Expertadvies NVN-CEN/TS 18026 2024 EN

Aan:	Forum Standaardisatie
Van:	Innovalor Advies B.V.
Datum:	woensdag 17 juni 2026
Versie:	1.0
Bijlagen:	geen

1 Advies

De experts die betrokken waren bij het expertonderzoek adviseren om NVN-CEN/TS 18026:2024 EN aan te bevelen aan de overheid via plaatsing op de lijst aanbevolen standaarden van het Forum Standaardisatie.

Het opgestelde functioneel toepassingsgebied voor NVN-CEN/TS 18026 is:

> *NVN-CEN/TS 18026 kan worden toegepast bij de aanschaf van een ICT-dienst of ICT-product indien deze (geheel of gedeeltelijk) gebruikmaakt van cloud computing.*
>
> *Toepassing vindt risico-gebaseerd plaats naar eigen inzicht, waarbij het niveau 'basis' wordt gehanteerd als minimum om aan de standaard te kunnen voldoen.*

In dit expertadvies en het verdere verloop van de toetsingsprocedure wordt de definitie van cloud computing gehanteerd zoals opgenomen in de door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 16 april 2026 vastgestelde Begrippenlijst Cloudterminologie. Hiermee sluit dit expertadvies aan op het Rijkscloudbeleid en de uniforme clouddefinities die binnen de Nederlandse overheid worden gehanteerd. De definitie luidt als volgt:

> *Een model dat het mogelijk maakt om plaats- en tijdsonafhankelijk, op een gemakkelijke manier, op afroep, via een netwerk toegang te krijgen tot een voortdurend beschikbare gedeelde verzameling van configureerbare computing resources die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met de aanbieder.*

Een nadere uitwerking van deze definitie, inclusief de essentiële karakteristieken van cloud computing en de onderscheiden service- en implementatiemodellen, is te vinden in de Begrippenlijst Cloudterminologie van het OBDO.

Daarnaast worden voor de definities van informatiebeveiliging en cyberbeveiliging de volgende definities gehanteerd:

> *Informatiebeveiliging: het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, zoals gehanteerd binnen de ISO/IEC 27000-serie en uitgewerkt in ISO/IEC 27001.*
>
> *Cyberbeveiliging: de bescherming van netwerk- en informatiesystemen, hun gebruikers en andere betrokkenen tegen cyberdreigingen, met als doel de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van gegevens en diensten te waarborgen. Deze definitie sluit aan bij de benadering uit de Cyberbeveiligingswet (NIS2-richtlijn).*

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

- Welke andere standaarden een soortgelijke functionaliteit bieden en mogelijk als alternatief moeten worden overwogen voor toetsing in plaats van NVN-CEN/TS 18026:2024 EN;
- Aandacht voor de omschrijving van het functioneel toepassingsgebied;
- Aandacht voor het draagvlak onder clouddienstproviders voor NVN-CEN/TS 18026:2024 EN, ten behoeve van het vermijden van onevenredige leveranciersafhankelijkheid van hyperscalers;
- Aandacht voor hoe NVN-CEN/TS 18026:2024 EN bijdraagt aan meer digitale autonomie voor de Nederlandse overheid;
- Aandacht voor het verkennen van de toepassing van NVN-CEN/TS 18026:2024 EN bij gemeenten en waterschappen.

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 lijst aanbevolen standaarden. Tot slot geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het OBDO om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

NVN-CEN/TS 18026:2024 EN is een recent gepubliceerde Europese norm die een reeks cybersecurityvereisten bevat voor de cyberbeveiliging van clouddiensten. De standaard is in eerste aanleg ontwikkeld door de European Union Agency for Cybersecurity (ENISA) op

verzoek van de Europese Commissie onder de regels van de Europese Cybersecurity Act en vervolgens omgezet naar een Europese Norm (EN) door CEN/CENELEC als Europese standaardisatieorganisatie. De standaard sluit inhoudelijk aan op bestaande internationale kaders voor informatiebeveiliging en cybersecurity, zoals de ISO/IEC 27000-serie, en bevat daarnaast eisen die zijn afgestemd op Europese wet- en regelgeving. Hierdoor is de standaard zowel internationaal herkenbaar als Europees specifiek toepasbaar.

