Concept Agenda werkgroep IBP (maart 2024)

14 maart 2024, 13:00 – 14:30, locatie: online

**Agenda**

1. Opening
2. Ruimte voor toelichtingen en voorstellen*.*
*De werkgroep ik lange tijd niet bijeen geweest en de werkgroep heeft veel nieuwe leden.*
3. Stand van zaken
4. Algemeen
*Huidig gebruik, voorgaande wijzigingen op hoofdlijnen, en andere ontwikkelingen (zoals ROSA scan op Surf Baseline) bespreken.*
Doel: zorgen dat iedereen dezelfde informatiepositie heeft, vooral voor de nieuwe werkgroep leden.
5. Ontwerpgebied IBP
*In 2023 is er een nieuwe versie van* [*ROSA*](https://rosa.wikixl.nl/index.php/Hoofdpagina) gep*ubliceerd. Naar aanleiding hiervan zijn ook de principes voor IBP herzien en uitgewerkt in een IV-domein (*[Inrichten IBP-maatregelen](https://rosa.wikixl.nl/index.php/Id-225ebca8097947a99121c278e18126a0)*) binnen de ROSA.*
*Doel: informeren over de uitwerking IV-domein IBP en bespreken van eventuele vragen of aandachtspunten.*
6. Document Toezicht
*Toezicht vindt steeds vaker plaats en gaat komende jaren toenemen. Binnen de onderwijssector lopen daar verschillende trajecten voor, zoals ook binnen Digitaal Veilig Onderwijs door SIVON. Daarnaast zijn enkele opmerkingen binnengekomen op het document Toezicht. i) Zo leidt classificatie van onafhankelijkheid (laag, midden, hoog) verwarring op; deze heeft dezelfde classificatie categorieën heeft als de BIV, waardoor de lezer hier een koppeling in maakt. Deze is er alleen niet. ii) Ook zijn de eisen voor de externe audit niet voldoende duidelijk. Registratie van een auditor kan bijvoorbeeld op meerdere niveaus.*
*Voorstel is om het document te herzien met een review door belanghebbenden, mede op basis van de huidige en gewenste toezicht in de sector.*
Doel: voorstel bespreken en bepalen wie een actieve rol kan of moeten spelen in de review van het document Toezicht.
7. Wetgeving NIS2
*Op 17 oktober 2024, of later door uitstel, treedt de Nederlandse versie van NIS2 in werking. Waarschijnlijk door middel van opvolging van de Wet beveiliging netwerk- en informatiesystemen (Wbni). In* [artikel 21 lid 2 (NIS2)](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555&qid=1695042128616#d1e3367-80-1) *staan maatregelen die getroffen moeten worden. Zoals over bekendmaking van kwetsbaarheden (sub f) en gebruik multifactor-authenticatie (sub j). De vraag is in hoeverre deze overeenkomen en in lijn zijn met het Toetsingskader. Wanneer dat wel het geval is, draagt dat op een effectieve wijze bij aan het conformeren aan deze wetgeving (indien een aanbieder van ict-toepassingen hieraan moet voldoen).*
*Doel: bespreken en besluiten om impact van NIS2 mee te nemen in herziening van het Toetsingskader.*
8. Inhoudelijk
9. Vaststellen BIV-classificatie
*De BIV hoort door de proces/data-eigenaar (de verwerkingsverantwoordelijke) vastgesteld te worden, echter wordt dit met de huidige opzet door de leverancier bepaald door het invullen van de vragenlijst. In de praktijk wordt dit ook veelal door alle schoolinstellingen (de verwerkingsverantwoordelijke) overgenomen, echter is de vraag of de BIV-classificatie in dat geval juist is. In geval van een hogere BIV door de leverancier hoeft dit geen probleem te zijn, echter bij een lagere BIV wel; de (persoons)gegevens zijn in dat geval onvoldoende beschermd conform de baseline. De verantwoordelijkheid om dit te controleren ligt bij schoolinstelling, echter is enige mate van uniformiteit gewenst. De sectorale Referentie Architectuur (zoals* [FORA](https://fora.wikixl.nl/index.php/FORA/id-86533216-bcdf-432a9-9d43-9985ce3e7d9)*,* [MORA](https://mora.mbodigitaal.nl/index.php/BIV-classificatie) *en* [HORA](https://hora.surf.nl/index.php/BIV_classificaties)*) kunnen hier mogelijk een rol in spelen. Daarin zijn BIV-classificaties opgenomen als referentiecomponent en kan naar verwezen worden.*
*Doel: Situatie en mogelijke verbeteringen bespreken. Indien mogelijk tot een besluit komen, welke uitgewerkt kan worden in het Cert. schema. Mogelijk ook een bestellingen richting andere initiatieven, zoals modelverwerkersovereenkomsten t.b.v. de blijvende verantwoordelijkheid tot controle.*
10. Uitbesteden van maatregelen en de controle hierop
*Steeds vaker worden clouddiensten gebruikt waarmee ict-toepassingen in het onderwijs worden aangeboden. In dat geval worden meerdere maatregelen door de cloudprovider verzorgt, echter blijft de aanbieder/verwerker verantwoordelijk dat dit afdoende is ingevuld. Daarnaast zijn maatregelen standaard verzorgt (zoals fysieke beveiliging), of op basis van een instelling (zoals encryptie). Edustandaard heeft het signaal ontvangen dat hier meer informatie per maatregel en leverancier over gewenst is. Wellicht dat collectief hier een FAQ voor ingericht kan worden, zodat alle aanbieders hierin het onderwijs profijt van kunnen hebben.*
*Doel: bespreken of een FAQ hier passend is en op welke manier dit collectief georganiseerd kan worden.*
11. Afsluiting
12. Werksessie per onderdeel (Toezicht en Toetsingskader) vaststellen, zowel de leden als het moment.
13. Planning voor de volgende werkgroep bijeenkomst, zowel voor dit overleg met de werkgroep als voor de kerngroep ter voorbereiding op het overleg van deze werkgroep.