruik van het certificeringsschema.	NVT	**PRODUCT:** 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	In de ROSA-wiki is een afbeelding opgenomen die de de relatie tussen de Edukoppeling Transactiestandaard en het Certificeringsschema weerggeeft. I dit diagram wordt voor het certificeringsschema weergegeven dat deze van toepassing is op SAAS-leveranciers (oude situatie). Dat dient te worden veranderd in “Leveranciers van

			beschrijving) **CONTEXT:** 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.	ICT-toepassingen".
Beheer en (door)ont-wikkeling	Aanpassingen aan het toetsingskader worden (in afwijking van het reguliere standaardisatieproces) direct gepubliceerd. Jaarlijks wordt de hele standaard als geheel opnieuw vastgesteld.	NVT		Ten aanzien van het ROSA katern IBP: Het certificeringsschema geeft aanleiding voor een herziening van (delen van) het ROSA katern IBP. In ieder geval moet de positie van het Certificeringsschema als toetsingskader (niet langer alleen voor cloud leveranciers) juist worden weergegeven. Ten aanzien van (nieuwe versies van) het certificeringsschema: Voer vanuit de Architectuurraad niet vaker dan jaarlijks een architectuurscan uit voor het CS, namelijk bij aanbieding van de jaarlijkse nieuw vatsgestelde versie. Neem kennis van de tussentijdse wijzigingen.
Implementatie				

Bijlage 1: **ARCHITECTURE COMPLIANCE (TOGAF)**



Bron: http://pubs.opengroup.org/architecture/togaf9-doc/arch/Figures/48_conformance.png

Een Nederlandse vertaling van de beschrijving van de TOGAF-categorieen:

a. **irrelevant** = er is geen relatie tussen het ingebrachte en ROSA
b. **consistent** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is het ingebrachte conform ROSA gerealiseerd, de overlap is echter niet **volledig** = sommige specificaties van ROSA zijn niet overgenomen, en het ingebrachte heeft onderdelen die niet door ROSA worden gedekt.
c. **compliant** = het ingebrachte valt volledig binnen ROSA (subset) en is conform ROSA gerealiseerd
d. **conformant** = ROSA dekt alleen een deel van het ingebrachte, maar dat deel is wel conform ROSA gerealiseerd
e. **fully conformant** = ROSA dekt het geheel van het ingebrachte, en niets van het ingebrachte valt buiten ROSA
f. **non-conformant** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is er iets van het ingebrachte *niet* conform ROSA gerealiseerd