



NCC-BE CYBERSECURITY OPROEP 2025 “FUNDING FOR CYBER” – OPEN VAN 8 OKTOBER 2025 TOT 8 DECEMBER 2025

Inhoud

NCC-BE CYBERSECURITY OPROEP 2025 “FUNDING FOR CYBER”	1
Doel van dit document	1
A. Inleiding	1
B. Beschrijving van de oproep “Funding for Cyber” en de toelatingscriteria	2
C. Aanvraag- en beoordelingsprocedure	9
D. Monitoring, rapportage en terugbetaling	11
E. Gegevensbescherming	12
F. Contactgegevens	12

Doel van dit document

Het doel van dit document is om de referentiekaders te schetsen voor de NCC-BE cybersecurity cascade financieringsoproep 2025 “Funding for Cyber”. Dit document schetst de context van de oproep, de toelatingscriteria en de aanvraag-, beoordelings- en toekenningsprocedure.

Dit document biedt potentiële subsidieaanvragers alle relevante informatie over het financieringsprogramma. Het beschrijft ook de voorwaarden waarmee rekening moet worden gehouden alvorens een aanvraag in te dienen.

Dit document heeft tot doel om, in duidelijke taal, richtlijnen voor deelnemers aan het subsidieprogramma uiteen te zetten en om eerlijkheid, transparantie en gelijke kansen te waarborgen.

A. Inleiding

1. Het Nationaal Cybersecurity Coördinatiecentrum België (NCC-BE)

De Belgische regering heeft het Nationaal Cybersecurity Coördinatiecentrum België (NCC-BE) opgericht krachtens artikel 6 van Verordening 2021/887 binnen het Centrum voor Cybersecurity België (CCB) bij koninklijk besluit van 16 februari 2022 (tot wijziging van het koninklijk besluit van 10 oktober 2014 tot oprichting van het CCB).



De ambitie van de Belgische regering is dat het NCC-BE de voorkeurspartner wordt op het gebied van cybersecurity van alle belanghebbenden, zowel uit de publieke als de private sector, op lokaal, gewestelijk en nationaal niveau. Daarnaast vervult het NCC-BE een proactieve en dynamische rol binnen het kader van het European Cybersecurity Competence Centre (ECCC) en binnen het netwerk van NCC's. Dit zal het Belgische cybersecurity ecosysteem versterken, bijdragen tot grensoverschrijdende samenwerking met andere NCC's waar relevant, en nieuwe groei op het vlak van digitalisering en beveiliging helpen realiseren. Bovendien zal dit het digitale concurrentievermogen van België en bij uitbreiding dat van de Europese Unie vergroten.

2. Digital Europe Programme

De oproep “Funding for Cyber” wordt gedeeltelijk gefinancierd door het Digital Europe Programme (DEP) en medegefinancierd door het Centrum voor Cybersecurity België. Het DEP heeft financiering toegekend aan het Centrum voor Cybersecurity België in het kader van de oproep DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION. Het NCC-BE wil een veilig digitaal landschap creëren, de nationale veerkracht versterken en de capaciteit om op cyberincidenten te reageren, verbeteren. Elk project, elke mijlpaal en deliverable die een aanvrager voorstelt, is in lijn met de doelstellingen zoals uiteengezet in het officiële oproepdocument.

Strategische afstemming

Dit financieringsprogramma ondersteunt de taken en verantwoordelijkheden die aan NCC's zijn toegewezen krachtens Verordening (EU) 2021/887, met de nadruk op het versterken van kritieke digitale capaciteiten en het bevorderen van kennis en innovatie op het gebied van cybersecurity. Bovendien sluit het financieringsprogramma aan bij de Belgische Cybersecurity Strategie en zal het blijven evolueren in reactie op nieuwe cyberdreigingen en -uitdagingen.

