Implementatieadvies WDO standaarden

Voor:	Standaardisatieraad
Van:	Architectuurraad Edustandaard
Datum	nov 2020

Aanleiding

Op verzoek van de KRO's heeft de Standaardisatieraad besloten om de WDO beveiligingsstandaarden te volgen. Hierbij zijn 2 verzoeken gedaan. Het eerste verzoek was om de WDO standaarden op te nemen in de ROSA. De tweede vraag was om advies te geven op welke wijze de WDO standaarden geïmplementeerd kunnen worden.

WDO standaarden in de ROSA (vraag 1)

De Standaardisatieraad heeft ingestemd met het eerste verzoek. Op basis van dit verzoek heeft de Architectuurraad een procesvoorstel gedaan voor opstellen van architectuurkaders voor de WDO standaarden waarbij de werkgroep Uniforme beveiligingsvoorschriften wordt belast met de uitvoering van dit proces. Dit voorstel is goedgekeurd door de Standaardisatieraad.
De WDO standaarden worden opgenomen in de ROSA bij de verplichte standaarden. Een standaard is verplicht als dit in de wet is opgenomen of hierover een bestuurlijke afspraak is gemaakt. Een voorbeeld van een wettelijke verplichte standaard zijn de toegankelijks richtlijnen. Scholen moeten deze volgen door Europese regelgeving. De WDO standaarden zijn verplicht voor de overheid door nationale regelgeving. De B-organen (private organen met publieke taak) vallen binnen de scope van de wet maar de B-organen worden niet landelijk aangewezen. Binnen het onderwijsdomein hebben de KRO's de bestuurlijke beslissing genomen de beveiligingsstandaarden te volgen. In de ROSA wordt de volgende toelichting gegeven

- Doel standaard
- Achtergrond van verplichting (wettelijk of bestuurlijke beslissing)
- Datum waarop standaard moet zijn ingevoerd. Bij de WDO standaarden worden de implementatiedata van de overheid overgenomen.
- Werkingsgebied, hier wordt de scope beschreven.
- Toepassingsgebied. Hier wordt aangeven welke processen worden geraakt.

Implementatie WDO standaarden (vraag 2)

De KRO's hebben besloten dat het wenselijk is om zo veel mogelijk aan te sluiten bij de WDO standaarden. Hierbij moet rekening worden naar de context omdat de impact per toepassingsgebied (sector of keten) kan verschillen. Op basis van een analyse moet worden bepaald of, waar en op welke wijze standaarden geïmplementeerd worden. Waarbij per toepassingsgebied andere keuzes gemaakt kunnen worden. De besluitvorming hierover ligt bij de KRO's. Om besluiten te kunnen nemen moeten zij de consequenties kunnen overzien. Daarom hebben zij een implementatieadvies nodig dat verstrekt kan worden door Edustandaard. Bij de implementatie kunnen de volgende rollen worden onderscheiden:

- Kadersteller
  De kadersteller bepaalt op welke wijze aangesloten wordt op de WDO standaarden.
- Regie orgaan
  Het regie orgaan neemt besluit tot implementatie.
- Implementatie orgaan
  Het implementatie orgaan stuurt in opdracht van het regie orgaan op de implementatie.
- Evaluatie orgaan
  Het evaluatie orgaan evalueert in opdracht van het regie orgaan in welke mate afgesproken standaarden daadwerkelijk geïmplementeerd zijn.

