Verslag reacties consultatie NVN-CEN/TS 18026 2024 EN aanbevelen

Aan:	Forum Standaardisatie
Van:	Bureau Forum Standaardisatie
Datum:	7 september 2026
Versie:	1.0
Bijlage:	n.v.t.

1.Inleiding

Dit verslag bevat de openbare reacties uit de openbare consultatie NVN-CEN/TS 18026 2024 EN aanbevelen van het Forum Standaardisatie van 19 juni 2026 tot en met 31 juli 2026 op internetconsultatie.nl.

De consultatie is onderdeel van de toetsing van het Forum Standaardisatie of NVN-CEN/TS 18026 2024 EN geschikt is om aan te bevelen aan de overheid.

In deze openbare consultatie kon men reageren op het advies van de experts die waren betrokken bij het expertonderzoek voor deze toetsing. Dit expertadvies maakte deel uit van de openbare consultatie.

In de openbare consultatie zijn drie reacties ontvangen. In het volgende hoofdstuk is het antwoord van de respondent een-op-een en ongewijzigd overgenomen van de Pagina reacties van de consultatie. Indien de respondent zijn reactie heeft aangeleverd in de vorm van een brief, is deze brief als bijlage bij dit verslag opgenomen.

2. Reacties uit de openbare consultatie

2.1. Reactie van N. Noorland en J. Stedehouder (Gemeente Rotterdam)

Rotterdam

Datum: 28 juli 2026

De reactie is aangeleverd in de vorm van een brief (zie bijlage 1).

2.2. Reactie van Anoniem (Nederlandse Orde van Register EDP-Auditors (NOREA))

Hoofddorp

Datum: 30 juli 2026

Onderstaand is de reactie een-op-een en ongewijzigd overgenomen van de pagina reacties van de consultatie. Daarnaast heeft de respondent zijn reactie aangeleverd in de vorm van een brief met daarin een samenvatting van de antwoorden op de consultatievragen (zie Bijlage 2).

2.2.1. Vraag 1

Geef hier indien gewenst uw reactie op het advies van de experts om NVN-CEN/TS 18026, versie 2024: EN aan te bevelen aan de overheid via plaatsing op de lijst Aanbevolen van het Forum Standaardisatie (hoofdstuk 1 van het expertadvies).

"NOREA ondersteunt het advies om NVN-CEN/TS 18026:2024 EN te plaatsen op de lijst Aanbevolen van het Forum Standaardisatie. De standaard adresseert een belangrijk en actueel vraagstuk: het ontbreken van uniforme, herkenbare en Europees afgestemde beveiligingseisen voor clouddiensten binnen de overheid. Het expertadvies geeft aan dat de standaard cybersecurityvereisten bevat voor cloudbeveiliging en aansluit op bestaande internationale kaders zoals de ISO/IEC 27000-serie, aangevuld met eisen die zijn afgestemd op Europese wet- en regelgeving.
NOREA acht de status Aanbevolen passend omdat de standaard relevant is. Wel vraagt deze nog om een in Nederland passend ecosysteem rondom implementatie, toetsbaarheid en certificering. In het expertadvies wordt vastgesteld dat EUCS nog niet formeel is vastgesteld en dat er nog geen implementatietoets voor cybersecuritycertificering van clouddiensten op basis van deze standaard beschikbaar is.
Wij adviseren daarom om plaatsing op de lijst Aanbevolen te combineren met een expliciete adoptie-roadmap, zodat overheidsorganisaties ervaring kunnen opdoen en de standaard op een beheerste, proportionele en auditbare wijze kan worden toegepast."

2.2.2. Vraag 2

Geef hier indien gewenst uw reactie op het voorgestelde functioneel toepassingsgebied (hoofdstuk 1 van het expertadvies).

"NOREA kan zich vinden in het voorgestelde functioneel toepassingsgebied: toepassing bij de aanschaf van een ICT-dienst of ICT-product indien deze geheel of gedeeltelijk gebruikmaakt van cloud computing, waarbij toepassing risicogebaseerd plaatsvindt en het niveau Basis als minimum geldt.
Wij vinden vooral de risicogebaseerde formulering belangrijk. Niet iedere clouddienst kent hetzelfde risicoprofiel. Factoren zoals gegevensclassificatie, kritikaliteit van de dienstverlening, verwerking van persoonsgegevens, afhankelijkheid van ketenpartijen, exitmogelijkheden en continuïteitsimpact zouden richtinggevend moeten zijn bij de keuze voor het niveau Basis, Substantieel of Hoog.
NOREA adviseert wel om het toepassingsgebied in de adoptieondersteuning nader te verduidelijken met praktijkvoorbeelden. Denk aan voorbeelden voor SaaS-oplossingen, IaaS/PaaS-diensten, hybride cloud, managed services en situaties waarin een ICT-product slechts gedeeltelijk cloudfunctionaliteit bevat."