B. Beschrijving van de oproep “Funding for Cyber” en de toelatingscriteria

1. Beschrijving van de oproep “Funding for Cyber”

Het doel van deze financiële steun is om Belgische begunstigden, zoals start-ups, scale-ups, kmo's¹ en/of mid-caps, te helpen bij de invoering of ontwikkeling van digitale innovatie. De sub-subsidieovereenkomst tussen de begunstigde van de financiële steun en het CCB (NCC-BE) moet “de invoering en verspreiding van state-of-the-art cybersecurity oplossingen door kmo's” ondersteunen.

a. Thema van het financieringsprogramma

Het thema van deze oproep is “Ontwikkeling van infrastructuur of digitale bewustmakingsinstrumenten met behulp van state-of-the-art technologieën die essentiële mogelijkheden bieden op het gebied van cybersecurity voor kmo's”. Dit thematische onderwerp kan onder meer de volgende aspecten omvatten, maar is niet beperkt tot:

¹ Kleine en middelgrote ondernemingen (kmo's) worden gedefinieerd in Aanbeveling 2003/361/EG van de Commissie en worden ingedeeld op basis van het aantal werknemers, de jaaromzet en het balanstotaal. Een kmo moet minder dan 250 werknemers hebben en een jaaromzet van maximaal 50 miljoen euro of een balanstotaal van maximaal 43 miljoen euro. Verdere onderverdelingen zijn kleine ondernemingen (< 50 werknemers, ≤ 10 miljoen euro omzet of balanstotaal) en micro-ondernemingen (< 10 werknemers, ≤ 2 miljoen euro omzet of balanstotaal).

- het creëren van infrastructuren die cloudcomputing-diensten, gratis gegevensback-ups en/of een betrouwbaar domeinnaamsysteem bieden;
- het creëren van oplossingen voor multi-factor authenticatie;
- het creëren van IT-oplossingen voor cybersecurity-bewustmaking op basis van artificiële intelligentie, met behulp van interactieve lessen en/of game-based leertechnieken, waarbij gebruikers hun voortgang kunnen volgen.

b. Beoogde begunstigden

De primaire doelgroep van dit financiële steunprogramma zijn organisaties (particuliere bedrijven, kmo's, start-ups – niet-uitputtende lijst) die aantoonbare expertise hebben op het gebied van:

- (a) het creëren en leveren van inhoud om de cybersecurity-bewustmaking te vergroten, of
- (b) de ontwikkeling en implementatie van cybersecurity gerelateerde infrastructuur op maat van kleine en middelgrote ondernemingen (kmo's).

Deze begunstigde organisaties zullen steun ontvangen voor het ontwerpen, implementeren of opschalen van oplossingen die gericht zijn op het verbeteren van de cybersecurity van kmo's.

c. Eindgebruikers

Hoewel de directe ontvangers van de financiële steun de hierboven genoemde deskundige organisaties zijn, zijn de uiteindelijke begunstigden/eindgebruikers van de ondersteunde oplossingen Belgische kmo's. Deze kmo's zullen naar verwachting profiteren van:

- (a) betere toegang tot gebruiksvriendelijke digitale bewustmakingsinstrumenten – die helpen om personeel te informeren over veilige cyberpraktijken, of
- (b) de invoering van essentiële cybersecurity infrastructuur die hun digitale veerkracht vergroot.

d. Begroting en betalingsregeling

De subsidie per begunstigde bedraagt 60 000 EUR, met een maximum van zes subsidies (één per aanvrager), wat neerkomt op een totaalbedrag van 360 000 EUR. De minimale projectkosten bedragen 60 000 EUR. Het budget wordt berekend op basis van de geraamde subsidiabele directe kosten (personeelskosten, kosten voor onderaanneming, aankoopkosten, andere kostencategorieën). De subsidie wordt uitbetaald in de vorm van:

- een voorschot van 45 000 EUR na het besluit tot toekenning van de subsidie en binnen 30 kalenderdagen na verstrekking van een ondertekend exemplaar van de subsidietoekenning,
- een eindbetaling of terugvordering die overeenkomt met de aanvaarde subsidiabele kosten (gemaakt vanaf de datum van publicatie van deze oproep tot 11 december 2025) na indiening van het ingevulde verslag, de terugbetalingsaanvraag en de bewijsstukken, op voorwaarde dat de ingediende documenten door het CCB worden goedgekeurd.