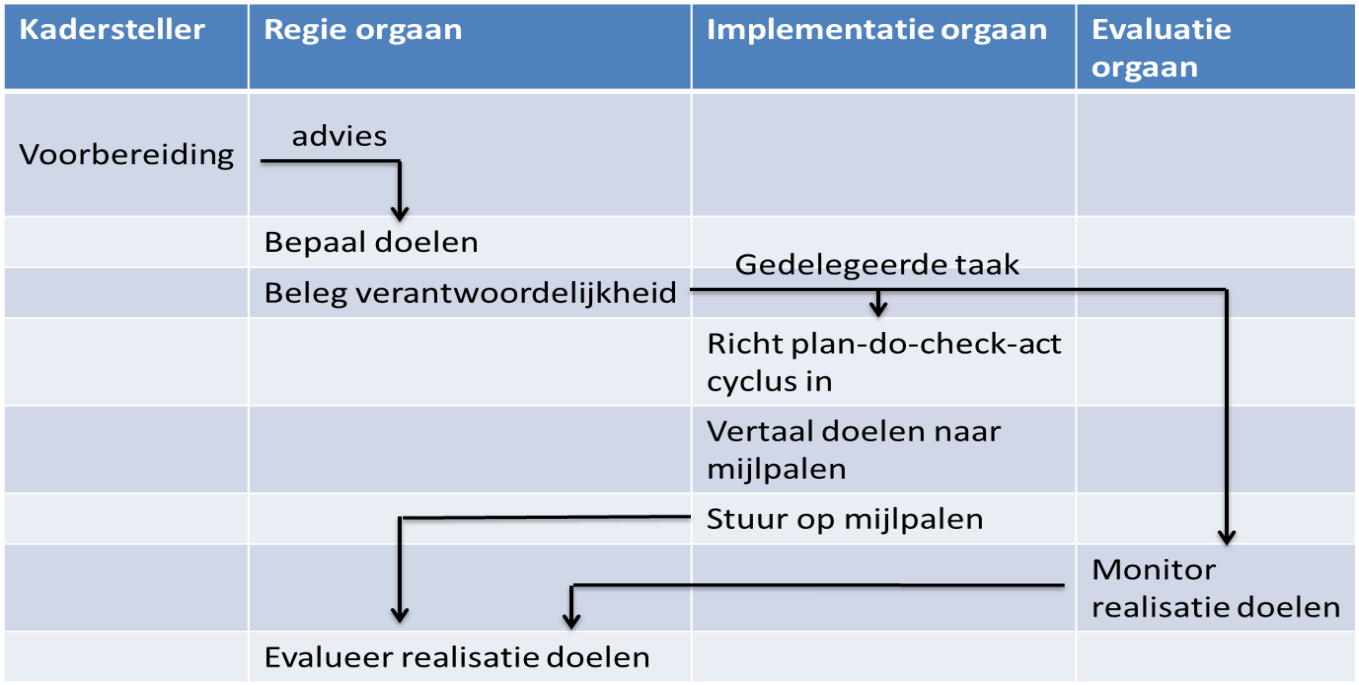
Deze rollen zijn belegd bij verschillende partijen. Voor de implementatie is het nodig dat afspraken worden gemaakt over de taken en verantwoordelijkheden die horen bij een rol. En de wijze waarop interactie tussen deze partijen wordt vorm gegeven.

Edustandaard heeft een advies opgesteld voor de wijze waarop KRO's kunnen sturen op de implementatie van de WDO standaarden. Dit Het advies bestaat uit 3 onderdelen:

- Een voorstel voor de procesflow
  Dit is bedoeld om inzicht te geven in de rolverdeling en de benodigde interactie.
- Toelichting processtappen
  Hier wordt beschreven welke processtappen nodig zijn voor de implementatie en welke principes gebruikt worden bij elke processtap.
- Toelichting inhoudelijke paragraaf
  De inhoudelijke paragraaf geeft per standaard een inhoudelijk advies voor de wijze van implementatie met de consequenties. In dit stuk is een inhoudelijke advies opgenomen voor de TLS standaard en er wordt een vooruitblik gegeven voor de mailstandaarden. Doel is de KRO's voldoende te adviseren om een besluit te kunnen nemen over de TLS standaard. Tevens laat dit zien dat bij verschillende standaarden de consequenties kunnen verschillen. En deze 2 voorbeelden geven meer inzicht in het proces.

Procesflow

Onderstaand schema geeft een beeld van de procesflow, de verantwoordelijkheden en de interactie tussen de betrokkenen.



Procesfasen

Het voorgesteld proces is onderverdeeld in 3 fasen: voorbereiding, realisatie en evaluatie.
In de WDO zullen periodiek nieuwe standaarden worden opgenomen. Bij elke nieuwe standaard zal dit proces opnieuw doorlopen moeten worden. Implementeren van standaarden gebeurt nu ook al, dit geldt ook voor beveiligingsstandaarden.

