Expertadvies SBOM

Aan:	Forum Standaardisatie
Van:	InnoValor Advies B.V.
Datum:	28 juli 2026
Versie:	1.0
Bijlagen:	geen

1 Advies

De experts die betrokken waren bij het expertonderzoek adviseren om de standaarden CycloneDX versie 1.7 en Software Package Data Exchange (SPDX) versie 2.2 onder de registratie SBOM te verplichten (‘Pas toe of leg uit’) aan de overheid via plaatsing op de ‘Pas toe of leg uit’-lijst van het Forum Standaardisatie.

Het opgestelde functioneel toepassingsgebied voor SBOM is:

> *CycloneDX of SPDX moeten worden toegepast op software die de overheid zelf ontwikkelt, laat ontwikkelen, inkoopt of als onderdeel van een dienst afneemt.*

Een SBOM (Software Bill of Materials) is een overzicht van alle onderdelen waaruit software is opgebouwd. Dit kunnen softwarecomponenten, bibliotheken, frameworks en andere afhankelijkheden zijn die onderdeel uitmaken van een softwareproduct. CycloneDX en SPDX zijn standaarden die deze informatie op een machineleesbare wijze vastleggen.

De indiener heeft voor de invulling van een SBOM twee open standaarden aangemeld, die ook zijn getoetst in het expertonderzoek: CycloneDX versie 1.6, beheerd door de Open Worldwide Application Security Project (OWASP), en SPDX versie 2.2, beheerd door The Linux Foundation.

De experts adviseren echter om CycloneDX versie 1.7 verplicht te stellen (‘Pas toe of leg uit’) aan de overheid in plaats van versie 1.6 die de indiener oorspronkelijk had aangemeld. Volgens de experts zijn de wijzigingen in versie 1.7 beperkt ten opzichte van versie 1.6 en hebben deze geen gevolgen voor de conclusies van de toetsing. Daarnaast adviseren de experts om het profiel van het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) te gebruiken als invulling van een functioneel doel en om duidelijkheid te bieden over

de wijze waarop een SBOM wordt ingevuld. Daarbij blijft de toepassing minimaal verplicht beperkt tot de hiervoor beschreven source- en build-SBOM-typen.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte beschrijving van het nut en belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 geeft de samenstelling van de expertgroep weer. Hoofdstuk 5 documenteert hoe de experts de standaard beoordelen op basis van de inhoudelijke hoofdcriteria voor opname op de 'Pas toe of leg uit'-lijst of lijst aanbevolen standaarden. Tot slot geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De aangemelde standaarden CycloneDX 1.6 en SPDX 2.2 zijn beide SBOM-standaarden. Een SBOM is een overzicht van alle onderdelen waaruit software is opgebouwd. Dit kunnen softwarecomponenten, bibliotheken, frameworks en andere afhankelijkheden zijn die onderdeel uitmaken van een softwareproduct. CycloneDX en SPDX zijn standaarden waarmee deze informatie op een machineleesbare wijze kan worden vastgelegd. Beide standaarden ondersteunen daarbij onder meer de reeds door Forum Standaardisatie aanbevolen JavaScript Object Notation (JSON)-standaard voor de uitwisseling van SBOM-informatie.

Beide standaarden kunnen specificeren hoe informatie over softwarecomponenten, versies, relaties tussen componenten en licenties moet worden beschreven. Hierdoor ontstaat inzicht in de opbouw van softwareproducten en de afhankelijkheden waarvan deze gebruikmaken.

CycloneDX 1.6 en SPDX 2.2 hebben ieder een eigen oorsprong: CycloneDX 1.6 is van oorsprong ontwikkeld om inzicht te bieden in informatiebeveiligingsrisico's binnen de softwareketen, terwijl SPDX 2.2 is ontstaan om inzicht te bieden in gebruikte open source licenties en softwarecomponenten. Hoewel beide standaarden vanuit verschillende doelen zijn ontwikkeld, groeien zij steeds meer naar elkaar toe. Om die reden worden ze in dit expertadvies gezamenlijk beschouwd. Vanwege de mogelijke overlap in functionaliteit tussen de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2, en indien beide standaarden een 'Pas toe of leg uit'-verplichting krijgen toegekend, is het aan de inkopende organisatie om te bepalen welke standaard het beste aansluit bij de specifieke toepassing en situatie.

De toepassing van de standaarden kan plaatsvinden in verschillende fasen van het proces: van het ontwikkelen van digitaal werk tot het gebruiken en bekijken ervan. Om de invulling van een SBOM eenduidig te maken, wordt voorgesteld om het profiel van het Duitse BSI te volgen. Dit profiel geeft invulling aan een functioneel doel en biedt duidelijkheid over de wijze waarop een SBOM wordt ingevuld. Hierin zijn twee SBOM-typen beschreven: de source-SBOM en de build-SBOM. Deze vormen de minimale verplichting; het gebruik van aanvullende SBOM-typen blijft uiteraard mogelijk.