De standaard voorziet in drie verschillende zekerheidsniveaus, namelijk: 'Basis', 'Substantieel' en 'Hoog'. Sommige eisen zijn op alle niveaus van toepassing, soms uitgebreid op hogere niveaus, terwijl enkele eisen alleen van kracht zijn op het hoogste niveau. Er wordt een risicobeoordeling uitgevoerd om de specifieke risico's voor de clouddienst te bepalen, waarbij ook rekening wordt gehouden met de mogelijkheden van het niveau en de specifieke cyberrisico's voor de clouddienst. De risicobehandeling behelst vervolgens de selectie van passende beheersmaatregelen door de organisatie om te voldoen aan de eisen voor dat niveau.

Binnen de Europese markt sluit NVN-CEN/TS 18026:2024 EN aan bij het EU Cybersecurity Certification Scheme for Cloud Services (EUCS), een raamwerk voor het certificeren van de cybersecurity van clouddienstverleners. Ten tijde van het opstellen van dit advies (16 juni 2026) is EUCS nog niet formeel vastgesteld door de Europese Commissie. Zodra EUCS in werking treedt en van toepassing wordt, zullen nationale certificeringsschema's naar verwachting gedurende een overgangsperiode van drie jaar worden afgebouwd. Tot die tijd blijven bestaande nationale schema's relevant voor zover deze nog van toepassing zijn en kan reeds worden verwezen naar de criteria en eisen uit EUCS. Clouddienstleveranciers hoeven zich dan nog maar één keer te certificeren volgens het EUCS-schema (op het gekozen niveau) om aan de cybersecurity-eisen van alle deelnemende EU-lidstaten te voldoen.

2.2 Waarom is deze standaard belangrijk?

Momenteel ontbreken duidelijke en uniforme overheidsvereisten op het gebied van cloudbeveiliging. Met behulp van deze standaard kan de vraag naar beveiligingseisen helder worden uitgevraagd in aanbestedingen. Daarnaast beperkt de standaard versnippering van veiligheidsvoorschriften binnen de EU door één uniform beveiligingsniveau vast te leggen. Verder draagt het toepassen van de standaard bij aan betere bescherming van gegevens en systemen, waardoor overheidsorganisaties veiliger kunnen opereren.

Tot slot kan het toepassen van één uniform beveiligingsniveau bijdragen aan een gelijk speelveld binnen de Europese markt, met kansen voor Nederlandse cloudleveranciers in die markt. Leveranciers hebben dan te maken met uniforme veiligheidsvoorschriften waaraan ze moeten voldoen. Daarbij geldt wel dat voldoende leveranciers in staat moeten zijn daaraan te voldoen.

3 Betrokkenen en proces

Op 6 mei 2025 heeft het Ministerie van Economische Zaken en Klimaat NVN-CEN/TS 18026:2024 EN aangemeld voor toetsing om aan te bevelen aan de overheid.

Op 30 juni 2025 heeft een intakegesprek plaatsgevonden met de indiener, de procedurebegeleider en Bureau Forum Standaardisatie. In dit gesprek is verkend of de standaard NVN-CEN/TS 18026:2024 EN 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 11 februari 2026 besloten de aanmelding in procedure te nemen.

Vervolgens heeft de procedurebegeleider met raadpleging van Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld om de standaard in een expertsessie nader te bespreken en te toetsen aan de vier inhoudelijke hoofdcriteria van Forum Standaardisatie.

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

De leden van de expertgroep zijn op 11 mei 2026 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en het organisatorisch werkingsgebied opgesteld. Dit expertadvies geeft de uitkomst van de expertsessie weer.

Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie via de website van Internetconsultatie. Gedurende de consultatieperiode kan iedereen op het expertadvies reageren.

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

Het Forum Standaardisatie neemt op basis van dit Forumadvies (opgesteld op basis van het expertadvies, de reactie(s) uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf) een besluit over het wel of niet aanbevelen van de standaard.

