Het (Meervoudig) DigiD Assessment

Toelichting op tijdlijn, proces en normen

Axel Vogelzang

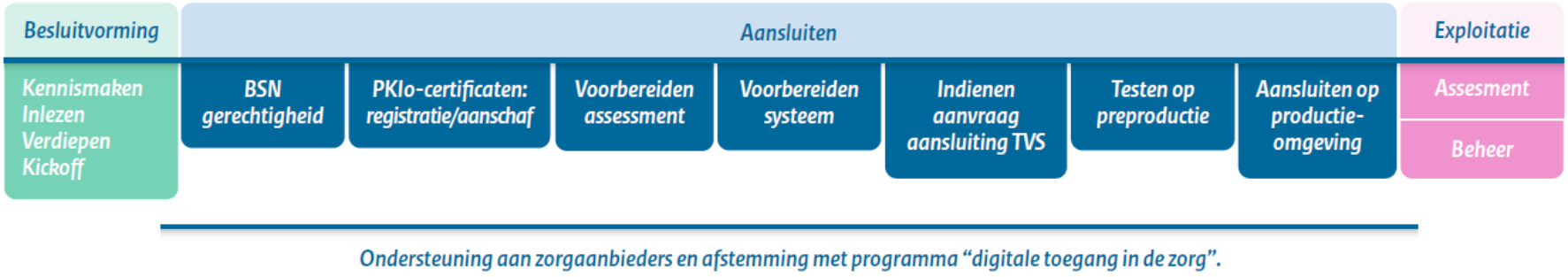
Adviseur Audit

Agenda

- Welkom
- Context van het (meervoudig) assessment
- Waarom een (meervoudig) assessment?
- Het meervoudig assessment toegelicht
- Voorwaarden toepassen meervoudig Digid assessment
- Voorbereiden op meervoudig assessment; tijdlijn, stappen
- Normen op hoofdlijnen
- Vragen

Context van het (meervoudig) assessment

- De afronding van het aansluitproces op de productie-omgeving DigiD
- Het kunnen aantonen van de 'meervoudigheid' van de aansluiting
- Na een positief assessmentrapport: het begin van het (grootschalig) aansluiten van de dienstverleners



Waarom een (meervoudig) assessment?

- Digitale uitwisseling van privacygevoelige data tussen (zorg)instellingen en burgers wordt steeds belangrijker
- Het vertrouwen in DigiD is hierbij cruciaal
- De DigiD - aansluiting dient aantoonbaar aan de gestelde eisen te (blijven) voldoen
- Het (meervoudig) assessment gaat in op de formele, procedurele en technische eisen aan de directe - of clusteraansluiting

Het meervoudig assessment toegelicht

- De Wdo* eist een inlogmiddel met (minimaal) het betrouwbaarheids-niveau ‘substantieel’ bij de uitwisseling van privacygevoelige informatie, zoals in de zorg
- Om aansluiten op DigiD voor dienstverleners te vergemakkelijken is het concept van de clusteraansluiting bedacht
- Via één IT- leverancier kan een groot aantal dienstverleners aansluiten op DigiD; de leverancier laat de initiële en periodieke meervoudige Digid - assessments uitvoeren