- Source SBOM: een Source SBOM geeft inzicht in de softwarecomponenten en afhankelijkheden die tijdens de ontwikkeling van digitale software worden gebruikt. Het beschrijft de bestanden in de code repository en alle afhankelijkheden die binnen de scope van de ontwikkeltools en -straat in eigen beheer nodig zijn om digitaal werk te ontwikkelen. Afhankelijkheden die doelplatformspecifiek door package managers worden binnengehaald, vallen buiten de scope.
- Build SBOM: een Build SBOM geeft inzicht in de softwarecomponenten die in een gebouwde versie van digitale software zijn geïntegreerd. Het beschrijft alle componenten die in een digitaal werk in hun binary- of blobverschijningsvorm zijn geïntegreerd, zoals static-linked libraries. Het betreft afhankelijkheden die tijdens de runtime niet meer nodig zijn om het digitale werk te gebruiken.

De SBOM wordt zo volledig mogelijk opgesteld met een redelijke inspanning. Daarbij worden minimaal de directe (eerste laag van) afhankelijkheden opgenomen. Waar mogelijk worden ook verderliggende afhankelijkheden vastgelegd. Dit betreft zowel de diepte van de afhankelijkhedenstructuur als de mate waarin informatie over componenten wordt vastgelegd.

2.2 Waarom is deze standaard belangrijk?

Als SBOM-standaarden bieden CycloneDX 1.6 en SPDX 2.2 inzicht in de samenstelling van een softwareproduct, hetgeen bijdraagt aan transparantie, hergebruik, veiligheid en beheer van deze producten. Deze stellen organisaties in staat om naleving van licenties en regelgeving beter te waarborgen, het hergebruik van componenten te beoordelen, afhankelijkheden in kaart te brengen en sneller te reageren op veiligheidsincidenten rond componenten.

Veiligheid en risicobeheersing: Het komt regelmatig voor dat ernstige kwetsbaarheden in componenten worden aangetroffen. Dat kan als gevolg hebben dat softwareproducten die een dergelijke component gebruiken, zelf ook kwetsbaar zijn. Alle softwareproducten die dit component gebruiken, moeten worden geïdentificeerd, zodat passende maatregelen kunnen worden genomen. CycloneDX en SPDX versnellen dit proces dankzij het geboden inzicht. Wanneer ze in een doorzoekbaar register beschikbaar zijn, kan bij het bekend worden van een kwetsbaarheid de geraakte softwarecomponent direct worden achterhaald.

Naleving van wet- en regelgeving: Er gelden wettelijke verplichtingen, zoals de Wet hergebruik van overheidsinformatie (Who), die instellingen met een publieke taak verplichten overheidsinformatie open en herbruikbaar beschikbaar te stellen. Om hier invulling aan te geven en te voldoen aan cybersecurity- en informatiebeveiligingsverplichtingen (onder andere de Europese Network and Information Security Directive (NIS2) en de Cyber Resilience Act (CRA)), is inzicht in de softwarecomponenten essentieel. Een SBOM is hierbij een belangrijke bouwsteen voor risicobeheersing, compliance en supply chain security, zoals ook beschreven staat in de SBOM-startersgids van het NCSC.

Inzicht in softwarecomponenten en licenties: Om dit met de juiste zorgvuldigheid vorm te geven, is het nodig inzicht te hebben in de componenten waaruit het softwareproduct is opgebouwd. Van elk van de componenten moet men controleren onder welke licenties ze zijn vrijgegeven. Met CycloneDX en SPDX wordt het eenvoudiger om inzicht te krijgen in de componenten waaruit een softwareproduct is opgebouwd.

Transparantie, hergebruik en vertrouwen: Toepassing van een SBOM-standaard kan met het geboden inzicht ook het vertrouwen in het softwarelandschap versterken, wat belangrijk is in een tijd waarin software in grote mate afhankelijk is van open source componenten en componenten van derden. Voor het daadwerkelijk hergebruik van overheidssoftwareproducten helpt het wanneer anderen kunnen zien uit welke componenten deze zijn opgebouwd. Met het geboden inzicht dat CycloneDX en SPDX bieden kan bepaald worden of de software en/of de componenten compliant zijn met de daarvoor vastgestelde regels. Dit maakt het voor derden makkelijker om de herbruikbaarheidswaarde van door de overheid ontwikkelde software te bepalen. Datzelfde geldt ook bij het gebruik van open source software en/of componenten. Ook voor de overheid wordt het makkelijker om deze aan de eigen compliance regels te toetsen.

3 Betrokkenen en proces

Op 25 juni 2024 heeft Maurice Hendriks (Ministerie van Volksgezondheid, Welzijn en Sport) de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2 aangemeld voor registratie onder SBOM voor toetsing om deze te verplichten (‘Pas toe of leg uit’) aan de overheid. Deze aanmelding is mede ondersteund door Karel Rietveld (Belastingdienst) en Leon C. Roeleveld (UWV).

Op 7 november 2024 heeft een intakegesprek plaatsgevonden met de indiener, de procedurebegeleider en Bureau Forum Standaardisatie. In dit gesprek werd verkend of SBOM voldoet aan de criteria om in procedure te worden genomen. De resultaten van het onderzoek zijn vastgelegd in het intakeadvies. Op basis van dit intakeadvies heeft het Forum Standaardisatie op 25 juni 2025 besloten om de procedure tijdelijk te pauzeren.