Het maximale subsidiebedrag van 60 000 EUR mag niet worden overschreden. Bij projecten waarvan de totale kosten hoger zijn dan het maximale subsidiebedrag, moeten de begunstigden het bedrag bovenop het maximale subsidiebedrag zelf financieren.

e. Periode voor indiening van subsidieaanvragen

De oproep "Funding for Cyber" gaat open op 8 oktober 2025 en blijft open gedurende een periode van 60 kalenderdagen, zoals vereist door de Europese Commissie. De deadline voor het indienen van aanvragen is 8 december 2025. Alle gevraagde documentatie moet vóór deze datum worden ingediend om te worden beoordeeld. Aanvragen die te laat zijn ingediend worden niet in behandeling genomen.

f. Uitvoering

De acties voor projecten die worden gefinancierd in het kader van de cascade financieringsoproep moeten ten minste worden uitgevoerd gedurende de periode waarin de kosten subsidiabel zijn. Aan het einde van deze periode moeten begunstigden ervoor zorgen dat de beschreven acties in de 'beschrijving van de actie' zijn uitgevoerd zoals overeengekomen in de sub-subsidieovereenkomst. De desbetreffende kosten moeten uiterlijk op 31 december 2025 worden gedeclareerd. Begunstigden moeten ervoor zorgen dat alle verslagen, verzoeken om terugbetaling en ondersteunende documentatie uiterlijk op deze datum zijn ingediend.

g. Regelgevend kader

Verordening (EU, Euratom) 2024/2509 van het Europees Parlement en de Raad van 23 september 2024 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie.

<http://data.europa.eu/eli/reg/2024/2509/oj>

Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het Digital Europe Programme (DEP). Deze verordening stelt een financieel kader vast voor het Digital Europe Programme voor de periode 2021-2027.

<http://data.europa.eu/eli/reg/2021/694/2025-02-04> (geconsolideerde wet)²

Financiële steun wordt toegekend overeenkomstig Verordening (EU) 2023/2831 van de Commissie van 13 december 2023 betreffende de toepassing van de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie op de minimis-steun.

Koninklijk besluit van 1 oktober 2025 tot vaststelling van de voorwaarden voor het toekennen van subsidies voor de uitvoering van projecten voor de ontwikkeling van infrastructuur of digitale instrumenten die de cybersecurity capaciteiten van kmo's verbeteren.

<https://www.ejustice.just.fgov.be/eli/bsluit/2025/10/01/2025007335/justel>

2. Toelatingscriteria

De toelatingscriteria voor cascade financiering worden vastgesteld in overeenstemming met de toelatingscriteria die overeenkomen met de oproep DIGITAL-2022-CYBER-03.

a. Ontvankelijkheid en bewijsstukken

- Voorstellen moeten vóór de uiterste indieningsdatum worden ingediend. Alle aanvragen en bewijsstukken moeten uiterlijk op 8 december 2025 ontvangen zijn.
- Voorstellen moeten elektronisch worden ingediend via email via het emailadres ncc@ccb.belgium.be, met behulp van de verstrekte template, dat toegankelijk is via de [NCC-BE pagina](#) op de CCB-website en onder de cascade financieringsoproep op het EU Funding & Tenders Portal.
- Voorstellen (inclusief bijlagen en bewijsstukken) moeten worden ingediend volgens de instructies op de NCC-BE pagina van de CCB-website en op het EU Funding & Tenders Portal.
- Voorstellen moeten volledig zijn en alle gevraagde informatie, alle vereiste bijlagen en bewijsstukken bevatten, zoals aangegeven op de NCC-BE pagina van de CCB-website en op het EU Funding & Tenders Portal.