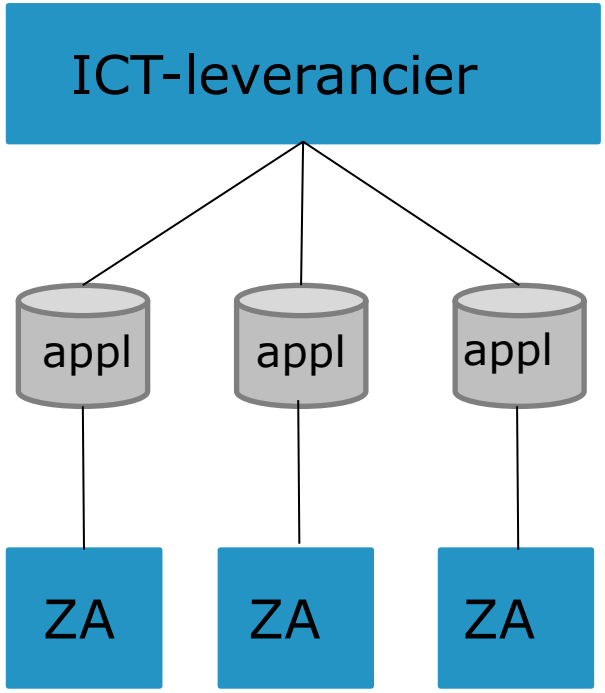
* Wet Digitale Overheid

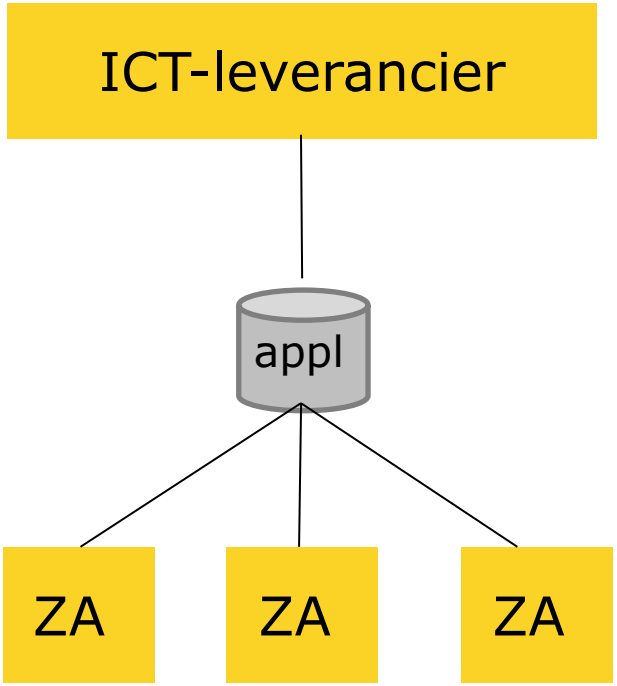
Het meervoudig assessment toegelicht

Waar de clusteraansluiting voordelen oplevert ten aanzien van de inspanningen en kosten, ontstaan ook nieuwe verplichtingen. De leverancier:

- Legt contractueel vast dat hij erop toeziet dat aansluithouders aan de gestelde eisen en voorwaarden van Digid (blijven) voldoen en
- grijpt in bij ongewenste situaties op de infrastructuur, sluit eventueel een zorgpartij af.

Enkelvoudig versus meervoudig assessment





Samenvatting en verschillen

Enkelvoudige assessment	Meervoudige assessment
Per aangesloten dienstverlener jaarlijkse auditverplichting	Per **leverancier** jaarlijkse auditverplichting
Assessment nieuwe aansluiting binnen twee maanden na activering	**Nieuw aangesloten dienstverlener “lift mee” op de jaarlijkse audit**
Kosten audit geheel voor rekening dienstverlener	**Kosten audit kunnen worden verdeeld over dienstverleners**
Uitvoerder audit: IT- auditor (RE)	Uitvoerder audit: IT- auditor (RE)

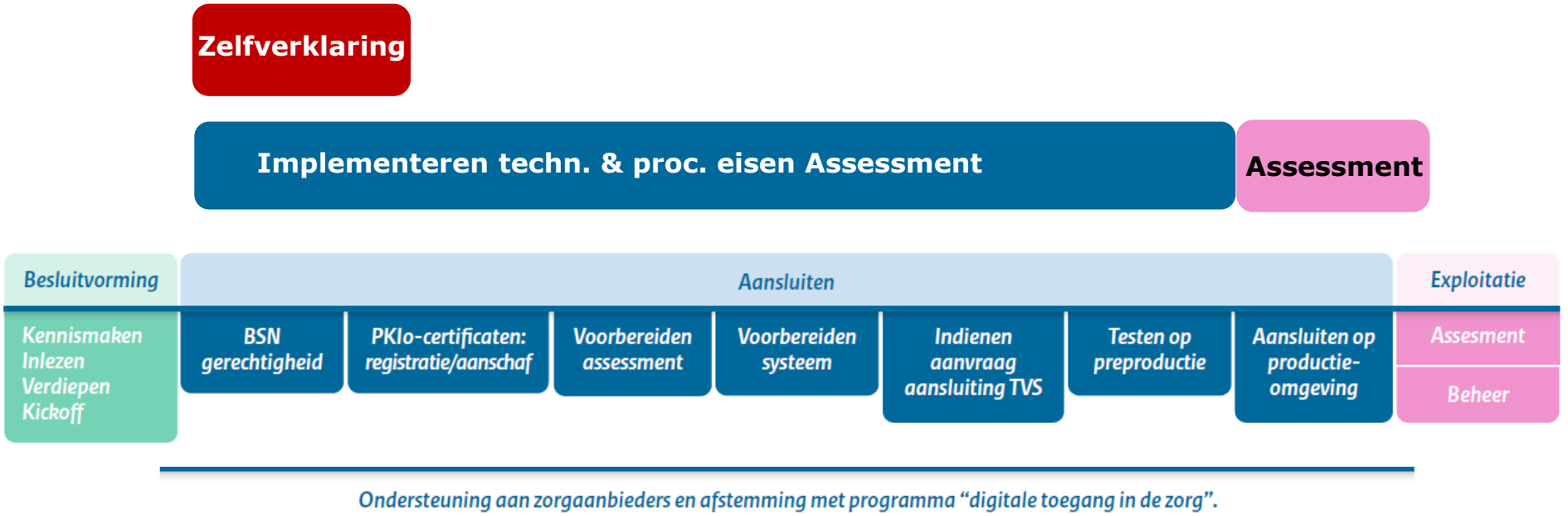
Voorwaarden uitvoeren Meervoudig Assessment