De aanleiding hiervoor was onduidelijkheid over de Europese normering binnen het kader van de CRA. Het was destijds onzeker of CycloneDX en SPDX zouden aansluiten bij de toekomstige geharmoniseerde Europese standaarden. Inmiddels heeft NEN een draft gepubliceerd van een geharmoniseerde norm ter ondersteuning van de CRA. In dit concept worden CycloneDX en SPDX expliciet genoemd als gangbare formaten. Belangrijk is dat er geen alternatieve of concurrerende standaarden exclusief worden voorgeschreven. Hiermee is de grondslag voor de eerdere pauzering komen te vervallen, waarna op 8 april 2026 is besloten de toetsingsprocedure te hervatten.

Vervolgens heeft de procedurebegeleider na raadpleging van Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld om de standaard in een expertsessie nader te bespreken.

Voorafgaand aan de expertbijeenkomst ontvingen de leden van de expertgroep een concept-expertadvies gekregen dat was samengesteld met informatie uit de aanmelding en het intake-onderzoek.

De leden van de expertgroep kwamen op 25 juni 2026 bijeen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Doordat niet alle geïnventariseerde inhoudelijke bespreekpunten binnen de beschikbare tijd van de eerste expertbijeenkomst konden worden behandeld, werd besloten een vervolgexpertbijeenkomst te organiseren. Deze bijeenkomst vond plaats op 2 juli 2026 en bood ruimte om de overgebleven onderwerpen zorgvuldig te bespreken en een inhoudelijk volledig en zorgvuldig proces te waarborgen.

Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies werd extra aandacht besteed aan de volgende punten:

1. Aandacht voor de vraag in hoeverre CycloneDX 1.6 en SPDX 2.2 de meest geschikte standaarden zijn voor het uitwisselen van SBOMs, mede gezien de lopende ontwikkelingen rondom de toepassing van deze standaarden;
2. Aandacht voor de vraag of een Nederlands profiel noodzakelijk is voor de toepassing van de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2;
3. Aandacht voor de vraag in hoeverre het Duitse BSI-profiel voor de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2 als referentie kan dienen en in Nederland kan worden overgenomen;
4. Aandacht voor het beleggen van de regierol voor de standaarden CycloneDX 1.6 en SPDX 2.2 bij een geschikte nationale organisatie, ter bevordering van de adoptie in Nederland en de vertegenwoordiging van Nederlandse belangen bij de doorontwikkeling.
5. Aandacht voor de vraag hoe om te gaan met de mogelijke overlap in functionaliteit tussen de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2 en hoe wordt bepaald welke standaard voor welke toepassing het meest passend is, indien beide standaarden een ‘Pas toe of leg uit’-verplichting krijgen.

Daarnaast werd tijdens de toetsingsprocedure een nieuwe versie van CycloneDX (versie 1.7) gepubliceerd. De huidige aanmelding was gebaseerd op CycloneDX versie 1.6, waardoor de toetsing formeel op deze versie is uitgevoerd. De experts adviseren echter om CycloneDX versie 1.7 verplicht te stellen (‘Pas toe of leg uit’) aan de overheid in plaats van versie 1.6. Volgens de experts zijn de wijzigingen in versie 1.7 beperkt ten opzichte van versie 1.6 en hebben zij geen gevolgen voor de conclusies van de toetsing. Tijdens deze bijeenkomst werden ook het functioneel toepassingsgebied en het organisatorisch werkingsgebied opgesteld.

Dit expertadvies geeft de uitkomsten van de expertsessies weer. Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie op de website van Internetconsultatie. Gedurende de consultatieperiode kan iedereen reageren op het expertadvies.

Na afsluiting van de openbare consultatie ontvangen de leden van de expertgroep en de indiener een terugkoppeling over de reactie(s).

4 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een samenstelling van de expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt. De deelnemers hebben ingestemd met het vermelden van hun voornaam, achternaam en organisatie.

Aan de expertbijeenkomst hebben de volgende personen deelgenomen:

- Maurice Hendriks (VWS - Indiener)
- Gerrit Berkouwer (AZ/DPC)
- Rutger Gerritsen (PSG technauts)
- Floris Hendriks (RDI)
- Hidde-Jan Jongsma (TNO)
- Jan Klopper (Geonovum)
- Shakha Mirza (Gemeente Den Haag)
- Eric Nieuwland (ICTU)
- Wim de Rave (JenV)
- Leon Schipper (Gemeente Rotterdam)
- Maikel Severins (Belastingdienst)
- Thomas Steenbergen (Liaison voor het CycloneDX- en SPDX-coreteam)
- Christian Veenman (NCSC)

De volgende personen waren telefonisch beschikbaar:

- Anne Jan Brouwer (VWS - Indiener)
- Jeroen Dekkers (VWS - Indiener)

Als onafhankelijk voorzitter is opgetreden Claudia Vermeulen, Managing Partner bij InnoValor Advies.