2.2.3. Vraag 3

Geef hier indien gewenst uw reactie op het geformuleerde nut en de geformuleerde mogelijkheden van het gebruik van NVN-CEN/TS 18026, versie 2024: EN voor en door de overheid (hoofdstuk 2, paragraaf 2 van het expertadvies).

"NOREA onderschrijft het geformuleerde nut van de standaard. De standaard kan bijdragen aan betere vraagarticulatie in aanbestedingen, uniformering van beveiligingseisen, versterking van cybersecurity bij clouddiensten en vermindering van versnippering van eisen binnen de Europese markt. Het expertadvies benoemt expliciet dat uniforme eisen kunnen helpen om beveiliging helder uit te vragen in aanbestedingen en versnippering van veiligheidsvoorschriften binnen de EU te beperken.
Vanuit IT-auditperspectief is de meerwaarde vooral gelegen in het creëren van een gemeenschappelijk referentiekader. Dit kan helpen bij inkoop, contractmanagement, leveranciersbeoordeling, auditplanning, assurance-opdrachten en periodieke monitoring van cloudbeveiliging.
NOREA adviseert om bij adoptie nadrukkelijk aandacht te besteden aan de vertaling naar assurance. Overheidsorganisaties moeten niet alleen eisen kunnen stellen, maar ook kunnen vaststellen of leveranciers aantoonbaar aan die eisen voldoen."

2.2.4. Vraag 4

Geef hier indien gewenst uw reactie op het doorlopen proces van het expertadvies (hoofdstuk 3 van het expertadvies).

"NOREA heeft waardering voor het gevolgde proces. Uit het expertadvies blijkt dat het Ministerie van Economische Zaken en Klimaat de standaard op 6 mei 2025 heeft aangemeld, dat een intakegesprek is gevoerd, dat het Forum Standaardisatie op 11 februari 2026 heeft

besloten de aanmelding in procedure te nemen en dat de expertgroep op 11 mei 2026 bijeen is gekomen.
Het proces lijkt zorgvuldig en transparant te zijn ingericht. Positief is dat in de expertsessie expliciet aandacht is besteed aan onder meer het functioneel toepassingsgebied, mogelijke alternatieve standaarden, draagvlak onder clouddienstproviders, leveranciersafhankelijkheid, digitale autonomie en toepassing bij gemeenten en waterschappen.
NOREA adviseert wel om in het vervolgproces aanvullende vertegenwoordiging te betrekken vanuit IT-audit, internal audit, privacy, informatiebeveiliging, procurement en assurance. Daarmee wordt geborgd dat de standaard niet alleen normatief juist is, maar ook praktisch toetsbaar en controleerbaar wordt."

2.2.5. Vraag 5

Geef hier indien gewenst uw reactie op de samenstelling van de expertgroep (hoofdstuk 4 van het expertadvies).

"NOREA constateert dat de expertgroep bestond uit vertegenwoordigers van onder meer CIP, RDI, SURF, ODC-Noord en DINL, onder onafhankelijk voorzitterschap van InnoValor Advies. Deze samenstelling bevat relevante expertise vanuit overheid, infrastructuur, cloud en digitale dienstverlening. Tegelijkertijd adviseert NOREA om bij vervolgtrajecten aanvullende expertise vanuit NOREA te betrekken op het gebied van IT-audit, assurance, compliance, privacy, aanbesteding en leveranciersmanagement.
De standaard zal in de praktijk immers niet alleen worden gebruikt als technisch beveiligingskader, maar ook als toetsingskader in aanbestedingen, contracten, audits, leveranciersbeoordelingen en mogelijk toekomstige certificeringstrajecten. Daarvoor is betrokkenheid vanuit het audit- en assurance-domein wenselijk.
Het betrekken van NOREA draagt bij aan de kwaliteit en toepasbaarheid van de standaard, doordat vanuit het perspectief van IT-auditors expliciet wordt gekeken naar toetsbaarheid, controleerbaarheid en aansluiting op bestaande assurancepraktijken (zoals NOREA-richtlijn 3000/3402, ook SOC-rapportages genoemd). Daarnaast kan NOREA bijdragen aan het vertalen van de standaard naar praktische toepassing in governance-, risk- en complianceprocessen, waardoor de standaard niet alleen normatief sterk is, maar ook effectief implementeerbaar en aantoonbaar werkend in de praktijk."

