ROSA Architectuurscan/advies: Certificeringsschema IBP ROSA v4

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Joeri van Es
Versie	2e concept
Datum	29/01/2026
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding Betreft	Major release van Certificeringsschema IBP ROSA v4
Brondocument(en)	[1] Aanmeldformulier 2026 [2] Certificeringsschema_toetsingskader-v4.0.xlsx [3] RFCs-Toetsingskader-3.0-versus-4.0.pdf
Begeleidende documenten	[4] Certificeringsschema_algemene_beschrijving-v3.0.pdf [5] Advies-van-Bureau-Edustandaard...v3-0.pdf

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 IBP ROSA v4**. 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 IBP ROSA v4**. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van het **Certificeringsschema IBP ROSA v4** bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen het **Certificeringsschema IBP ROSA v4** 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 IBP ROSA v4**, 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:

- **Pitch Architectuurscan**: Het doel van de architectuurpitch is om een eerste indruk te krijgen van een ketenafspraak . Op basis van de pitch en de aangeleverde documentatie voert Bureau Edustandaard een architectuurscan uit. Voor de leden van de Architectuurraad (en andere geïnteresseerden) verduidelijkt deze pitch de context van de afspraak en de resultaten uit de architectuurscan.
- **ROSA architectuurscan *bevindingen***: aan het invullen van het adviesdeel van een architectuurscan (dit formulier) gaat het verzamelen van feitelijke informatie, en het analyseren daarvan, vooraf. Die informatie, en de analyses, worden vastgelegd in het bevindingendeel van de architectuurscan. De lezer van het adviesdeel kan die erop na slaan als hij wil weten hoe het advies tot stand is gekomen. Het lezen van het bevindingendeel is niet vereist om het adviesdeel te begrijpen. Waar van toepassingen verwijst het bevindingendeel naar specifieke locaties van de brondocumenten die als input dienden voor de architectuurscan. Ook het lezen van de brondocumenten is niet vereist om het adviesdeel te begrijpen.

[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.

ROSA Architectuurscan/advies: Certificeringsschema IBP ROSA v4

ROSA-onderdeel	Bevindingen uit project: Certificeringsschema IBP ROSA v4	Relatie met ROSA (blauw: ROSA, geel: Certificeringsschema IBP ROSA v4)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkingsgebied	Het schema is toepasbaar op het gehele onderwijsdomein (po, vo, mbo, ho).	 **Fully conformant -** Het werkingsgebied dekt de volledige sector en sluit aan bij de ROSA-doelgroepen..	**PRODUCT:** **CONTEXT:** Blijf benadrukken dat dit schema ook voor het HO relevant is, in relatie tot de SURF Security Baseline.	
Ketendomeinen en -processen	Het schema is niet gebonden aan één specifiek ketenproces, maar is onderdeel van de generieke infrastructuur voor alle ketenprocessen die ondersteund worden door ICT (o.a. Informatielevering, Leerproces, Bedrijfsvoering). Het schema richt zich op ICT-toepassingen (voorzieningen) en niet op de organisatie zelf. [3]	 **Compliant -** De standaard is randvoorwaardelijk voor veilige uitvoering van ketenprocessen. 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:** **CONTEXT:**	