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 onafhankelijke voorzitter die de expertsessie leidt.

Aan de expertsessie hebben de volgende personen deelgenomen:

- Eric van Arragon (CIP)
- Ruud Kerssens (RDI)

- John Segers (SURF)
- Jitze van der Vinne (ODC-Noord)
- Octavia de Weerdt (DINL)

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

Claudia Vermeulen, 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.

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 NVN-CEN/TS 18026:2024 EN wel 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 NVN-CEN/TS 18026:2024 EN op de lijst aanbevolen standaarden is:

NVN-CEN/TS 18026:2024 EN kan worden toegepast bij de aanschaf van een ICT-dienst of ICT-product indien deze (geheel of gedeeltelijk) gebruikmaakt van cloud computing.

Toepassing vindt risico-gebaseerd plaats naar eigen inzicht, waarbij het niveau 'basis' wordt gehanteerd als minimum om aan de standaard te kunnen voldoen.

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

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het opgestelde organisatorisch werkingsgebied voor NVN-CEN/TS 18026:2024 EN op de lijst aanbevolen standaarden 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 lijst aanbevolen standaarden 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, toepassing van de standaard overstijgt een enkele organisatie of sector, aangezien deze betrekking heeft op het gehele ICT-portfolio van de (semi-)overheid. Daarmee is de toepassing breed en kan deze in elke sector van de (semi-)overheid worden toegepast.

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, NVN-CEN/TS 18026:2024 EN conflicteert niet met de reeds opgenomen standaarden NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 op de lijst van open standaarden van het Forum Standaardisatie.

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

Ja, de standaard biedt meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied. De standaard bevat diverse eisen die aansluiten op ISO/IEC 27001, waaronder eisen ten aanzien van een Information Security Management System (ISMS). De standaard bouwt daarmee voort op bestaande normen en kaders voor informatiebeveiliging, maar werkt deze verder uit met

specifieke en gedetailleerde eisen voor clouddiensten. Hierdoor biedt de standaard aanvullende handvatten voor de beveiliging van cloudomgevingen.

De Cloud Computing Compliance Criteria Catalogue (C5) van het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) is niet opgenomen op de lijst van open standaarden van het Forum Standaardisatie. De standaard is qua structuur gebaseerd op C5 en bevat aanvullingen vanuit het Franse SecNumCloud-certificeringsschema van Agence nationale de la sécurité des systèmes d'information (ANSSI), bijdragen vanuit de ENISA-expertgroep en verdere uitwerking binnen CEN/CENELEC.

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

Niet van toepassing. Er zijn geen andere bestaande concurrerende standaarden bekend.

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

Ja, het betreft een internationale standaard, namelijk een recent ontwikkelde Europese norm voor de cyberbeveiliging van clouddiensten en is opgesteld door CEN/CENELEC, in opdracht van de Europese Commissie (EC) aan ENISA. De standaard is afgestemd op Europese wet- en regelgeving, waaronder de Europese Cyber Security Act, en is daarmee zowel internationaal herkenbaar als Europees specifiek toepasbaar. De standaard sluit inhoudelijk aan op bestaande internationale kaders voor informatiebeveiliging en cyberbeveiliging en bevat aanvullende, specifiek op de Europese context afgestemde eisen.

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?

Ja, de kosten van implementatie voor inkopende organisaties van NVN-CEN/TS 18026:2024 EN worden in algemene zin als acceptabel beschouwd. Tegelijkertijd zijn er geen concrete voorbeeldcases beschikbaar en zijn de totale implementatiekosten nog niet eenduidig bekend of volledig inzichtelijk. Organisaties dienen op basis van een eigen risicobeoordeling de specifieke risico’s van de clouddienst te bepalen, waarbij rekening wordt gehouden met het benodigde beveiligingsniveau en de specifieke cyberrisico’s van de betreffende clouddienst. Het voldoen aan hogere niveaus kan aanvullende kosten met zich meebrengen. Daarnaast bestaan er onzekerheden over de impact van de benodigde investeringen, met name voor middelgrote en kleinere cloudaanbieders.