2.2.6. Vraag 6

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium "Toegevoegde waarde" (hoofdstuk 5, paragraaf 1 van het expertadvies).

"NOREA onderschrijft de conclusie dat NVN-CEN/TS 18026:2024 EN toegevoegde waarde heeft. De standaard bouwt voort op bestaande kaders zoals ISO/IEC 27001 en ISO/IEC 27002, maar werkt deze specifieker uit voor cloudomgevingen. Het expertadvies geeft aan dat de standaard specifieke en gedetailleerde eisen voor clouddiensten bevat en daarmee aanvullende handvatten biedt voor cloudbeveiliging.
Voor NOREA is vooral relevant dat de standaard kan bijdragen aan eenduidigheid in normenkaders en toetscriteria. Overheidsorganisaties gebruiken nu vaak een combinatie van

BIO, ISO 27001/27002, contractuele beveiligingseisen, cloudcontrols, privacyvereisten en sectorspecifieke kaders. NVN-CEN/TS 18026 kan helpen om cloudspecifieke eisen consistenter te structureren.
Wel moet worden voorkomen dat de standaard wordt gezien als vervanging van bestaande governance-, risk- en complianceverplichtingen. De standaard moet worden gepositioneerd als cloudspecifieke aanvulling binnen een breder stelsel van informatiebeveiliging, risicomanagement, privacy en assurance."

2.2.7. Vraag 7

Heeft NVN-CEN/TS 18026:2024 EN meerwaarde ten opzichte van bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname (hoofdstuk 5, vraag 5.1.3.3)?

"NOREA onderschrijft voorzichtig de conclusie dat er geen direct concurrerende standaard bekend is die op dit moment hetzelfde doel en toepassingsgebied afdekt. Het expertadvies stelt dat er geen andere bestaande concurrerende standaarden bekend zijn die in aanmerking zouden kunnen komen voor opname.
Tegelijkertijd is het belangrijk om de verhouding tot bestaande kaders goed te blijven duiden. In de praktijk werken organisaties al met onder meer ISO/IEC 27001, ISO/IEC 27002, BIO, SOC 2, ISAE 3402/3000-rapportages, CSA CCM, C5 en sectorspecifieke cloudvereisten. NVN-CEN/TS 18026 heeft meerwaarde als deze kaders niet worden verdrongen, maar juist worden verbonden via mappings, guidance en assuranceafspraken.
NOREA adviseert daarom om bij adoptie een overzicht te ontwikkelen waarin de relatie tussen NVN-CEN/TS 18026 en bestaande normen, frameworks en assurance-rapportages inzichtelijk wordt gemaakt."

2.2.8. Vraag 8

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium "Open standaardisatieproces" (hoofdstuk 5, paragraaf 2 van het expertadvies).

"NOREA onderschrijft de conclusie dat de standaard voldoet aan het criterium Open standaardisatieproces. Het expertadvies beschrijft dat de documentatie beschikbaar is via NEN, dat het ontwikkel- en beheerproces via CEN/CENELEC inzichtelijk is, dat inspraak en bezwaarprocedures zijn geborgd en dat periodieke evaluatie van de standaard plaatsvindt.
Wel merkt NOREA op dat praktische toegankelijkheid meer omvat dan formele beschikbaarheid. Voor brede adoptie binnen de overheid en bij kleinere leveranciers is het belangrijk dat er laagdrempelige implementatiehandreikingen, samenvattingen, mappings en praktijkvoorbeelden beschikbaar komen.
NOREA adviseert daarom om naast de formele standaard ook praktische adoptie-instrumenten te ontwikkelen, bij voorkeur publiek beschikbaar en afgestemd op verschillende doelgroepen zoals inkopers, CISO's, auditors, contractmanagers en leveranciers."