Ruud Kosman, Managing Partner, en Aday Destici, Projectondersteuner bij InnoValor Advies, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Wouter Kobes en Joram Verspaget van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

Doordat niet alle geïnventariseerde inhoudelijke bespreekpunten binnen de beschikbare tijd van de eerste expertbijeenkomst konden worden behandeld, is besloten een vervolgexpertbijeenkomst te organiseren. Deze bijeenkomst vond plaats op 2 juli 2026 en bood ruimte om de overgebleven onderwerpen zorgvuldig te bespreken en een inhoudelijk volledig en zorgvuldig proces te waarborgen.

Aan de vervolgexpertbijeenkomst hebben de volgende personen deelgenomen:

- Maurice Hendriks (VWS - Indiener)
- Gerrit Berkouwer (AZ/DPC)
- Rutger Gerritsen (PSG technauts)
- Floris Hendriks (RDI)
- Hidde-Jan Jongsma (TNO)
- Jan Klopper (Geonovum)
- Shakha Mirza (Gemeente Den Haag)
- Eric Nieuwland (ICTU)
- Leon Schipper (Gemeente Rotterdam)
- Thomas Steenbergen (Liaison voor het CycloneDX- en SPDX-coreteam)

De volgende personen waren telefonisch beschikbaar:

- Anne Jan Brouwer (VWS - Indiener)
- Jeroen Dekkers (VWS - Indiener)

Als onafhankelijk waarnemend voorzitter is opgetreden Ruud Kosman, Managing Partner bij InnoValor Advies.

Aday Destici, Projectondersteuner bij InnoValor Advies, heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Wouter Kobes en Joram Verspaget van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

5 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier inhoudelijke hoofdcriteria om te bepalen of een standaard in aanmerking komt voor verplichten (‘Pas toe of leg uit’) of aanbevelen aan de overheid via plaatsing op ‘Pas toe of leg uit’-lijst of lijst aanbevolen standaarden van het Forum Standaardisatie:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Bevordert opname van de standaard op de ‘Pas toe of leg uit’-lijst de adoptie?

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan op de website van het Forum Standaardisatie. Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing.

5.1 Toegevoegde waarde

Met dit criterium wordt bepaald of het toepassingsgebied van de standaard duidelijk is, of deze zich goed verhoudt tot andere standaarden die al dan niet op de lijst staan, of de standaard een duidelijke meerwaarde heeft en of deze opweegt tegen eventuele risico’s en nadelen.

5.1.1 Waardering van het criterium criteria 'Toegevoegde waarde'

De experts komen tot de conclusie dat SBOM voldoet aan het criterium 'toegevoegde waarde'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.1.2 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.2.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Het opgestelde functioneel toepassingsgebied voor SBOM op de 'Pas toe of leg uit'-lijst is:

> *CycloneDX of SPDX moet worden toegepast op software die de overheid zelf ontwikkelt, laat ontwikkelen, inkoopt of als onderdeel van een dienst afneemt.*

De experts oordelen dat dit functioneel toepassingsgebied voldoende duidelijk is en het verplichte gebruik van de standaard eenduidig beschrijft.

Onderstaande toelichting verduidelijkt de afbakening van het functioneel toepassingsgebied.

De standaarden CycloneDX en SPDX ondersteunen menselijke controle op beveiligingsrisico's, privacyrisico's en licentievoorwaarden doordat zij softwarecomponentinformatie machineleesbaar en herleidbaar vastleggen.

De standaarden kunnen voor uiteenlopende functionele doelen worden toegepast. Voorbeelden hiervan zijn het machineleesbaar vastleggen, uitwisselen, valideren en beheren van softwarecomponentinformatie voor ICT-producten en ICT-diensten ter ondersteuning van beveiligings-, beheer- en complianceprocessen.

Vanwege de mogelijke overlap in functionaliteit tussen de SBOM-standaarden CycloneDX 1.7 en SPDX 2.2, en indien beide standaarden een 'Pas toe of leg uit'-verplichting krijgen toegekend, is het conform het opgestelde functioneel toepassingsgebied aan de inkopende organisatie om te bepalen welke van de twee standaarden het beste aansluit bij de specifieke toepassing en situatie.

Daarbij is het BSI-profiel voorgesteld als invulling van een functioneel doel en om duidelijkheid te bieden over de wijze waarop een SBOM wordt ingevuld. Daarbij blijft de toepassing minimaal verplicht beperkt tot de hiervoor beschreven source- en build-SBOM-typen.

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het opgestelde organisatorisch werkingsgebied voor SBOM op de 'Pas toe of leg uit'-lijst is:

> *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.*

Dit is het gangbare organisatorisch werkingsgebied voor standaarden op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.

5.1.2.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)?

Ja, de standaarden kunnen over de grenzen van organisaties of sectoren worden gebruikt en zijn niet alleen bedoeld voor gegevensuitwisseling binnen één organisatie of sector.

5.1.3 Verhoudt de standaard zich goed tot andere standaarden?

5.1.3.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast?

Ja, CycloneDX en SPDX conflicteren niet met bestaande gegevensuitwisselingsstandaarden. Integendeel, zij bouwen hierop voort door gebruik te maken van de reeds door Forum Standaardisatie aanbevolen JSON-standaard.