Scenario	Informatiebeveiliging is een randvoorwaarde voor betrouwbare ketenprocessen. Het certificeringsschema borgt de kwaliteit van IBP-maatregelen voor de voorzieningen die onderwijsprocessen ondersteunen. [4]	**Compliant** - Relatie met IV-Domein IBP. In het speciaal met IV-procesmodel Inrichten IBP-maatregelen De standaard wordt ook direct aan gerefereerd binnen dit IV-procesmodel.	**PRODUCT:** **CONTEXT:** Zorg dat de verwijzingen in de Edu-V afspraken en het Privacyconvenant worden bijgewerkt naar v4.0 zodra deze is vastgesteld.	
Ontwerpgebied **Governance**	Het beheer van het schema is belegd bij de Werkgroep Informatiebeveiliging en Privacy (IBP) van Edustandaard. Er is sprake van een open beheerproces waarbij stakeholders (onderwijsinstellingen en leveranciers) vertegenwoordigd zijn [1, 5.1.1]. Besluitvorming verloopt via de Architectuurraad en Standaardisatieraad [4]. Het schema bevat een specifiek 'Toezichtdocument' dat definieert hoe compliance wordt getoetst (self-assessment, audit). Dit model wordt juridisch verankerd via de verwerkersovereenkomsten van het Privacyconvenant en het Edu-V afsprakenstelsel [1, 3.2.2 en 4.1.1]. Het schema legt verantwoordelijkheden neer bij de leverancier (aantonen) en de onderwijsinstelling (eisen/controleren). Er is echter in RFC 2024025 opgemerkt dat het onduidelijk is wie verantwoordelijk is voor toezicht om certificering van	**Compliant** - De inrichting voldoet aan de ROSA-governance ontwerpkaders, met een specifiek aandachtspunt rondom toezicht. Het beheer door de werkgroep is compliant met ROSA ontwerpkader Betrokken belanghebbenden.	**PRODUCT:** Naar aanleiding van RFC 2024025: Maak in het procesdocument explicieter *wie* de trigger moet geven voor de jaarlijkse herziening. Is dit een push vanuit de leverancier (vervaldatum certificering) of een pull vanuit de school/Edu-V? Voorkom dat dit in het midden blijft hangen. **CONTEXT:**	

	leveranciers *jaarlijks* te herzien [3, RFC 2024025].			
Ontwerpgebied **IBP**	Het schema is bijgewerkt naar aanleiding van de ISO 27002:2022 structuur en bevat aangescherpte maatregelen [1, 2.6]. In tegenstelling tot de scan uit 2017, bevat v4.0 expliciete maatregelen voor incident respons. Bij niveau Midden/Hoog is een "gestructureerd proces voor notificatie aan de afnemer en herstel van de keten" verplicht en moet een "rollback-scenario" beschikbaar zijn bij onderhoud [2, regel 339, 344]. De eerdere omissie van veilige softwareontwikkeling is gecorrigeerd. Het kader eist nu expliciet: "Secure software development/secure coding guidelines worden toegepast" en toetst periodiek op OWASP Top 10 (Privacy Risks) [2, Vertrouwelijkheid, regel 758].	 **Compliant** - De bevindingen tonen aan dat het Certificeringsschema v4.0 een sterke invulling geeft aan de ROSA IBP kaders en eerdere tekortkomingen heeft aangepakt. De toevoeging van expliciete rollback-scenario's en notificatieprocessen maakt de afspraak *compliant* met het ROSA-kader dat ketenpartners transparantie en afstemming over incidenten vereist. Hoewel het schema zelf geen ISMS is, dwingt het leveranciers wel tot procesmatige borging van IBP (Plan-Do-Check-Act cyclus in beheer). Dit is compliant met ROSA ontwerpkader: Ketenpartijen hebben een kwaliteitssysteem	**PRODUCT:** Borg dat de verwijzingen naar externe standaarden (zoals NIST voor wachtwoorden en OWASP voor logging) in het Toetsingskader actueel blijven, gezien deze standaarden zelf ook evolueren. **CONTEXT:**	
Ontwerpgebied **Interoperabiliteit**	Het schema wordt expliciet gepositioneerd als specificatie van informatiebeveiligingseisen voor toepassingen die via Edukoppeling zijn aangesloten [1, 3.2.2]. Het is daarmee een randvoorwaarde voor	 **Compliant** - Het schema scoort **compliant** op interoperabiliteit door het gebruik van bestaande open	**PRODUCT:** **CONTEXT:**	