2.2.9. Vraag 9

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium "Draagvlak" (hoofdstuk 5, paragraaf 3 van het expertadvies).

"NOREA onderschrijft de genuanceerde conclusie dat het criterium Draagvlak nog niet volledig is ingevuld. Het expertadvies stelt dat meerdere belangrijke overheidsstakeholders de adoptie ondersteunen, maar dat er nog geen zicht is op de mate waarin gemeenten, waterschappen, provincies en uitvoeringsorganisaties de adoptie ondersteunen.
Ook wordt vastgesteld dat meerdere leveranciers op dit moment nog niet aantoonbaar ondersteuning bieden voor de standaard en dat de toepassing op zekerheidsniveau Hoog mogelijk slechts haalbaar is voor een beperkt aantal grote leveranciers.
NOREA vindt dit een belangrijk aandachtspunt. Draagvlak moet niet alleen worden gemeten bij beleidsdepartementen en grote marktpartijen, maar ook bij decentrale overheden, uitvoeringsorganisaties, kleinere cloudleveranciers, auditors en inkoopprofessionals. Wij adviseren om het draagvlak periodiek te monitoren en expliciet mee te nemen in de verdere adoptieroadmap."

2.2.10. Vraag 10

Bieden meerdere leveranciers ondersteuning voor NVN-CEN/TS 18026:2024 EN> Daarbij wordt opgemerkt dat de toepassing van deze standaard voor het zekerheidsniveau 'Hoog', gelet op de gestelde eisen, mogelijk slechts haalbaar is voor een beperkt aantal grote leveranciers. Dit kan ertoe leiden dat de afhankelijkheid van een klein aantal grote clouddienstverleners toeneemt indien gebruikers kiezen voor het hoogste zekerheidsniveau (hoofdstuk 5, vraag 5.3.2.1).

"NOREA deelt de zorg dat het zekerheidsniveau Hoog in de praktijk mogelijk slechts haalbaar is voor een beperkt aantal grote leveranciers. Het expertadvies benoemt expliciet dat toepassing op niveau Hoog, gezien de gestelde eisen, mogelijk alleen haalbaar is voor een beperkt aantal grote leveranciers en dat dit de afhankelijkheid van een klein aantal grote clouddienstverleners kan vergroten.
Dit vraagt om een zorgvuldige, proportionele toepassing. Overheidsorganisaties zouden niet standaard het hoogste niveau moeten eisen, maar eerst een expliciete risicobeoordeling moeten uitvoeren. Het niveau Hoog zou vooral passend zijn bij clouddiensten met zeer hoge eisen aan vertrouwelijkheid, integriteit, beschikbaarheid, continuïteit, publieke taakuitvoering of nationale veiligheid.
NOREA adviseert om in de adoptiehandreiking duidelijke criteria op te nemen voor de keuze tussen Basis, Substantieel en Hoog. Daarbij moet ook aandacht zijn voor markteffecten, vendor lock-in, exitmogelijkheden, dataportabiliteit, auditrechten en de positie van Nederlandse en Europese cloudleveranciers."

2.2.11. Vraag 11

Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard? (vraag 5.3.3.1 van het expertadvies)?

"NOREA constateert dat belangrijke stakeholders zoals RDI, BZK en JenV achter adoptie staan, en dat ook de Online Trust Coalitie betrokken is als publiek-private samenwerking op het gebied van clouddiensten.
Tegelijkertijd blijkt uit het expertadvies dat er nog geen volledig zicht is op steun vanuit waterschappen, gemeenten, provincies en uitvoeringsorganisaties.
NOREA adviseert daarom om adoptie niet top-down te benaderen, maar te combineren met actieve consultatie en ondersteuning van decentrale overheden en uitvoeringsorganisaties. Juist deze organisaties beschikken vaak over beperkte capaciteit voor cloudrisicomanagement, leveranciersbeoordelingen en technische norminterpretatie."

2.2.12. Vraag 12

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

"NOREA onderschrijft de conclusie dat deze vraag op dit moment niet van toepassing is, omdat het voorstel ziet op plaatsing op de lijst Aanbevolen en niet op verplichte toepassing via'Pas toe of leg uit'.
NOREA acht dat juist. Gezien de huidige stand van adoptie, toetsbaarheid en certificering is verplichtstelling nog niet passend. Eerst moet ervaring worden opgedaan met toepassing in aanbestedingen, contracten, leveranciersbeoordelingen en assuranceprocessen.
Een eventuele latere verplichting zou pas moeten worden overwogen nadat EUCS-certificering formeel is vastgesteld, implementatieprofielen beschikbaar zijn, voldoende marktpartijen ondersteuning bieden en er een volwassen toetsings- of assurancemechanisme bestaat."