Wanneer mag het Meervoudig Assessment worden uitgevoerd?

- ✓ de leverancier voldoet aan de eisen van de zelfverklaring*; standaardcontract (nu: versie 1.4) met Logius en voorwaarden in de overeenkomst met de dienstverleners;
- ✓ Twee dienstverleners zijn aangesloten op DigiD en maken gebruik van de gedeelde functionaliteit geleverd via hetzelfde platform waar de gebruiker (patiënt) op inlogt met DigiD;
- ✓ de auditor kan het assessment (hoofdzakelijk) op één centrale locatie uitvoeren.

* door Logius 'Accreditatie' genoemd

Voorbereiding van het (meervoudig) assessment



Voorbereiden op (Meervoudig) Assessment - stappen

Direct na de intake - start van het aansluittraject:

- **Zelfverklaring*** (afsluiten standaardcontract met Logius) voor een meervoudig assessment
- Het kennisnemen van de Handreiking en de daarin opgenomen procedurele en technische normen
- Het zo snel mogelijk opstellen van een gap - analyse t.o.v. de huidige situatie en de vereisten
- Het selecteren van de auditor
- Het plannen van pre-assessment, pentest en assessment

* door Logius 'Accreditatie' genoemd

Voorbereiden op (Meervoudig) Assessment - tijdlijn

Vanaf het moment van de *aansluiting* van de (eerste) dienstverlener op de productie-omgeving, heeft de dienstverlener of leverancier twee maanden om de assessmentrapportage bij de toezichthouder (Logius) in te dienen. Het meervoudig assessment kan pas worden uitgevoerd na het aansluiten van een tweede dienstverlener.
Dit wil zeggen dat er op het moment van aansluiten van de (eerste) dienstverlener geen (majeure) audit - issues meer mogen openstaan!
Daarom wordt een pre-assessment sterk aanbevolen.

Normenkader “DigiD assessments”

