edustandaard

Memo: Positionering Certificeringsschema IBP ROSA ten opzichte van andere beveiligingskaders

Voor:	Architectuurraad en Standaardisatieraad, Edustandaard
Van:	Jordy van den Elshout en Bureau Edustandaard
Datum:	07-05-2026
Betreft:	Positionering van het Certificeringsschema IBP ROSA

Inhoud

1. Samenvatting

Binnen het onderwijs worden verschillende kaders gebruikt om informatiebeveiliging te organiseren en te toetsen, zoals het Normenkader IBP FO, het SURFaudit Toetsingskader Informatiebeveiliging en ISO27001. Deze kaders richten zich primair op de inrichting, sturing en beheersing van informatiebeveiliging binnen organisaties.

Het Certificeringsschema IBP ROSA heeft een andere functie. Het schema richt zich op onderwijsapplicaties en maakt concreet welke beveiligingseisen daaraan gesteld kunnen worden. Daarmee vormt het geen alternatief voor bestaande organisatienormenkaders, maar een aanvullende sectorafspraak op applicatieniveau.

Deze positionering is van belang omdat onderwijsinstellingen bij het gebruik van digitale diensten afhankelijk zijn van leveranciers. Instellingen moeten kunnen sturen op informatiebeveiliging, terwijl leveranciers op een eenduidige manier moeten kunnen aantonen dat hun applicaties voldoen aan de gestelde eisen. Het Certificeringsschema IBP ROSA biedt daarvoor een gemeenschappelijke taal en een uniforme verantwoordingswijze.

2. Aanleiding

In de onderwijssector bestaan meerdere kaders voor informatiebeveiliging. Voor instellingen zijn onder meer het Normenkader IBP FO en het SURFaudit Toetsingskader Informatiebeveiliging relevant. Leveranciers hanteren daarnaast vaak ISO27001 of een vergelijkbaar normenkader voor hun eigen organisatie.

Het bestaan van meerdere kaders kan de indruk wekken dat sprake is van overlap of dubbele eisen. Dat roept vragen op over de onderlinge verhouding tussen deze kaders en over de specifieke rol van het Certificeringsschema IBP ROSA.

De kern van het vraagstuk is dat de genoemde kaders verschillende rollen hebben. Organisatienormenkaders richten zich op de inrichting van informatiebeveiliging binnen organisaties. Het Certificeringsschema IBP ROSA vertaalt deze verantwoordelijkheid naar concrete, toetsbare eisen aan onderwijsapplicaties.

Dit memo duidt deze verhouding en beschrijft waarom het wenselijk is om het Certificeringsschema IBP ROSA te positioneren en te borgen als sectorafspraak voor applicatiegerichte informatiebeveiliging.

3. Positionering ten opzichte van andere beveiligingskaders

Het Certificeringsschema IBP ROSA moet worden gezien als een sectorale invulling van beveiligingseisen voor onderwijsapplicaties. Het schema vervangt geen bestaande kaders zoals het Normenkader IBP FO, het SURFaudit Toetsingskader of ISO27001.
De verhouding kan als volgt worden samengevat:

- Organisatienormenkaders ondersteunen de inrichting en beheersing van informatiebeveiliging binnen organisaties;
- Het Certificeringsschema IBP ROSA concretiseert beveiligingseisen voor onderwijsapplicaties;
- De auditverklaring biedt een uniforme manier om naleving van die applicatiegerichte eisen aantoonbaar te maken.

Daarmee ontstaat een onderscheid tussen organisatieniveau en applicatieniveau. Op organisatieniveau kunnen instellingen en leveranciers verschillende kaders hanteren, ook bij toekomstige eisen zoals vanuit NIS2. Op applicatieniveau is juist uniformiteit wenselijk, omdat onderwijsapplicaties vaak sectoroverstijgend worden gebruikt en afwijkende eisen per sector of instelling leiden tot interpretatieverschillen en extra verantwoordingslast.