Vanwege de mogelijke overlap in functionaliteit tussen de SBOM-standaarden CycloneDX 1.7 en SPDX 2.2, en indien beide standaarden een 'Pas toe of leg uit'-verplichting krijgen toegekend, is het aan de inkopende organisatie om te bepalen welke standaard het beste aansluit bij de specifieke toepassing en situatie.

5.1.3.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?

Niet van toepassing. Er is geen overlap met reeds opgenomen standaarden. CycloneDX en SPDX kennen onderling wel een overlap in functionaliteit.

5.1.3.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

Ja, de aangemelde standaarden bieden meerwaarde ten opzichte van bestaande concurrerende standaarden, zoals Software identification Tags (SWID Tags) en ISO/IEC 19770-2. Deze standaarden zijn geen open standaarden en komen daardoor niet in aanmerking voor opname. Daarnaast blijkt uit het ENISA-document Adoption State of Play dat in juni 2026 is gepubliceerd dat CycloneDX en SPDX de meest gebruikte standaarden voor SBOM's zijn.

5.1.3.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

Ja, CycloneDX 1.6 is een internationale open standaard onder European Computer Manufacturers Association (ECMA)-424. SPDX 2.2 is erkend als internationale open standaard onder ISO/IEC 5962:2021.

5.1.4 Wegen de voordelen van de standaard op tegen de nadelen?

5.1.4.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Specifieke kosten van implementatie van de standaarden zijn niet bekend; de experts geven aan dat deze afhankelijk zijn van de gekozen implementatie. Wel zijn de kosten minimaal, omdat voor het implementeren van de standaarden tools en libraries kosteloos beschikbaar zijn. Daarnaast zijn voor het verzamelen van SBOM-gegevens de benodigde stappen in de praktijk al voorzien door wetgeving zoals de CRA.

5.1.4.2 Is er een (kwalitatieve) business case van de standaard aanwezig?

Nee, voor organisaties binnen het organisatorisch werkingsgebied die niet onder de CRA vallen, is geen directe business case aanwezig. Wel kan het gebruik van deze standaarden bijdragen aan een beter inzicht in de softwareketen, een efficiënter beheer van kwetsbaarheden en een eenvoudiger informatie-uitwisseling met leveranciers en afnemers.

Voor organisaties die onder de CRA vallen, is een kwalitatieve business case aanwezig. De CRA stelt eisen aan het beschikbaar stellen van een Software Bill of Materials (SBOM). De standaarden CycloneDX 1.6 en SPDX 2.2 bieden een gestandaardiseerde wijze om aan deze verplichting invulling te geven. Daarnaast blijkt uit het ENISA-rapport SBOM Adoption State of Play 2026 dat organisaties investeren in SBOM-generatie en automatisering om te voldoen aan de eisen van de CRA en om hun software supply chain beter beheersbaar te maken. Het rapport noemt onder meer voordelen op het gebied van naleving van regelgeving, risicobeheersing, kostenvermijding en operationele efficiëntie.

5.1.4.3 Is de meerwaarde van de standaard goed inzichtelijk te maken?

Ja, de meerwaarde van de SBOM-standaarden CycloneDX 1.6 en SPDX 2.2 is goed inzichtelijk te maken. Door het gebruik van de standaarden kunnen organisaties sneller vaststellen welke componenten worden geraakt door een kwetsbaarheid. Hierdoor kan sneller en gerichter worden gehandeld. Daarnaast biedt het gebruik van de standaarden direct inzicht in onder andere licenties, afhankelijkheden en aspecten van business continuïteit, wat bijdraagt aan betere besluitvorming binnen organisaties. Wanneer door gebruik van deze standaarden de genereerde inzichten geautomatiseerd worden verwerkt en gekoppeld aan meldingen van het NCSC, kan dit proces verder worden versneld en wordt sneller inzichtelijk welke kwetsbare componenten in welke softwareproducten zijn opgenomen.

5.1.4.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de beveiligingsrisico's zijn beheersbaar en nagenoeg afwezig. Wel kan een risico ontstaan wanneer SBOM's openbaar beschikbaar worden gemaakt. In dat geval kan informatie over gebruikte softwarecomponenten inzichtelijk worden voor kwaadwillenden. Indien veiligheid (deels) is gebaseerd op security-by-obscurity, kan dit principe door een openbare SBOM worden verzwakt.

5.1.4.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de privacyrisico's aan overheidsbrede adoptie van de standaarden zijn acceptabel. Wel moet er rekening mee worden gehouden dat de standaarden persoonsgegevens kunnen bevatten, waardoor privacy- of Algemene Verordening Gegevensbescherming (AVG)-implicaties kunnen ontstaan. Het risico zit dus niet in de standaard zelf, maar in de data die ermee wordt uitgewisseld.

5.2 Open standaardisatieproces

Met dit criterium wordt bepaald of het beheer en de (door)ontwikkeling van de standaard op een open, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

Forum Standaardisatie kan het predicaat 'Uitstekend beheer' toekennen aan een beheerorganisatie als die volledig voldoet aan het criterium 'Open standaardisatieproces' en er vertrouwen is bij het Forum Standaardisatie dat in het beheerproces alle mogelijke belangen die spelen rondom de standaard zorgvuldig worden afgewogen. De kwalificatie 'Uitstekend beheer' wordt toegekend aan een Nederlandse beheerorganisatie voor een specifieke standaard.