<u>Voorbereiding</u>

De voorbereiding wordt gedaan door de werkgroep UBV. Het doel is om de veiligheid van de informatiehuishouding te borgen. De beveiligingsstandaarden zijn een middel om dit doel te bereiken. Er moet ook gekeken worden naar de samenhang met andere standaarden en de organisatorische maatregelen. Dit heeft als consequentie dat het implementeren van beveiligingsstandaarden wordt ingebed in grotere werkpakketten die als 1 geheel worden geïmplementeerd. De volgende principes worden gehanteerd bij de voorbereiding:

Principe 1 Koppel standaarden aan doelen

De overheid stuurt op maatschappelijke waarden. De WDO standaarden kunnen gekoppeld worden aan het doel "borgen van veiligheid en continuïteit van de informatievoorziening.

Principe 2 Maak een context specifieke analyse

- Onderscheid toepassingsgebieden
  Voor elk toepassingsgebied kan het nodig zijn een andere implementatiestrategie te hanteren. Bepaal voor welke toepassingsgebieden een analyse moet worden uitgevoerd.
- Voer risico analyse uit. Voer per toepassingsgebied een risico analyse uit. Bepaal het huidige en het gewenste beveiligingsniveau.
- Bepaal de inhoudelijke randvoorwaarden
  Bepaal de randvoorwaarden voor implementatie. Kijk hierbij naar de samenhang met andere standaarden en welke aanpassingen aan processen en informatievoorziening nodig zijn om het gewenste beveiligingsniveau te bereiken. Deze samenhang wordt geborgd met een beveiligingsbaseline, de Rijksoverheid gebruikt hiervoor de BIO, binnen het onderwijsdomein wordt hiervoor het certificeringsschema IBP gebruikt. Het certificeringsschema geeft invulling aan de beveiligingsmaatregelen van de modelverwerkersovereenkomst van het Privacyconvenant. De WDO standaarden worden opgenomen in het certificeringsschema. Het object van implementatie is een nieuwe versie van het certificeringsschema, met alle onderliggende standaarden.
- Bepaal de prioriteit voor de implementatie. Voor elk toepassingsgebied wordt bepaald welke urgentie de implementatie heeft. Dit wordt bepaald door het verschil tussen het gewenste beveiligingsniveau en het huidige beveiligingsniveau. Dit bepaalt het beveiligingsrisico, dit wordt afgezet tegen de kosten die gepaard gaan met de implementatie. Daarnaast wordt gekeken naar het verandervermogen van de organisatie. Het verandervermogen wordt mede bepaald door het totaalpakket aan veranderingen die een organisatie binnen een bepaald tijdsbestek moet realiseren.
- Bepaal stuurmogelijkheden op de implementatie
  De mate waarin gestuurd kan worden op de implementatie verschilt per toepassingsgebied en soms per organisatie. Hierbij kan gebruik worden gemaakt om een logische fasering in de implementatie aan te brengen. DUO zal als A-orgaan WDO standaarden sneller moeten implementeren en zal de betreffende standaarden in al haar uitwisselingen met ketenpartijen verplicht zal stellen. Omdat die ketenpartijen het daarmee al beschikbaar hebben, kunnen ze het makkelijker toepassen in andere uitwisselingen. De context van OSO kent een goed georganiseerde governance met sterke vertegenwoordiging vanuit het publieke domein en ook hier is de verwachting dat het snel doorvoeren van afgesproken standaarden op draagvlak kan rekenen. Een vergelijkbare redenering geldt voor uitwisselingen van het OSR (Onderwijs serviceregister) van Kennisnet, deze zal snel de nieuwe beveiligingsstandaarden adopteren en dus ook hanteren in alle uitwisselingen. Ketens waar minder regie is vanuit het publieke domein bijv. leermiddelenketens zijn afhankelijk van de mate waarop hier regie kan worden uitgevoerd
- Analyseer belemmeringen en overtuigingen die adoptie in de weg kunnen staan. Binnen een toepassingsgebied kunnen maatregelen zijn getroffen die wel de veiligheid in betreffende keten kunnen garanderen maar waarvoor andere standaarden zijn gebruikt. Dat maakt uitwisseling met andere domeinen minder voorspelbaar en hierdoor minder veilig. Er is een verschil tussen een lokaal belang en het stelselbelang.
- Maak een implementatieadvies met voorstellen voor realisatie en evaluatie

Realisatie

Op basis van het implementatie advies besluiten de KRO's of en op welke wijze een standaard geïmplementeerd wordt. De KRO's stellen de doelen vast die bereikt moeten worden.