² De oorspronkelijke wet is te raadplegen via de volgende link: <http://data.europa.eu/eli/reg/2021/694/oj>.

- Het voorstel moet het volgende bevatten:
 - 1) een kopie van de statuten van de entiteit;
 - 2) een ingevulde en ondertekende verklaring inzake eigendom en zeggenschap, op grond waarvan de NCC-BE een beoordeling van eigendom en zeggenschap (OCA) kan uitvoeren overeenkomstig artikel 12, § 5, van bovengenoemde Verordening (EU) 2021/694;
 - 3) een beschrijving van het project, met name het doel, de doelgroep en de geschatte ontwikkelingstijd, volgens de template op de NCC-BE pagina van de CCB-website;
 - 4) een raming van de kosten van het project, met vermelding van de subsidiabele kosten (zie punt “c. Financiële draagkracht”);
 - 5) een verklaring waarin wordt bevestigd dat er geen sprake is van dubbele financiering voor de projectactiviteiten;
 - 6) alle feitelijke of juridische informatie voor de beoordeling van het expertise niveau van de entiteit op het gebied van cybersecurity-bewustmaking of infrastructuurcreatie voor kmo's;
 - 7) alle feitelijke of juridische gegevens voor de beoordeling van de financiële draagkracht van de entiteit om de ontwikkeling van het project bedoeld in 3) te ondersteunen, zoals gespecificeerd in punt “c. Financiële draagkracht” van dit document.
- De persoon die het voorstel indient, moet bevoegd zijn om namens de indienende entiteit(en) op te treden.
- Voorstellen moeten leesbaar, toegankelijk en afdrukbaar zijn.

b. Deelnemers die in aanmerking komen

De beoogde begunstigden van de oproep “Funding for Cyber” zijn organisaties met expertise op het gebied van cybersecurity-bewustmaking of het opzetten van infrastructuur voor kmo's. De eindgebruikers die baat zouden moeten hebben bij het gebruik van het digitale bewustmakingsinstrument of de infrastructuur zijn Belgische kmo's.

Om in aanmerking te komen, moeten de aanvragers en deelnemers:

- rechtspersonen zijn
- gevestigd zijn in één van de in aanmerking komende landen, namelijk:
 - o EU-lidstaten (met inbegrip van landen en gebieden overzee (LGO)).
 - o EER-landen (Noorwegen, IJsland, Liechtenstein).
- overeenkomstig artikel 12, § 5, van bovengenoemde Verordening (EU) 2021/694 niet direct of indirect gecontroleerd worden vanuit een land dat niet in aanmerking komt
- niet onderworpen zijn aan beperkingen op grond van de bepalingen inzake strategische autonomie van de EU.

Specifieke gevallen

- Internationale organisaties komen niet in aanmerking, tenzij het internationale organisaties van Europees belang zijn in de zin van artikel 2 van de Digital Europe verordening.
- Entiteiten die volgens hun nationale recht geen rechtspersoonlijkheid hebben, kunnen bij wijze van uitzondering deelnemen, op voorwaarde dat hun vertegenwoordigers bevoegd zijn om namens hen juridische verplichtingen aan te gaan en garanties kunnen bieden voor de bescherming van de financiële belangen van de EU die gelijkwaardig zijn aan degene die door rechtspersonen geboden worden.
- EU-organen (met uitzondering van het European Commission Joint Research Centre)

kunnen niet deelnemen.