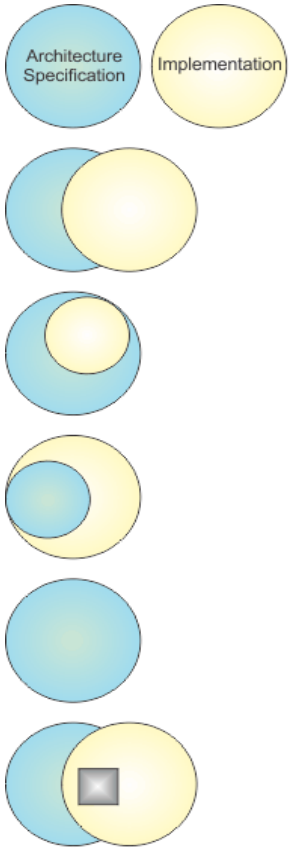
	vertrouwen binnen deze ketenstandaard. Het schema vindt aansluiting bij diverse (inter)nationale open standaarden: • Structuur gebaseerd op ISO 27002:2022 [1, 2.6]. • Wachtwoordeisen conform NIST richtlijnen [2, Vertrouwelijkheid, regel 740]. • Kwetsbaarheidstests conform OWASP Top 10 [2, Integriteit, regel 546]. • Encryptie-eisen conform Uniforme Beveiligingsvoorschriften (UBV) [2, Vertrouwelijkheid, regel 753].	standaarden en de naadloze integratie met Edukoppeling. De expliciete koppeling maakt het schema **Fully Conformant** met de ROSA-eis om Edukoppeling te ondersteunen. Het schema fungeert als het 'trust framework' onder de technische koppeling. Door niet zelf nieuwe cryptografische of procesmatige standaarden te verzinnen, maar te verwijzen naar UBV, NIST, ISO en OWASP, is het schema **Compliant** en voorkomt het vendor-lock-in of propriëtaire beveiligingsaanpakken.		
Ontwerpgebied **Identiteiten**	In tegenstelling tot de algemene eisen uit de 2017-scan, schrijft v4.0 nu expliciete authenticatiemiddelen voor per niveau. • Laag: Wachtwoordeisen conform NIST-richtlijnen [2, Vertrouwelijkheid, regel 740]. • Midden: Twee-factor authenticatie (2FA) is verplicht voor alle gebruikers, tenzij men enkel eigen niet-gevoelige gegevens inziet [2, Vertrouwelijkheid, regel 741]. • Hoog: 2FA is verplicht voor alle gebruikers [2, Vertrouwelijkheid, regel 741]. Het schema erkent federatieve authenticatie expliciet als geldig mechanisme. Er is een specifieke bepaling opgenomen: *"Bij federatieve*	 **Compliant** - Door NIST-richtlijnen en MFA verplicht te stellen op basis van risico (BIV), is het schema **Compliant** met het ROSA-ontwerpprincipe Digitale identiteit passend bij betrouwbaarheidsniveau. De expliciete clausule over federatief inloggen zorgt dat het schema Compliant is met ROSA ontwerpkader Universele digitale identiteit.	**PRODUCT:** **CONTEXT:**	

	inlog: de toepassing vertrouwt op de 2FA van de Identity Provider (mits contractueel/technisch geborgd) of dwingt deze zelf af" [2, Vertrouwelijkheid, regel 741].			
Ontwerpgebied **M2M Interactie**	Het schema bevat een 'Rapportage' tabblad dat automatisch een samenvatting genereert ten behoeve van de Verwerkersovereenkomst [2, Rapportage]. Dit standaardiseert de output van de audit, zodat deze uitwisselbaar is tussen leverancier en school.	**Onbepaald** - Er zijn op dit moment nog geen kaders vastgesteld voor dit ontwerpgebied. Daarom is relatie onbepaald. Hoewel de rapportage gestandaardiseerd is, is het formaat (Excel/PDF) nog niet machine-leesbaar (geen XML/JSON API).	**PRODUCT:** Overweeg om de output van het tabblad 'Rapportage' ook aan te bieden in een machine-leesbaar formaat (bijv. een simpele JSON-structuur of OSCAL-subset). Dit maakt het voor scholen en inkoopcollectieven (zoals SIVON/SURF) mogelijk om compliance-data geautomatiseerd in te lezen in registers. **CONTEXT:**	
Ontwerpgebied **H2M Interactie**	Het schema verwijst voor wachtwoordbeleid expliciet naar NIST Digital Identity Guidelines (SP 800-63) in plaats van ouderwetse complexiteitseisen. Dit betekent in de praktijk minder frustratie voor gebruikers (geen verplichte periodieke wijziging, focus op lengte/zinnen) [2, Vertrouwelijkheid, regel 740]. De RFCs tonen aan dat vragen in het schema zelf zijn herschreven om dubbelzinnigheid voor de invuller (de mens) weg te nemen (bijv. RFC 2024003 over 'kwetsbare groepen'). Het doel is het schema "zo gebruiksvriendelijk mogelijk" te maken [1, 2.4 en 3].	**Onbepaald** - Er zijn op dit moment nog geen kaders vastgesteld voor dit ontwerpgebied. Daarom is relatie onbepaald. Door de NIST-richtlijnen te adopteren (die password fatigue tegengaan), lijkt het schema compliant met het concept ontwerpprincipe Passende gebruiksvriendelijke digitale identiteit. Hier is de relatie compliant met concept ontwerpprincipe Digitale toegankelijkheid.	**PRODUCT:** **CONTEXT:**	