Vragen startende met UB dienen positief te worden beantwoord wil een Nederlandse organisatie in aanmerking kunnen komen voor het predicaat 'Uitstekend beheer' voor deze standaard.

In het geval van een standaard met een internationale beheerorganisatie is het van belang dat een Nederlandse intermediaire organisatie toeziet op het bevorderen van de adoptie in Nederland en dat deze organisatie als vertegenwoordiger fungeert van de Nederlandse gebruikers. Voor deze Nederlandse intermediair is het mogelijk om het predicaat 'Erkend Nederlands Intermediair' toegekend te krijgen; het predicaat 'Erkend Nederlands Intermediair' is gebaseerd op de principes van predicaat 'uitstekend beheer'. De kwalificatie 'Erkend Nederlands Intermediair' wordt toegekend aan een Nederlandse intermediaire organisatie voor een specifieke standaard.

Vragen startende met NL_int dienen naast de vragen die starten met UB aanvullend positief te worden beantwoord en zijn essentieel wil een Nederlandse intermediaire organisatie in aanmerking kunnen komen voor het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair).

5.2.1 Waardering van het criterium criteria 'Open standaardisatieproces'

De experts komen tot de conclusie dat SBOM voldoet aan het criterium 'Open standaardisatieproces'. Deze conclusie wordt in de volgende paragrafen toegelicht.

Er is momenteel geen Nederlandse intermediair voor de SBOM-standaarden CycloneDX 1.7 en SPDX 2.2. Experts zien het NCSC als een geschikte kandidaat om deze rol te vervullen.

5.2.2 Is de documentatie voor eenieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, de specificatiedocumenten voor CycloneDX 1.6 en SPDX 2.2 zijn zonder belemmeringen beschikbaar.

5.2.2.2 Is de documentatie over het ontwikkel- en beheerproces beschikbaar zonder dat er sprake is van belemmeringen?

Ja, de documentatie over het ontwikkel- en beheerproces van CycloneDX 1.6 en SPDX 2.2 is zonder belemmeringen beschikbaar.

5.2.3 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.3.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, CycloneDX 1.6 wordt gepubliceerd onder de Apache 2.0-licentie en SPDX 2.2 onder de Creative Commons Attribution 3.0 Unported-licentie, waarmee de standaarden voor eenieder royalty-free beschikbaar zijn.

5.2.3.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja, de standaardisatieorganisaties van CycloneDX 1.6 en SPDX 2.2 publiceren hun standaarden onder een open source licentie.

5.2.4 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.4.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?

Ja, voor CycloneDX 1.6 en SPDX 2.2 is het besluitvormingsproces toegankelijk voor alle belanghebbenden.

5.2.4.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Ja, voor beide standaarden vindt geen besluitvorming plaats vanuit specifieke belangen, anders dan de belangen die de deelnemers zelf inbrengen.

5.2.4.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, zowel binnen de community van CycloneDX 1.6 en SPDX 2.2 als binnen de standaardisatieorganisaties ECMA en ISO, waar de standaarden verder worden gestandaardiseerd, bestaan formele mogelijkheden om bezwaar te maken tegen de gevolgde procedure.

5.2.4.4 (UB) Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja, voor beide standaarden worden regelmatig overleggen georganiseerd waaraan belanghebbenden kunnen deelnemen. Voor zowel CycloneDX 1.6 als SPDX 2.2 gelden voorwaarden voor deelname. Voor CycloneDX zijn deze voorwaarden beschreven in het OWASP-beleid voor community engagement. Voor SPDX zijn deze voorwaarden beschreven op de pagina Participate van SPDX.

5.2.4.5 (NL_int) Wat doet de Nederlandse intermediair om deze overleggen in Nederland voldoende onder de aandacht te brengen?

Er is momenteel geen Nederlandse intermediair.

5.2.4.6 Organiseert de standaardisatieorganisatie een openbare consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Ja, zowel voor CycloneDX 1.6 als voor SPDX 2.2 vindt voorafgaand aan het vaststellen van een nieuwe versie een publieke consultatie plaats.

5.2.4.7 (NL_int) Wat doet de Nederlandse intermediair om deze publieke consultatie actief onder de aandacht te brengen bij de Nederlandse overheid?

Er is momenteel geen Nederlandse intermediair.

5.2.5 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.5.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, CycloneDX 1.6 wordt beheerd door de onafhankelijke non-profitorganisatie OWASP. SPDX 2.2 wordt beheerd door de onafhankelijke non-profitorganisatie The Linux Foundation.

5.2.5.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor ten minste drie jaar gegarandeerd?

Nee, de financiering van het beheer van CycloneDX is niet gegarandeerd voor ten minste drie jaar, maar de standaard wordt wel actief ondersteund door diverse multinationals. Zie onder andere de CycloneDX Supporters. De financiering van het beheer van SPDX is eveneens niet gegarandeerd voor ten minste drie jaar, maar de standaard wordt wel actief ondersteund door verschillende multinationals en een actieve community.

5.2.6 Is het (versie)beheer van de standaard goed geregeld?

5.2.6.1 (UB) Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard?