De kosten voor het verkrijgen van het specificatiedocument worden als acceptabel beschouwd. Op dit moment geldt een tarief van 185 euro exclusief BTW. De deelname aan het standaardisatieproces via NEN brengt jaarlijkse kosten van 2.680 euro exclusief BTW met zich mee voor het lidmaatschap. De overheid kan de documentatie kosteloos raadplegen via NENconnect.

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

Nee, de standaard is nog te recent ontwikkeld om een uitgewerkte (kwalitatieve) business case beschikbaar te hebben.

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

Ja, het gebruik van clouddiensten (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS)) neemt zowel in de publieke als in de private sector sterk toe. Daarmee groeit de noodzaak voor betrouwbare, consistente en breed erkende vereisten voor de cyberbeveiliging van clouddiensten. Volgens de standaard dient elke Cloud Service Provider (CSP) de scope en de grenzen van de aangeboden dienst te documenteren, zodat duidelijk is welke onderdelen onder de verantwoordelijkheid van de CSP vallen.

NVN-CEN/TS 18026:2024 EN bevat vereisten voor het beveiligen van de opslag van gegevens en kan indirect een bijdrage leveren aan leveranciersonafhankelijkheid doordat meerdere leveranciers een gelijk referentiekader gebruiken voor het inrichten van cybersecurity.

De standaard bevat geen specifieke bepalingen die interoperabiliteit tussen verschillende overheidsorganisaties bevorderen of die de afhankelijkheid van bepaalde leveranciers verminderen. Daarmee is het effect van de standaard op leveranciersafhankelijkheid of interoperabiliteit beperkt.

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

Ja, er zijn geen beveiligingsrisico's verbonden aan overheidsbrede adoptie van de standaard.

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

Ja, er zijn geen privacyrisico's verbonden aan overheidsbrede adoptie van de standaard.

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.

5.2.1 Waardering van het criterium criteria 'Open standaardisatieproces'

De experts komen tot de conclusie dat NVN-CEN/TS 18026:2024 EN voldoet aan het criterium 'Open standaardisatieproces. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.2.2 Is de documentatie voor eenieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, het specificatiedocument is zonder belemmeringen beschikbaar via NEN.nl. Zie ook 5.1.4.1.

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 (CEN/CENELEC) is vrij beschikbaar voor de overheid en kan zonder belemmeringen worden ingezien.

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, de standaardisatieorganisatie stelt het intellectueel eigendomsrecht op (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar.

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

5.2.4 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.4.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?

Ja, het besluitvormingsproces is toegankelijk voor alle belanghebbenden waaronder gebruikers, leveranciers, adviseurs en wetenschappers.

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

Ja, dit proces volgt de op consensus gebaseerde aanpak van CEN/CENELEC, met nationale implementatie via NEN in Nederland.

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

Ja, dit proces volgt de procedures van CEN/CENELEC.

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

Ja, de standaardisatieorganisatie organiseert regelmatig overleggen met belanghebbenden over de doorontwikkeling en het beheer van NVN-CEN/TS 18026. Herzieningen volgen de standaardprocedure van CEN/CENELEC, waarbij de standaard elke vier à vijf jaar wordt geëvalueerd. Afhankelijk van de uitkomst kan de standaard worden ingetrokken, gewijzigd of

ongewijzigd blijven. Eerdere aanpassing of intrekking is ook mogelijk, afhankelijk van de situatie.

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

Ja, openbare consultaties maken deel uit van het proces van de standaardisatieorganisatie CEN/CENELEC voordat (een nieuwe versie van) de standaard wordt vastgesteld.

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, de ontwikkeling en het beheer van de standaard zijn belegd bij een onafhankelijke non-profit standaardisatieorganisatie, te weten CEN/CENELEC (Informatie Normcommissieleden).

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

Ja, de financiering van de ontwikkeling en het onderhoud van de standaard is voor ten minste drie jaar gegarandeerd.