Het Certificeringsschema IBP ROSA biedt in dat opzicht een brug tussen onderwijsinstellingen en leveranciers. Een onderwijsinstelling kan sturen vanuit bijvoorbeeld het Normenkader IBP FO of SURFaudit, terwijl een leverancier zijn interne informatiebeveiliging kan organiseren op basis van ISO27001. Het Certificeringsschema biedt vervolgens de gedeelde taal voor de eisen aan de applicatie zelf.

4. Toepassing in de praktijk

Het Certificeringsschema IBP ROSA ondersteunt onderwijsinstellingen bij het stellen en toetsen van beveiligingseisen aan applicaties. Het helpt onder meer bij:

- Het concretiseren van beveiligingseisen voor onderwijsapplicaties;
- Het toetsen van naleving door leveranciers;
- Het uitvoeren van leveranciersmanagement;
- Het hergebruiken van een uniforme verantwoordingswijze.

Voor leveranciers biedt het schema eveneens duidelijkheid. Zij hoeven niet voor iedere instelling, sector of afspraak afzonderlijk beveiligingseisen te interpreteren. Via het Certificeringsschema kunnen zij op een eenduidige manier aantonen dat hun applicatie voldoet aan de eisen die binnen de onderwijssector worden gesteld.

Dit is ook relevant voor afsprakenstelsels en modelovereenkomsten. Stelsels zoals Edu-V en afspraken rond gegevensuitwisseling, zoals Edukoppeling, kunnen naar het Certificeringsschema verwijzen in plaats van eigen beveiligingseisen te ontwikkelen. Ook modelverwerkersovereenkomsten, zoals binnen het Privacyconvenant, kunnen hierbij aansluiten.

Daarmee voorkomt het Certificeringsschema versnippering en dubbele verantwoordingslast. Het biedt een gedeelde basis voor applicatiegerichte beveiligingseisen binnen de onderwijssector, terwijl instellingen en leveranciers op organisatieniveau ruimte houden om een eigen passend normenkader te hanteren.

5. Verschillen per onderwijssector

De onderwijssectoren werken met verschillende kaders en praktijken voor informatiebeveiliging. De verschillen zitten vooral op organisatieniveau. Voor applicaties is uniformiteit wenselijk.

In het funderend onderwijs wordt gewerkt met het Normenkader IBP FO. Dit normenkader bevat een expliciete relatie met het Certificeringsschema IBP ROSA. Op applicatieniveau kan het Certificeringsschema worden gebruikt om beveiligingseisen concreet en toetsbaar te maken. Daarnaast wordt het Certificeringsschema gebruikt of betrokken bij afsprakenstelsels en modelafspraken, zoals Edu-V, Edukoppeling en het Privacyconvenant.

In het mbo wordt op organisatieniveau gewerkt met het SURFaudit Toetsingskader Informatiebeveiliging. Voor applicaties kan het Certificeringsschema IBP ROSA een uniforme invulling geven aan beveiligingseisen richting leveranciers. Ook voor het mbo is de meerwaarde vooral gelegen in leveranciersmanagement, toetsbaarheid en hergebruik binnen sectorale afspraken.

In het hoger onderwijs wordt gewerkt met SURFaudit en mogelijk ook met ISO27001 of andere normenkaders. Daarnaast bestaan er security baselines of vergelijkbare instrumenten voor applicaties en diensten. Voor het hoger onderwijs is nadere afstemming nodig over de verhouding tussen het Certificeringsschema IBP ROSA, de bestaande SURFaudit-systematiek, ISO27001 en eventuele sectorale security baselines. Daarbij is vooral van belang of en hoe een uniforme applicatiegerichte toetsing meerwaarde biedt naast bestaande kaders en ontwikkelingen.

Het uitgangspunt blijft dat sectoren op organisatieniveau eigen keuzes kunnen maken, terwijl het Certificeringsschema IBP ROSA kan bijdragen aan uniformiteit op applicatieniveau. Daarmee kan het Certificeringsschema dienen als gedeelde basis voor applicatiegerichte beveiligingseisen binnen afsprakenstelsels, modelovereenkomsten en leveranciersmanagement in het onderwijs.