Ja, OWASP voor CycloneDX 1.6 en The Linux Foundation voor SPDX 2.2 hebben een open proces voor de vrijgave van nieuwe versies.

5.2.6.2 (UB) *Is de beheerdocumentatie goed vindbaar en verkrijgbaar?*

Ja, de beheerdocumentatie van CycloneDX 1.6 en SPDX 2.2 is goed vindbaar en verkrijgbaar.

5.2.6.3 (UB) *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*

Ja, het belang van de Nederlandse overheid is voldoende geborgd bij de ontwikkeling en het beheer van de standaard.

5.2.6.4 (NL_int) *Wat doet de Nederlandse intermediair om het Nederlands belang voldoende te borgen? Op welke wijze wordt gecontroleerd of Nederlandse inbreng ook daadwerkelijk wordt opgepakt?*

Er is momenteel geen Nederlandse intermediair.

5.2.6.5 (UB) *Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?*

Ja, ENISA vertegenwoordigt de Europese Unie en Nederland bij de doorontwikkeling van de standaarden.

5.2.6.6 (NL_int) *Wat doet de Nederlandse intermediair om het Nederlandse belang bij het beheer van de standaard voldoende te borgen?*

Er is momenteel geen Nederlandse intermediair.

5.2.6.7 (UB) *Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?*

Niet van toepassing.

5.2.6.8 (NL_int) *Wat is de rol van de internationale standaardisatieorganisatie, wat is de rol van de Nederlandse intermediair en hoe versterken deze elkaar?*

Er is momenteel geen Nederlandse intermediair.

5.2.7 Is er adoptieondersteuning voor de standaard?

5.2.7.1 (UB) *Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?*

Ja, er is een toegankelijk aanspreekpunt waar meer informatie over de standaarden te vinden en op te vragen is. Namens het CycloneDX- en SPDX-coreteam is Thomas Steenbergen aangewezen als liaison en aanspreekpunt voor vragen over de standaarden.

5.2.7.2 (NL_int) *Is er een toegankelijk nationaal aanspreekpunt of organisatie?*

Er is momenteel nog geen Nederlandse intermediair.

5.2.7.3 (UB) Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, er wordt ondersteuning geboden bij de adoptie en implementatie van de SBOM-standaarden. Via The Linux Foundation en OWASP zijn er trainingen beschikbaar. Daarnaast biedt Awesome SBOM, dat via developer.overheid.nl is opgenomen in het Open Source Register, een overzicht van tooling voor de standaarden. Het NCSC heeft daarnaast kennisproducten ontwikkeld voor de implementatie van SBOM's en biedt ondersteuning voor de implementatie van de standaarden.

5.2.7.4 (NL_int) Wordt er vanuit een Nederlandse organisatie ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, namelijk via developer.overheid.nl en NCSC.

5.3 Draagvlak

Met dit criterium wordt bepaald of de opname van de standaard op de 'Pas toe of leg uit'-lijst of lijst aanbevolen standaarden op voldoende breed draagvlak kan rekenen binnen de overheid. Een voorwaarde hierbij is ook dat er voldoende marktondersteuning voor de standaard bestaat en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

5.3.1 Waardering van het criterium criteria 'Draagvlak'

De experts komen tot de conclusie dat SBOM voldoet aan het criterium 'Draagvlak'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.3.2 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.2.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja, CycloneDX en SPDX worden ondersteund door meerdere leveranciers, waaronder zowel aanbieders van open source-oplossingen als leveranciers van commerciële (gesloten) software en diensten.

5.3.2.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Ja, er zijn verschillende (open source) tools beschikbaar waarmee de conformiteit van de implementatie van de standaarden kan worden getoetst. Voor CycloneDX kan dit via de online validator. Voor SPDX is eveneens een online validatietool beschikbaar. Daarnaast zijn er ook verschillende command-line interface (CLI)-tools beschikbaar voor het valideren en verifiëren van implementaties.

5.3.2.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Ja, de standaarden zijn zelfstandig toepasbaar en hebben een duidelijk afgebakend doel.

5.3.2.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja, zowel op het GitHub-account van OWASP als dat van SPDX zijn voorbeeldimplementaties beschikbaar. Daarnaast kan het door het BSI ontwikkelde SBOM-profiel mogelijk ondersteuning bieden bij de adoptie en implementatie van de standaarden.

5.3.3 Kan de standaard rekenen op voldoende draagvlak?

5.3.3.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

Ja, de volgende stakeholders ondersteunen of passen de standaard toe:

- Ministerie van Financiën (MinFin): de Belastingdienst gebruikt SBOM actief voor het monitoren van het IV-landschap.
- Ministerie van Sociale Zaken en Werkgelegenheid (SZW): het Uitvoeringsinstituut Werknemersverzekeringen (UWV) is voornemens SBOM te implementeren.
- Ministerie van Justitie en Veiligheid (JenV): het NCSC, samen met TNO, raadt SBOM aan als belangrijke bouwsteen om de transparantie van de software supply chain te vergroten en de security te versterken.
- Ministerie van Algemene Zaken / Dienst Publiek en Communicatie (AZ/DPC): gebruikt SBOM's actief in technisch kwetsbaarhedenbeheer en voor het monitoren van het IV-landschap.
- ICTU: SBOM is al meerdere jaren onderdeel van de kwaliteitsaanpak.
- Rijkswaterstaat (RWS)
- Dienst ICT Uitvoering (DICTU)
- Centraal Justitieel Incassobureau (CJIB)
- Dienst Uitvoering Onderwijs (DUO)
- Vereniging van Nederlandse Gemeenten (VNG): ondersteunt het aanleveren van SBOM's.