IT auditor assessment

NCSC

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

ICT Beveiligingsrichtlijnen voor webapplicaties

NORMENKADER Meervoudig Assessment

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA HANDREIKING

Normen op hoofdlijnen

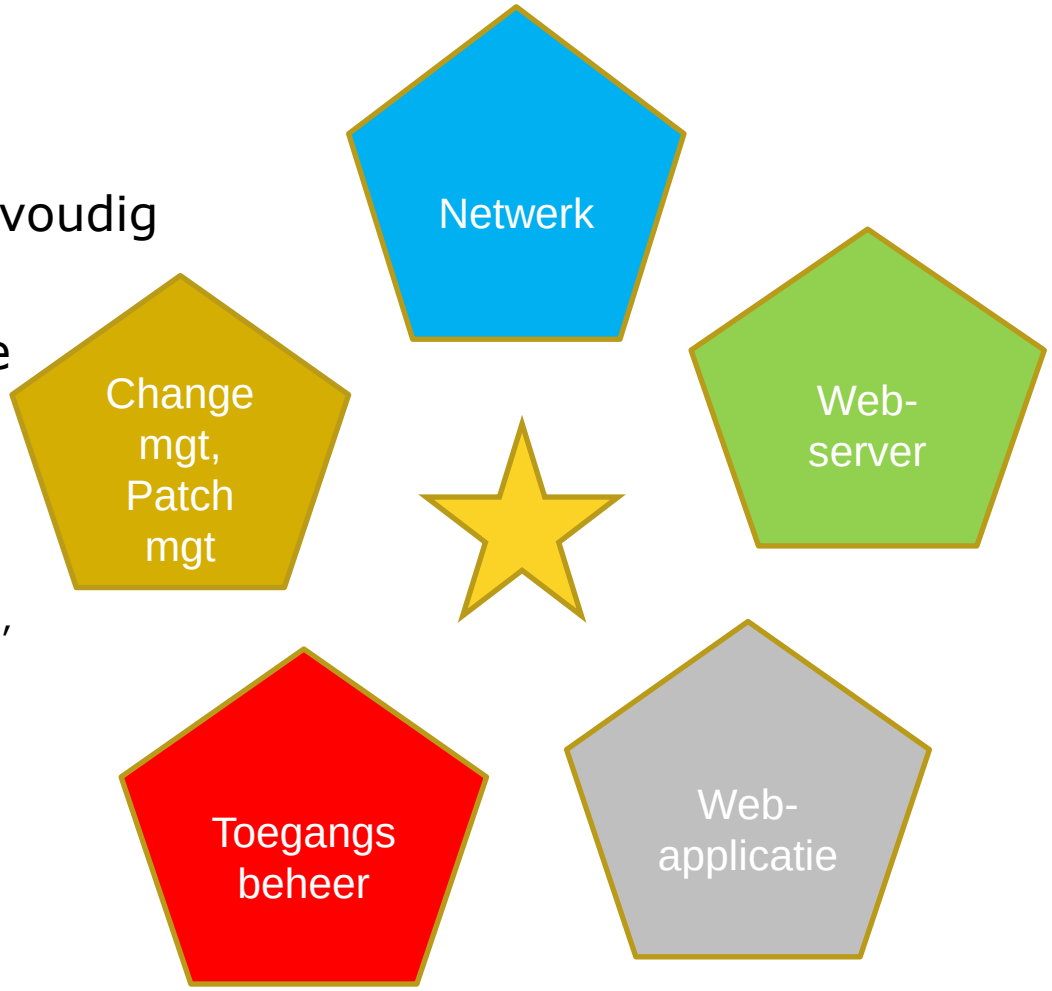
- Het (meervoudig) DigiD assessment is een audit op techniek en processen, met betrekking tot een *specifiek object*, namelijk de (meervoudige) DigiD - aansluiting.
- Het rapport dient *assurance* (zekerheid) te geven over de aantoonbare kwaliteit van de meervoudige aansluiting

(Ter vergelijking: een NEN7510 - certificering betreft het inrichten en onderhouden van een alomvattend ISMS)

Normen op hoofdlijnen

- 20 - tal normen, waarvan vijf aangevuld t.b.v. Meervoudig Assessment
- procedurele en technische aspecten

(beheerprocessen, identiteit - en toegangsmiddelen, configuratiebaseline, hardening, IDS/IPS, logging et cetera)



Normen op hoofdlijnen

- Beoordeling controls naar *opzet* en *bestaan*, dat wil zeggen of zij zijn beschreven en ingericht *en* of er aantoonbaar aan wordt voldaan;
- Voor controls die qua *opzet* als 'voldoende' worden aangemerkt maar waarvan het *bestaan* niet kan worden aangetoond (non - occurence) wordt in het rapport een opmerking geplaatst;
- Waar relevant kan een auditrapportage van een sub-leverancier in de assessment worden betrokken (toepassen carve - out).

Informatie, documenten

Het (Meervoudig) Assessment - uitgebreide informatie en documenten

Informatie over het Meervoudig Assessment:

https://logius.nl/diensten/digid/ict-beveiligingsassessments-digid/het-meervoudig-assessment

Documenten:

DigiD meervoudige assessment overeenkomst Logius en LMA

DigiD Meervoudige assessment - Verplichtingen tussen LMA en AMA (logius.nl)

Aanvragen zelfverklaring ('accreditatie') om Meervoudig Assessment te mogen toepassen:

https://logius.nl/diensten/digid/ict-beveiligingsassessments-digid/documentatie-voor-het-ict-beveiligingsassessments-digid-en-contactgegevens

De Handreiking voor het meervoudig assessment:

Update Handreiking DigiD-assessment met meervoudige aansluitingen 2020, versie 1.0) (norea.nl)

Verdere vragen: axel.vogelzang@minbzk.nl

Verdere vragen over het proces en de normen:
axel.vogelzang@minbzk.nl