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

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

Ja, CEN/CENELEC beschikt over gepubliceerd beleid met betrekking tot het versiebeheer van de standaard.

5.2.6.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, de beheerdocumentatie is goed vindbaar en verkrijgbaar. Dit is beschreven in het beleid Amendments/Revisions to European Standards.

5.2.6.3 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 in voldoende mate geborgd bij zowel de ontwikkeling als het beheer van de standaard. Nederland, vertegenwoordigd door het Ministerie van Economische Zaken en Klimaat (EZK), is nauw betrokken geweest bij het ontwikkelproces.

Gedurende meerdere jaren heeft Nederland een actieve en leidende rol vervuld, onder andere door het leveren van de voorzitter en een lead editor, en door het voeren van het secretariaat via de NEN-normcommissie Cybersecurity en Privacy. De NEN-normcommissie is betrokken geweest bij de initiële versie van de standaard maar niet bij latere versies.

Tevens zijn diverse faciliterende en coördinerende taken, in opdracht van de Europese Commissie, door Nederland uitgevoerd. Deze intensieve betrokkenheid strekte zich uit over

een periode van circa drie à vier jaar voor de specifieke standaardontwikkeling, en in bredere zin over ruim zeven jaar binnen het domein van Europese cybersecurity-initiatieven.

5.2.6.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Ja, de vertegenwoordiging van belanghebbenden bij het beheer van de standaard via de NEN-normcommissie is evenwichtig samengesteld en vormt een goede afspiegeling van zowel het werkingsgebied als het functioneel toepassingsgebied van de standaard. Deze vertegenwoordiging wordt bij iedere revisie opnieuw beoordeeld en, waar nodig, aangepast om blijvende aansluiting bij de belangen van alle relevante partijen te waarborgen.

5.2.6.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum Standaardisatie zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

Niet van toepassing. Het betreft een internationale standaard waarvoor geen predicaat 'Uitstekend beheer' voor een erkend Nederlands intermediair is aangevraagd.

5.2.7 Is er adoptieondersteuning voor de standaard?

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

Ja, NEN fungeert als toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard beschikbaar is en opgevraagd kan worden. De adoptie en implementatie van de standaard worden ondersteund door EZK en BZK.

5.2.7.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, er wordt ondersteuning gegeven bij de adoptie en de implementatie van de standaard door EZK en BZK binnen de overheid.

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 NVN-CEN/TS 18026:2024 EN niet volledig 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?

Nee, dit is nog niet aantoonbaar. Er zijn echter wel positieve signalen van marktpartijen (zie paragraaf 5.3.3.6) over de standaard, wat doet vermoeden dat meerdere leveranciers zich in de toekomst kunnen conformeren aan de standaard.

Tegelijkertijd zijn er signalen dat toepassing van deze standaard voor het zekerheidsniveau 'Hoog' – gezien de gestelde eisen – slechts haalbaar is voor een beperkt aantal grote leveranciers. De standaard zou de afhankelijkheid van een klein aantal grote clouddienst leveranciers kunnen vergroten indien gebruikers kiezen voor het hoogste zekerheidsniveau.

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

Nee, op dit moment is er nog geen implementatietoets voor cybersecurity certificering van diensten van cloudserviceproviders (CSP's) op basis van NVN-CEN/TS 18026:2024 EN.

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?

Nee, de standaard draagt niet direct bij aan interoperabiliteit, maar wel aan de standaardisering van processen en de manier waarop CSP's communiceren, inclusief uniformering van definities. Dit draagt tevens bij aan de verhoging van het beveiligingsniveau.

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

Nee, vooralsnog zijn er geen profielen of voorbeeldimplementaties van de standaard beschikbaar. De verwachting is dat, zodra de EUCS is vastgesteld als Europese act, deze profielen vanuit ENISA beschikbaar zullen worden gesteld.

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?

Deels. Belangrijke overheidsstakeholders ondersteunen de adoptie van de standaard. Het betreft onder meer de Rijksdienst voor Digitale Infrastructuur (RDI), het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het Ministerie van Justitie en Veiligheid (JenV).