Onderwijssemantiek	In de vorige scan (2017) werd geconstateerd dat de BIV-definities afweken van het ROSA Katern IBP. In v4.0 zijn de classificatievragen (Stap 2) aangescherpt en voorzien van motivatie-velden om de semantiek (betekenis) van "Laag/Midden/Hoog" eenduidig te maken voor de invuller. De definities zijn nu operationeel gemaakt voor risico-afweging (economische schade, reputatieschade) [2, 3]. Het schema hanteert voor specifieke begrippen de definities uit de AVG. Een concreet voorbeeld in v4.0 is de definitie van "Profilering", waarbij expliciet wordt verwezen naar Artikel 4 van de AVG om misverstanden over dit begrip te voorkomen [2 Stap 2, regel 22] [3, 2024003].	 **Consistent -** Het schema draagt bij aan eenduidige semantiek binnen het IBP-domein, hoewel het niet echt draait om semantiek, maar meer een pragmatisch instrument is. De bevinding uit 2017 is grotendeels geadresseerd. Hoewel de definities van BIV (Laag/Midden/Hoog) specifiek blijven voor dit instrument, zijn ze door de verduidelijking in v4.0 (via RFCs) wel Consistent gemaakt met de risicobelevingswereld van de onderwijsinstellingen. Het schema fungeert hierdoor als de de facto standaard voor de betekenis van "Beveiligingsniveau" in het onderwijsstelsel.	**PRODUCT:** Verwijs direct naar het ROSA Begrippenkader vanuit het certificeringsschema. Controleer of alle gebruikte begrippen al in het ROSA Begrippenkader aanwezig zijn.	
Referentie-componenten en ketenvoorzieningen	Het schema richt zich op "ICT-toepassingen" in de volle breedte. Specifiek worden genoemd: Digitale leermiddelen en Leerlingadministratiesystemen (LAS). Het schema stelt kwaliteitseisen aan deze applicaties. [1, 3.1.2].	 **Fully conformant -** De relatie is Fully Conformant. In het ROSA scenario *Inrichten IBP maatregelen* wordt gesteld dat ieder Gegevensverwerkend Systeem gebruik kan maken van het certificeringsschema. De transactiestandaard (Edukoppeling) regelt de techniek, dit schema regelt het vertrouwen in de beveiliging van applicaties binnen het onderwijsstelsel. Ze zijn	**PRODUCT:** **CONTEXT:**	

		onlosmakelijk verbonden, zoals ook in de scan van 2017 al werd geconstateerd en nu in v4 nogmaals bekrachtigd.		
Beheer en (door)ont-wikkeling			**PRODUCT:** **CONTEXT:**	
Implementatie	Er is geen centrale tooling voor validatie, maar wel een Excel-tool voor zelfevaluatie/audit. Implementatie is de verantwoordelijkheid van de leverancier/school.		**PRODUCT:** Overweeg voor een toekomstige versie (v5) of de Excel-tool vervangen kan worden door een online self-assessment tool om dataverzameling en benchmarking mogelijk te maken. **CONTEXT:**	

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



Irrelevant:
The implementation has no features in common with the architecture specification (so the question of conformance does not arise).

Consistent:
The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.

Compliant:
Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.

Conformant:
All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.

Fully Conformant:
There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.

Non-conformant:
Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.

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