Bij standaarden die geïmplementeerd moeten worden bepalen de KRO's:

1. Op welke wijze gestuurd zal worden op de implementatie
2. Op welke wijze geëvalueerd wordt of de doelen bereikt worden

De benodigde implementatie inspanning kan per standaard sterk verschillen. Bij implementaties met geringe impact is geen projectsturing nodig, het reguliere standaardisatieproces volstaat. De rol van de KRO's blijft beperkt tot het vaststellen van de implementatie doelstelling en de communicatie hier over. Wanneer de consequenties groter zijn kunnen de KRO's besluiten dat projectsturing nodig is. In dit geval moeten de KRO's de verantwoordelijkheid voor de implementatie beleggen bij een implementatie orgaan.

Voor de realisatie fase wordt voorgesteld de volgende principes te hanteren:

Principe 1 stel doelen vast

Principe 2 Beleg verantwoordelijkheid voor implementatie
De implementatieverantwoordelijkheid kan per toepassingsgebied verschillen. Beleg de verantwoordelijkheid voor de implementatie binnen een toepassingsgebied.

Principe 3 Beleg verantwoordelijkheid voor monitoring
Maak duidelijk welk evaluatie orgaan verantwoordelijk is voor de monitoring die nodig is om vast te stellen of de doelen gerealiseerd zijn.

Principe 4 Richt plan-do-check act cyclus in voor implementatie.
Het implementatie orgaan richt een plan-do-check act cyclus in om te sturen op de implementatie.

Principe 5 Koppel mijlpalen aan doelen
Het implementatie orgaan bepaalt welke mijlpalen nodig zijn om de doelen te realiseren en bepaalt doorlooptijd en kosten per mijlpaal.

Principe 6 Stuur op mijlpalen
Het implementatieorgaan stuurt op de mijlpalen en rapporteert over de voortgang en kosten.

Principe 7 Evalueer realisatie doelen
Het regie orgaan evalueert op welke wijze de doelen worden gerealiseerd aan de hand van de project voortgang.

Evaluatie

Voor monitoren van de realisatie van doelen kan gekozen worden tussen verschillende instrumenten. In deze paragraaf worden een aantal alternatieven beschreven. In het implementatieadvies wordt ook aandacht besteed aan de wijze van evaluatie.

Principe 1 Bepaal op welke wijze gemonitord wordt in welke mate doelen worden bereikt.
Hieronder zijn een aantal opties voor evaluatie. Hierbij is gekeken naar de wijze waarop evaluatie binnen de overheid wordt uitgevoerd. Voor het onderwijs moet nog gestart worden met evaluatie. Daarom wordt geadviseerd te starten met een lichte vorm van regie. En te werken aan een stapgewijze professionalisering. Hieronder wordt een toegelichting gegeven op de diverse opties voor monitoring:

- Softwarecatalogus
  Een softwarecatalogus kan inzicht bieden in de mate waaraan een leverancier aandacht besteed aan veiligheid. Het voorstel is dat te doen op basis van het certificeringsschema. Waardoor een instelling kan zien welke leveranciers zich committeren aan het certificeringsschema.
- Opnemen standaarden in de inkoopvoorwaarden
  In de inkoopvoorwaarden kan de eis worden opgenomen dat wordt aangesloten op het certificeringsschema. Op basis van de inkoopvoorwaarden kan bepaald worden of een instelling hier naar vraagt of niet.
- Motiveren afwijking in jaarverslag (comply or explain)
  In de jaarplan richtlijnen kan worden opgenomen dat als verplichte standaarden niet gevolgd worden dit in het jaarverslag gemotiveerd moet worden. Dit speelt vooral als bij nieuwe projecten verplichte standaarden niet zijn opgenomen in de inkoopvoorwaarden. Evaluatie is mogelijk door op basis van de jaarverslagen te monitoren wanneer wordt afgeweken. Hiermee wordt de verantwoordelijkheid voor de implementatie ook expliciet belegd bij een instelling. Er is een duidelijk kader dat aangeeft welke standaarden de instelling moet implementeren. Tevens is aangegeven dat de consequentie is dat de instelling middels de inkoopvoorwaarden aan de leverancier moet vragen om dit te doen. Bij gebruik van standaard inkoopvoorwaarden zoals die van SIVON hoeft de instelling geen technische kennis te hebben. Als de instelling hier bewust van afwijkt neemt ze hiervoor ook de bestuurlijke verantwoordelijkheid door dit te motiveren in het jaarverslag.
- Monitoring door meting
  Implementatie van standaarden kan niet volledig gevolg worden middels de inkoopvoorwaarden. Er is niet altijd sprake van een inkooptraject. Bijvoorbeeld omdat de standaard vraagt om beheerinstellingen op een specifieke manier te configureren. Bij sommige standaarden kan monitoring plaatsvinden door metingen. Hiermee kan een volledig beeld van de actuele situatie worden verschaft.
- Monitoring door enquête
  Middels een enquête kan instellingen worden gevraagd of ze standaarden kennen en implementeren. Nadeel hiervan is dat de respons op enquêtes laag is. En dat op schoolniveau vaak de kennis van standaarden onvoldoende is om antwoord te kunnen geven op de implementatie van specifieke standaarden. Er moeten dan meer generieke vragen worden gesteld. Of er wordt aan leveranciers gevraagd in welke mate zijn verplichte standaarden volgen.