Daarnaast is de Online Trust Coalitie (OTC) betrokken, als breed gedragen publiek-private samenwerking op het gebied van clouddiensten, met een sterke vertegenwoordiging op nationaal, Europees en internationaal niveau. Deze combinatie van partijen vormt een krachtige en representatieve stem voor het Nederlandse belang in de verdere ontwikkeling en

toepassing van de standaard. De eerdergenoemde overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard staan achter het gebruik ervan.

Er is geen zicht op de mate waarin waterschappen, gemeenten, provincies en uitvoeringsorganisaties de adoptie van de standaard ondersteunen.

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

Niet van toepassing. De aanvraag betreft het toekennen van de status Aanbevolen.

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

Nee, voor zover bekend hanteren overheidsorganisaties deze standaard niet als eis in aanschaf- en doorontwikkeltrajecten.

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

Niet van toepassing. De experts stellen vast dat er geen vorige versie van de standaard binnen het organisatorisch werkingsgebied door meerdere Nederlandse overheidsorganisaties wordt gebruikt.

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

Niet van toepassing. De experts stellen vast dat er geen sprake is van eerdere versies van de standaard waarmee de aangemelde versie compatibel moet zijn.

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

Ja, er zijn voldoende positieve signalen over toekomstig gebruik van de standaard.

Deze blijkt onder andere uit uitingen van communities zoals de OTC en de Dutch Cloud Community (DCC), organisaties zoals NEN en Eurosmart, en diverse andere marktpartijen op het gebied van clouddienstverlening, met name vanwege de behoefte aan een duidelijkere vraagcirculatie en het stimuleren van innovatie.

Vanuit het bedrijfsleven wordt het belang benadrukt van een wisselwerking met de adoptie door de overheid. Dit wordt onder meer onderbouwd in de position paper “Strategische digitale autonomie en het Rijksbreed cloudbeleid” van de DCC.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie dat NVN-CEN/TS 18026:2024 EN voldoet aan het criterium ‘Opname op lijst bevordert adoptie’.

De status van aanbevolen standaard is op dit moment het passende middel om de adoptie van NVN-CEN/TS 18026:2024 EN binnen de (semi)overheid te bevorderen, omdat de EUCS-certificering nog niet is afgerond. Opname op de lijst aanbevolen standaarden biedt de mogelijkheid om bekendheid met en ervaring in de toepassing van de standaard binnen de overheid op te bouwen. De ‘Pas toe of leg uit’-verplichting lijkt daarom op dit moment niet het passende middel om de adoptie van NVN-CEN/TS 18026:2024 EN binnen de (semi)overheid te bevorderen.

In een latere fase kan het toekennen van de status ‘Pas toe of leg uit’ mogelijk wel bijdragen aan verdere adoptie, bijvoorbeeld door uniformiteit in aanbestedingen te bevorderen en het belang van cloudbeveiliging op Europees niveau te versterken. Dit sluit aan bij signalen vanuit onder andere de OTC, overheidsaanbestedingen en relevante marktpartijen in de clouddienstverlening, die de behoefte aan duidelijke vraagarticulatie en het stimuleren van innovatie onderstrepen.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie en OBDO de volgende adviezen bij plaatsing van NVN-CEN/TS 18026:2024 EN op de lijst aanbevolen standaarden van het Forum Standaardisatie:

- Aan Ministerie van Economische Zaken en Klimaat om de promotie van de standaard te ondersteunen en verdere stappen te zetten in de adoptie ervan;
- Aan Ministerie van Economische Zaken en Klimaat om, zodra de EUCS-certificering is vastgesteld, NVN-CEN/TS 18026:2024 EN opnieuw aan te melden voor toetsing voor plaatsing op de ‘Pas toe of leg uit’-lijst van het Forum Standaardisatie;
- Aan Forum Standaardisatie om nader te reflecteren op de definities van autonomie, digitale soevereiniteit en leveranciersafhankelijkheid, zodat meer duidelijkheid ontstaat over de onderlinge samenhang en toepassing van deze begrippen.