edustandaard

Architectuurscan
Certificeringsschema IBP ROSA v4.0

Joeri van Es
Bureau Edustandaard

Architectuurraad
4 februari 2026

ROSA Scan

Certificeringsschema IBP ROSA v4.0

Samenvatting scanaanvraag

Om welke afspraak gaat het?	Certificeringsschema informatiebeveiliging en privacy ROSA
Doel van de afspraak	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. 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).
Aanleiding voor de afspraak	Het certificeringsschema is ontwikkeld om vertrouwen te creëren in de betrouwbaarheid en privacybescherming van ICT-toepassingen in het onderwijs. Het biedt een concrete normenkader-plus-toetsing voor IBP die aansluit op bestaande classificaties en normenkaders.

edustandaard

ROSA Scan

Certificeringsschema IBP ROSA v4.0

Samenvatting scanaanvraag

Scan aangevraagd door	Edustandaard Werkgroep IBP
Doel van de scan	Nieuwe major release alignen ten opzichte van de huidige versie van de ROSA (laatste scan was in 2017).
Wat gaat er nu gebeuren?	Nieuwe versie wordt aangeboden ter vaststelling aan de SR

edustandaard

ROSA Scan

Certificeringsschema IBP ROSA v4.0

Complexiteit en risico's

Projectfase	**Afgerond / inbeheername**	**Al even op weg**	**Prille begin**
Werkingsgebied	**Eén werkingsgebied**	**Meerdere werkingsgebieden**	**Gehele onderwijsdomein**
Processcope	**Beperkt aantal ketenprocessen**	**Meerdere ketenprocessen**	**(Vrijwel) alle ketenprocessen**
Privacy	**Geen persoonsgegevens**	**Enkele persoonsgegevens**	**Veel / bijzondere persoonsgeg.**
Informatiebeveiliging	**Geen BIV-eisen**	**Enkele BIV-eisen**	**Strikte BIV-eisen**
Toegang	**Openbaar / publiek**	**Obv groepslidmaatschap / rol**	**Obv identiteit**
Gegevensuitwisseling	**Geen m2m-koppelingen**	**Enkele koppelingen, meerdere gelijksoortige partijen**	**Veel koppelingen, veel verschillende partijen**
Realisatie / impl. / uitrol	**Triviaal**	**Gemiddeld**	**Complex**
Beheer en doorontw.	**Beheer en doorontwikkeling is belegd**	**Beoogde beheerpartij bekend, nadere afspraken maken**	**Nog onduideljk / onbekend**

edustandaard

Brondocumentatie

- [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

ROSA Scan

Certificeringsschema IBP ROSA v4.0

Overzicht scanresultaten

- Fully conformant — 1. Werkingsgebied
- Compliant — 2. Ketendomeinen en -processen
- Compliant — 3. Scenario
- Compliant — 4. Ontwerpgebied: Governance
- Compliant — 5. Ontwerpgebied: IBP
- Compliant — 6. Ontwerpgebied: Interoperabiliteit
- Compliant — 7. Ontwerpgebied: Identiteiten
- ? Onbepaald — 8. Ontwerpgebied: M2M Interactie
- ? Onbepaald — 9. Ontwerpgebied: H2M Interactie
- Consistent — 10. Onderwijssemantiek
- Fully conformant — 11. Referentiecomponenten en ketenvoorzieningen

edustandaard

Samenvatting scan

Hoofdlijnen:

1. **Opvolging aanbevelingen ROSA-scan 2017**
   a. IBP (Incident Respons): In tegenstelling tot 2017 zijn processen voor notificatie en 'rollback-scenario's' nu expliciet verplicht gesteld.
   b. Identiteiten (Authenticatie): In plaats van generieke eisen schrijft v4.0 nu specifieke middelen (zoals 2FA) voor per risiconiveau.
   c. Semantiek (Definities): De in 2017 geconstateerde afwijking op BIV-definities is hersteld door deze operationeel en AVG-consistent te maken.
2. **Governance en Sectorbrede Dekking**
   a. Scope: Het schema is Fully Conformant en dekt de gehele sector (PO, VO, MBO, HO) als generieke standaard.
   b. Borging: De governance is compliant en juridisch verankerd in het Privacyconvenant en Edu-V.
   c. Aandachtspunt: De verantwoordelijkheid (haal- of brengplicht) voor het toezicht op de jaarlijkse hercertificering moet explicieter.

Samenvatting scan

Hoofdlijnen:

3. **Interoperabiliteit via Open Standaarden**
    a. Fundament: Het schema is Compliant door volledige adoptie van externe standaarden (ISO 27002:2022, NIST, OWASP).
4. **Advies: Professionalisering naar Data-gedreven Toezicht**
    a. Product advies: Maak de output van de audit machineleesbaar (JSON/XML) zodat inkoopcollectieven dit automatisch kunnen verwerken.
    b. Product advies: Vervang de huidige Excel-tooling door een centrale online self-assessment applicatie voor betere benchmarking.
    c. Context advies: Werk verwijzingen in juridische kaders (Edu-V) direct bij naar v4.0 om eisen gelijk te trekken.

Adviezen aan ROSA (1/1)

- Geen

Adviezen aan product (1/1)

- 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.
- 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.
- 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.
- Verwijs direct naar het ROSA Begrippenkader vanuit het certificeringsschema. Controleer of alle gebruikte begrippen al in het ROSA Begrippenkader aanwezig zijn.
- 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.

Adviezen aan context (1/1)

- Blijf benadrukken dat dit schema ook voor het HO relevant is, in relatie tot de SURF Security Baseline.
- Zorg dat de verwijzingen in de Edu-V afspraken en het Privacyconvenant worden bijgewerkt naar v4.0 zodra deze is vastgesteld.