Inhoudelijke paragraaf

De Wet Digitale Overheid stelt een aantal standaarden op gebied van informatieveiligheid verplicht. In deze paraaf wordt per standaard beschreven wat de impact is en waarmee rekening gehouden moet worden met de implementatie.

Toelichting op rol werkgroep UBV
In het voorgestelde proces is de Edustandaard werkgroep UBV verantwoordelijk voor:

- Analyse
  Bij de analyse wordt bepaald hoe de standaard aansluit op de onderwijscontext
- Opstellen kaders
  Op basis van de analyse bepaalt de werkgroep UBV waar en op welke wijze de standaard geimplementeerd moet worden
- Bepalen globale impact
  De werkgroep maakt een inschatting van de globale impact van de implementatie van de kaders

De werkgroep heeft conform deze rol een analyse gedaan op de TLS standaard en een eerste verkenning voor de mailstandaarden. Hieronder wordt een inhoudelijke duiding gegeven op de TLS standaard en wordt een vooruitblik gedaan op de mailstandaarden

Implementatieadvies TLS

Analyse
De standaard TLS is bedoeld om een beveiligd transport te bieden bij machine koppelingen
De aangewezen standaarden (HTTPS, HTST en TLS) zijn geschikt om de veiligheid te borgen maar laten ruimte voor eigen interpretatie waardoor problemen kunnen ontstaan bij de samenwerking. Voor het onderwijsdomein zijn aanvullende maatregelen nodig..

Opstellen kaders
De werkgroep UBV heeft kaders opgesteld die aangeven hoe de standaarden geïmplementeerd moeten worden. In de huidige situatie is dat een advies aan applicatie leveranciers hoe zij de standaard moeten toepassen. Verwachting is dat op korte termijn een definitieve versie van deze standaard kan worden vastgesteld. Het kader voor gebruik TLS zal opgenomen worden in het certificeringsscha.

Globale impact
Bij de implementatie van de TLS standaard kan meegelift worden op de volgende ontwikkelingen:

<u>Machine-machine koppelingen op basis van Edukoppeling</u>
Gebruik van Edukoppeling vereist dat het certificeringsschema is ondertekend en Edukoppeling zal gebruikt gaan maken van TLS. Alle gegevensuitwisselingen die gebruik maken van Edukoppelingen worden daarmee automatisch compliant met de UBV TLS afspraken.

<u>Grote browserleveranciers gaan TLS gebruiken voor HTTPS</u>
Organisaties die een beveiligde website beheren ontkomen er niet aan TLS te gebruiken,

Veel leveranciers gaan al over op TLS, mede ook door bovengenoemde ontwikkelingen. Dit geldt echter nier voor alle leveranciers. Daarnaast moet niet alleen TLS worden geïmplementeerd maar ook voldaan worden aan de eisen van het certificeringsschema.

De impact zit vooral bij de leveranciers die niet vrijwillig aansluiten bij het certificeringsschema.

Monitoren en meten
De werkgroep UBV heeft een adviesrol. Leveranciers bepalen zelf hoe zij omgaan met het certificeringsschema. deze ook werkelijk toepassen.