2.2.13. Vraag 13

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

"NOREA neemt kennis van de conclusie dat de standaard voor zover bekend nog niet door meerdere Nederlandse overheidsorganisaties wordt gehanteerd als eis in aanschaf- en doorontwikkeltrajecten.
Dit bevestigt dat de status Aanbevolen passend is. De standaard bevindt zich nog in een vroege adoptiefase. Het is verstandig om eerst praktijkervaring op te bouwen voordat wordt overgegaan tot verdergaande verplichtingen.
NOREA adviseert om pilots te stimuleren bij verschillende typen organisaties, bijvoorbeeld Rijk, uitvoeringsorganisaties, gemeenten, waterschappen en instellingen in de semipublieke sector. De resultaten daarvan kunnen worden gebruikt voor nadere guidance, mappings, good practices en besluitvorming over eventuele toekomstige verplichtstelling."

2.2.14. Vraag 14

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

"NOREA onderschrijft dat er positieve signalen zijn over toekomstig gebruik. Het expertadvies noemt onder meer signalen vanuit OTC, Dutch Cloud Community, NEN, Eurosmart en marktpartijen in de clouddienstverlening.
Deze signalen zijn waardevol, maar moeten worden omgezet in aantoonbare adoptie. Voor NOREA is daarbij vooral van belang dat toekomstig gebruik niet alleen beleidsmatig wordt gestimuleerd, maar ook praktisch wordt ondersteund met toetsbare criteria, voorbeeldclausules, aanbestedingsteksten, risicobeoordelingsmodellen en assurance-aanwijzingen.
Daarmee kan de standaard daadwerkelijk landen in de dagelijkse praktijk van cloudinkoop, contractmanagement, leveranciersmonitoring en audit."

2.2.15. Vraag 15

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium "Opname op de lijst bevordert adoptie" (hoofdstuk 5, paragraaf 4 van het expertadvies).

"NOREA onderschrijft de conclusie dat opname op de lijst Aanbevolen adoptie kan bevorderen. Het expertadvies stelt dat deze status op dit moment het passende middel is, omdat EUCS-certificering nog niet is afgerond en omdat opname bekendheid en ervaring binnen de overheid kan opbouwen.
NOREA vindt dit een evenwichtige benadering. De standaard is relevant genoeg om actief onder de aandacht te brengen, maar nog niet volwassen genoeg voor brede verplichtstelling. Wel adviseren wij om de plaatsing op de lijst Aanbevolen te koppelen aan concrete adoptiedoelstellingen. Denk aan het aantal pilots, beschikbare handreikingen, mappings met bestaande kaders, betrokkenheid van decentrale overheden en evaluatie van markteffecten."

2.2.16. Vraag 16

Geef hier indien gewenst uw reactie op de aanvullende adoptieadviezen bij verplichting van NVN-CEN/TS 18026, versie 2024: EN door plaatsing op de lijst Aanbevolen (hoofdstuk 6 van het expertadvies).

"NOREA ondersteunt de aanvullende adoptieadviezen uit het expertadvies. Daarin wordt onder meer geadviseerd dat het Ministerie van Economische Zaken en Klimaat de promotie van de standaard ondersteunt, dat de standaard na vaststelling van EUCS opnieuw wordt aangemeld voor toetsing voor de lijst 'Pas toe of leg uit', en dat het Forum Standaardisatie nader reflecteert op begrippen als autonomie, digitale soevereiniteit en leveranciersafhankelijkheid.
NOREA adviseert hieraan toe te voegen:
1. ontwikkel een praktische implementatiehandreiking voor overheidsorganisaties;
2. maak mappings met BIO, ISO 27001/27002, SOC 2, ISAE 3000/3402, CSA CCM en relevante privacy- en continuïteitskaders;
3. ontwikkel guidance voor assurance en auditbaarheid;
4. monitor de impact op leveranciersafhankelijkheid en marktdynamiek;
5. stimuleer pilots bij verschillende typen overheidsorganisaties;

6. betrek IT-auditors, internal auditors, CISO's, privacy officers en inkopers bij verdere uitwerking."