Daarnaast staan alle aanwezige experts, namens de organisaties die zij vertegenwoordigen, achter de adoptie van de standaarden.

5.3.3.2 Staan de overheidsorganisaties die worden geraakt door een verplichting van de standaard achter het verplichte gebruik van de standaard?

Ja, de overheidsorganisaties die zijn genoemd in paragraaf 5.3.3.1 ondersteunen het verplichte gebruik van de standaard.

5.3.3.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, de organisaties die zijn genoemd in paragraaf 5.3.3.1 maken gebruik van de aangemelde SBOM-standaarden, maar niet allemaal van de versies CycloneDX 1.6 en SPDX 2.2.

De experts beschouwen nieuwere versies van de standaarden als beter passend bij de functionele doelen en het organisatorisch werkingsgebied van CycloneDX 1.6 en SPDX 2.2. Daarom adviseren zij om de nieuw vastgestelde versie (1.7) van CycloneDX te verplichten ('Pas toe of leg uit') aan de overheid.

5.3.3.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, er worden binnen het organisatorisch werkingsgebied oudere versies van de SBOM-standaarden gebruikt. Gezien de compatibiliteit van de standaarden met eerdere versies worden geen directe knelpunten verwacht wanneer organisaties oudere versies gebruiken dan CycloneDX 1.6 en SPDX 2.2.

5.3.3.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Ja, CycloneDX 1.6 en SPDX 2.2 zijn backwards compatible met eerdere versies van de standaarden.

5.3.3.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Het is onbekend of er voldoende positieve signalen zijn over toekomstig gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie dat SBOM voldoet aan het criterium 'Opname op de lijst bevordert adoptie'.

Opname van CycloneDX 1.7 (waarbij de toetsingsprocedure is uitgevoerd op basis van versie 1.6) en SPDX 2.2 onder registratie SBOM op de 'Pas toe of leg uit'-lijst bevordert de adoptie van deze standaarden doordat het de bekendheid vergroot, de vrijblijvendheid wegneemt en eenduidigheid stimuleert in het beschrijven van softwarecomponenten in ingekochte en zelfontwikkelde softwareproducten. Dit vergemakkelijkt hergebruik binnen de overheid en versterkt de onderhandelingspositie richting leveranciers.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie en OBDO de volgende adviezen bij plaatsing van SBOM op de 'Pas toe of leg uit'-lijst:

- Aan indiener om bij een nieuwe versie van de BSI te bezien of er een NL-profiel nodig is of de nieuwe versie overgenomen kan worden als profiel op de SBOM standaard;
- Aan NCSC om de mogelijkheid te verkennen om een nationale regierol (Nederlandse intermediair) voor SBOM's op zich te nemen. Deze rol richt zich op het bevorderen van de toepassing van SBOM's, waaronder het ontwikkelen van praktische handreikingen,

het beheren van profielen, het opstellen van validatiecriteria, het bieden van een overzicht van beschikbare tooling, het ondersteunen bij leveranciersvragen, het leggen van de koppeling met NCSC-meldingen en het monitoren van de adoptie. Daarnaast richt deze rol zich op het afstemmen van nationale initiatieven op relevante Europese en internationale ontwikkelingen en vice versa.

Zodra de regierol is belegd bij een Nederlandse intermediair, gelden onderstaande adviezen:

- Aan de Nederlandse intermediair om in samenwerking met een aantal Open Source Program Offices (OSPO's) een handreiking op te stellen die duidelijk maakt in welke situaties SPDX en wanneer CycloneDX de voorkeur heeft. Een dergelijke richtlijn biedt organisaties meer houvast bij de keuze voor een SBOM-formaat, bevordert een consistente toepassing van beide standaarden en voorkomt onnodige onduidelijkheid in de praktijk;
- Aan de Nederlandse intermediair om de ENISA Technical Advisory for Secure Use of Package Managers te gebruiken als input voor praktische richtlijnen over het veilig gebruik van softwareafhankelijkheden, waaronder het genereren van SBOM’s tijdens het buildproces en het monitoren van afhankelijkheden en kwetsbaarheden;
- Aan de Nederlandse intermediair om de aansluiting van de SBOM-standaarden op aankomende wet- en regelgeving, zoals de Cyber Resilience Act (CRA) en de Cyberbeveiligingswet (Cbw), inzichtelijk te maken. Dit ondersteunt overheidsorganisaties bij het onderbouwen hoe de standaard bijdraagt aan het voldoen aan de wettelijke eisen;
- Aan de Nederlandse intermediair om een generieke kwalitatieve business case voor de SBOM-standaarden op te stellen, waarin de verwachte baten en kosten van het gebruik van de standaarden voor organisaties binnen het organisatorisch werkingsgebied worden beschreven.