Bij leveranciers die het privacy convenant hebben ondertekend doen een self assesment en stellen een pas-toe-leg-uit verklaring op in de beveiligingsbijlage van de verwerkersovereenkomst. Tenminste voor toepassingen die binnen de scope van het Privacy convenant vallen. Voor toepassingen die daar buiten vallen bestaan nog geen afspraken.

Er is ook geen register van toepassingen waarin wordt bijgehouden of deze compliant zijn aan de van toepassing zijn beveiligingsstandaarden en afspraken. Het is hierdoor voor instellingen niet makkelijk verifieerbaar welke toepassingen voldoende waarborgen bieden voor privacy en beveiliging. Momenteel wordt wel gewerkt aan instrumenten die hier ondersteunde in zouden kunnen zijn. Binnen het funderend onderwijs is in het kader van een referentie architectuur, de FORA gewerkt de behoefte geuit aan een softwarecatalogus. Idee van deze softwarecatalogus is dat toepassingen die in het funderend onderwijs worden gebruikt hierin worden geregistreerd om compliancy aan de referentie architectuur te kunnen valideren. Deze tool zou mogelijk ook ingezet kunnen worden om compliancy aan Certificeringsschema en WDO standaarden te kunnen registreren.

Opbouwen draagvlak
Er moet draagvlak worden opgebouwd om de stap te zetten van vrijblijvende adviezen naar regie op het implementeren van kaders. Hierbij kan gebruik worden gemaakt van al lopende initiatieven. Door gebruik te maken van leveranciers die op vrijwillige wijze al het certificeringsschema ondertekenen en grote schoolbesturen die al samenwerken binnen de FORA om te komen tot een software catalogus. De sectorraden kunnen hiervan gebruik maken voor bewustwording van alle instellingen dat dit belangrijk is en dat het een gemeenschappelijk belang is om hier gemeenschappelijke afspraken over te maken.

Implementatieadvies e-Mail standaarden

De WDO stelt bij gebruik van mail de standaarden SPF, DKIM, DMARC, STARTTTLS en DANE verplicht.

Analyse
De emailstandaarden SPF, DKIM & DMARC zijn het meest effectief als ze gezamenlijk worden gebruikt. Deze standaarden vergroten gezamenlijk de afleverbetrouwbaarheid van email:

- Legitieme e-mailberichten worden niet meer onterecht als SPAM wordt aangemerkt
- Beperken risico's van misbruik (e-mail)domeinnaam door derden (phishing).

Zowel bij ingaand als bij uitgaand mailverkeer is er impact:

Uitgaand verkeer
De standaarden moeten goed worden toegepast anders wordt legitieme e-mail niet meer afgeleverd

Ingaand verkeer
De ontvangende partij moet controleren, er moet filtering op ingaand verkeer worden ingesteld.

Deze standaarden zijn pas effectief als ze breed worden toegepast. Waarbij een stapgewijze implementatie nodig is om geleidelijk ervaring met de standaard op te doen. De geleidelijke invoering geldt vooral voor de ontvangende kant. Bijvoorbeeld door wel te starten met analyseren maar nog niet met filteren

Kaders
Op basis van deze analyse gaat de werkgroep UBV kaders opstellen voor veilig en betrouwbaar e-mail verkeer. Deze afspraak bevat een nadere duiding van de standaarden en best practices voor implementatie.

Implementatie
Afspraken voor ketenbreed toepassen van deze afspraken zijn er nog niet.
Geadviseerd wordt om te beginnen met het adviseren van deze standaarden maar nog niet te verplichten. De reden is dat grote mailproviders (zoals Microsoft 365) de standaard op dit moment nog niet of maar beperkt ondersteunen. Organisaties dwingen om aan deze standaard te voldoen gaat daarmee voor problemen zorgen aangezien dit zou betekenen dat ze van mailprovider moeten wisselen.

De werkgroep UBV zal deze standaarden blijven volgen om te bepalen wat het juiste moment is om over te gaan van adviseren naar verplichten. Dit wordt mede bepaald door het moment dat grote leveranciers als Microsoft overstappen.

Monitoren en meten
De website internet.nl kan gebruikt worden voor zelf assessment door onderwijs instelling of leverancier. Hiermee kan gecontroleerd worden in hoeverre aan de standaarden wordt voldaan. Wanneer ketenbreed wordt afgesproken om dit te doen en de bevindingen te delen wordt hiermee inzicht verkregen in de implementatiegraad van de standaarden.