2.2.17. Vraag 17

Geef hier indien gewenst uw reactie op de vraag hoe NVN-CEN/TS 18026:2024 EN kan bijdragen aan het versterken van de digitale autonomie van de Nederlandse overheid.

"NVN-CEN/TS 18026 kan bijdragen aan digitale autonomie door een uniform Europees referentiekader te bieden voor cloudbeveiliging. Hierdoor kunnen overheidsorganisaties beter onderbouwde keuzes maken, leveranciers consistenter beoordelen en beveiligingseisen eenduidiger opnemen in aanbestedingen en contracten.
Het expertadvies geeft echter terecht aan dat de standaard zelf geen specifieke bepalingen bevat die interoperabiliteit bevorderen of leveranciersafhankelijkheid rechtstreeks verminderen. Het effect op leveranciersafhankelijkheid en interoperabiliteit is daarmee beperkt.
NOREA ziet de bijdrage aan digitale autonomie daarom vooral als indirect. De standaard kan helpen bij transparantie, vergelijkbaarheid, risicobeheersing en professionele vraagarticulatie. Maar digitale autonomie vraagt daarnaast ook aandacht voor exitstrategie, dataportabiliteit, contractuele auditrechten, ketentransparantie, Europese alternatieven, governance over uitbesteding en strategisch leveranciersmanagement.
Wij adviseren daarom om NVN-CEN/TS 18026 te positioneren als één bouwsteen binnen een bredere strategie voor digitale autonomie, niet als zelfstandig instrument dat afhankelijkheden oplost."

2.2.18. Vraag 18

Geef hier indien gewenst uw aanvullend commentaar aan het Forum Standaardisatie in verband met de inhoud van dit expertadvies en/of het gevolgde proces.

"NOREA waardeert het expertadvies en ondersteunt de voorgestelde plaatsing op de lijst Aanbevolen. De standaard is relevant, actueel en kan bijdragen aan meer eenduidigheid in beveiligingseisen voor clouddiensten binnen de overheid.
Tegelijkertijd adviseert NOREA om nadrukkelijk aandacht te besteden aan de praktische uitvoerbaarheid en auditbaarheid. Voor effectieve adoptie is het noodzakelijk dat overheidsorganisaties niet alleen weten dát zij de standaard kunnen gebruiken, maar ook hóe zij deze kunnen toepassen, beoordelen en laten toetsen.
NOREA adviseert het Forum Standaardisatie daarom om bij plaatsing op de lijst Aanbevolen de volgende randvoorwaarden mee te geven:
• pas de standaard risicogebaseerd en proportioneel toe;
• voorkom dat niveau Hoog onbedoeld leidt tot verdere concentratie bij enkele hyperscalers;
• ontwikkel praktische guidance voor aanbesteding, contractering, monitoring en assurance;
• stimuleer pilots en praktijkvoorbeelden;
• betrek audit- en assurance-expertise bij vervolguitwerking;
• evalueer periodiek de effecten op adoptie, marktdynamiek, leveranciersafhankelijkheid en digitale autonomie.

Met deze aanvullingen kan NVN-CEN/TS 18026:2024 EN uitgroeien tot een waardevol instrument voor betrouwbare, veilige en controleerbare inzet van clouddiensten binnen de Nederlandse overheid.”Reacties uit de openbare consultatie”

2.3. Reactie van Anoniem (Microsoft)

Schiphol

Datum: 31 juli 2026

De reactie is aangeleverd in de vorm van een brief (zie Bijlage 3).

Gemeente Rotterdam

Datum: 28 juli 2026

Betreft: Reactie Gemeente Rotterdam op consultatie Forum Standaardisatie voor NVN-CEN/TS 18026

Van: Nico Noorland, Jan Stedehouder

Vanuit de gemeente Rotterdam hebben we de volgende reactie op de consultatie van het Forum Standaardisatie op de technische specificatie NVN-CEN/TS 18026. Deze specificatie beschrijft veiligheidseisen voor clouddiensten.

- Wij onderschrijven het belang van deze technische specificatie en ondersteunen de aanbeveling om deze op de lijst Aanbevolen van het Forum Standaardisatie te plaatsen.
- We ondersteunen ook het advies om, zodra de EUCS-certificering is vastgesteld, de norm opnieuw aan te melden voor toetsing voor plaatsing op de 'Pas toe of leg uit'-lijst.

Wij hebben wel de volgende reacties op op het expertadvies.

- In het expertadvies staat dat: "Er geen zicht (is) op de mate waarin waterschappen, gemeenten, provincies en uitvoeringsorganisaties de adoptie van de standaard ondersteunen". Dit is wat ons betreft een serieuze omissie in het traject om tot dit advies te komen. Los van de ministeries zijn dit de voornaamste partijen die de norm moeten gaan hanteren bij hun inkooptrajecten. Het ontbreken van een vertegenwoordiging van deze partijen, al dan niet via het Waterschapshuis, IPO en/of VNG, in vermindert sterk de representativiteit en evenwichtigheid van de expertgroep.

- Het expertadvies begint onder andere met de vraag: "Aandacht voor hoe NVN-CEN/TS 18026:2024 EN bijdraagt aan meer digitale autonomie voor de Nederlandse overheid", om vervolgens deze vraag niet te beantwoorden. In het advies wordt wel gesteld dat: "Aan Forum Standaardisatie (wordt geadviseerd) 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". Maar tussen het stellen van de onderzoeksvraag en het advies in de slotparagraaf wordt het onderwerp in het expertadvies niet aangeraakt, anders dan wellicht de korte opmerking over de bijdrage aan interoperabiliteit en de opmerking dat voor het beveiligingsniveau Hoog het risico bestaat van een beperkt aantal aanbieders. Het kan zijn dat de onduidelijkheid over deze begrippen het beantwoorden van de onderzoeksvraag heeft verhinderd, maar dan nog was een meer expliciete en uitgebreider behandeling op haar plaats geweest.

Wij adviseren dan ook om bij een volgende toetsing van deze technische specificatie voor plaatsing op de 'Pas toe of leg uit'-lijst deze omissies op te lossen.

Met vriendelijke groet

Nico Noorland, Strategisch adviseur informatieveiligheid
Jan Stedehouder, Lead architect Rotterdams (Federatief) Datastelsel

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Microsoft Position on NVN-CEN/TS 18026:2024

Microsoft supports the Netherlands' objective of strengthening cybersecurity assurance for cloud services and welcomes efforts to promote secure and trusted cloud adoption across the public sector. We believe cybersecurity standards play an important role in enabling trust, transparency, and resilience across Europe's digital ecosystem.

International Standards

Microsoft supports building on internationally recognized and widely adopted standard like ISO/IEC 27001 and ISO/IEC 27002, which are already on the list of 'mandatory standards' (Past-toe-of-leg-uit). These standards provide mature and globally accepted approaches to cloud security assurance, support interoperability across jurisdictions, and help organizations benefit from consistent security practices across international markets. Specifically for Cloud Service Providers and Cloud Service Customers it would be helpful to add ISO/IEC 27017 to the list, as it builds on the ISO/IEC 27001 and ISO/IEC 27002 standards.

Security Outcomes

Cybersecurity assurance frameworks should remain focused on objective, risk-based, and technically robust measures that strengthen security in practice.

Effective and Implementable Frameworks

Certification frameworks deliver the greatest value when they are supported by practical implementation experience, clear governance, and broad stakeholder participation. As discussions on EUCS continue at the European level, ongoing work on EUCS would benefit from further implementation experience, market validation, and transparent stakeholder engagement.

Regulatory Coherence

Cybersecurity certification should support a coherent European cybersecurity framework and remain focused on improving security in practice.

Conclusion

Microsoft supports efforts to strengthen cybersecurity assurance for cloud services across Europe. Consistent with the Non-Paper on the Review of the Cyber Security Act and Microsoft's position on the revision of the EU Cybersecurity Act (CSA 2.0), we encourage an approach that promotes international interoperability, effective assurance mechanisms, regulatory coherence, meaningful cybersecurity outcomes, and broad stakeholder participation. Microsoft considers it premature to include NVN-CEN/TS 18026:2024 on either the recommended standards list or the mandatory "apply-or-explain" list. As discussions on the EUCS continue at the European level, further work may be needed to clarify its scope, implementation, and relationship with existing international standards. In the meantime, Microsoft recommends relying on mature, internationally recognized standards, including ISO/IEC 27001 and ISO/IEC 27017. Such an approach will best support secure cloud adoption, effective public procurement, innovation, competition, and a resilient European digital ecosystem.