- Er gelden speciale regels voor entiteiten die onderworpen zijn aan beperkende maatregelen van de EU op grond van artikel 29 van het Verdrag betreffende de Europese Unie (VEU) en artikel 215 van het Verdrag betreffende de werking van de Europese Unie (VWEU) en entiteiten die onder Richtlijn 2013/C 205/0514 van de Commissie vallen. Dergelijke entiteiten komen in geen enkele hoedanigheid in aanmerking voor deelname.

c. Financiële draagkracht

Overeenkomstig artikel 198 van het Financieel Reglement 2018/1046 van de EU en de artikelen 7 en 9 van het koninklijk besluit tot instelling van het subsidieprogramma “Funding for Cyber” moeten aanvragers aantonen dat zij over een stabiele en toereikende financiële draagkracht beschikken om de ontwikkeling van het voorgestelde project te ondersteunen. Dit is een verplichte toelatingsvoorwaarde en aanvragen die niet aan deze voorwaarde voldoen, worden afgewezen.

Financiële draagkracht is vereist om te garanderen dat de aanvrager de ontwikkelingsfase van het project kan ondersteunen zoals beschreven in de aanvraag, in overeenstemming met artikel 7, §1, lid 6, van het koninklijk besluit. De financiële draagkracht zal ook worden beoordeeld als onderdeel van het uitvoeringscriterium zoals uiteengezet in artikel 10, §1, lid 2, van het koninklijk besluit.

d. Bewijsstukken

Elke aanvrager moet als onderdeel van het aanvraagdossier (artikel 7, §1) de volgende documenten indienen voor de beoordeling van de financiële draagkracht:

- Overzicht van het projectbudget (met behulp van de verstrekte template).
- Alle feitelijke of juridische informatie die het mogelijk maakt om de financiële draagkracht van de aanvrager om het project te ondersteunen te beoordelen.

Niet-uitputtende lijst van documenten en informatie die kunnen worden verstrekt:

- Goedgekeurde resultatenrekening.
- Goedgekeurde balans.
- Toelichtingen en/of bijlagen die deel uitmaken van bovenstaande financiële overzichten.
- Extern auditverslag of eigen verklaring.
- In het geval van dochterondernemingen zonder eigen financiële overzichten: geconsolideerde rekeningen en het auditverslag / eigen verklaring van de moedermaatschappij of groep waarvan zij deel uitmaken. Er kunnen aanvullende documenten worden gevraagd om het verband met de moedermaatschappij aan te tonen.
- In het geval van moedermaatschappijen: een vereenvoudigd overzicht van de niet-geconsolideerde winst- en verliesrekening en balans, met inachtneming van de minimale rapportagevereisten, gedateerd en ondertekend door het management.
- In het geval van start-ups: prospectieve gegevens voor één jaar (businessplan).
- In het geval van recent opgerichte entiteiten die nog geen afgesloten rekeningen hebben: documenten voor het enige afgesloten boekjaar of geraamde financiële gegevens (d.w.z. een businessplan of een soortgelijk document met financiële prognoses over vlottende en vaste activa, eigen vermogen, kortlopende en langlopende verplichtingen, omzet, bedrijfs- en financiële baten en lasten).

- In het geval van natuurlijke personen: jaarlijkse aangifte inkomstenbelasting met gegevens over de inkomsten en uitgaven uit bedrijfsactiviteiten.
- In het geval van entiteiten die een kasboekhouding voeren: aangiften ondertekend door de bevoegde wettelijke vertegenwoordiger van de entiteit met informatie over vaste en vlottende activa en over inkomsten en uitgaven. Daarnaast wordt aanbevolen om alle beschikbare bewijsstukken ter staving van de opgegeven bedragen te verstrekken (bijvoorbeeld bankafschriften ter bevestiging van het beschikbare saldo op de afsluitingsdatum van de boekhouding, enz.).
- In het geval van entiteiten die onder een garant staan, financiële gegevens van de garant.

Als de verstrekte financiële informatie onvoldoende duidelijk is, kan de NCC-BE contact opnemen met deelnemers voor nadere toelichting.

e. Evaluatiebasis

Overeenkomstig artikel 10, §1, lid 2, van het koninklijk besluit maakt de beoordeling van de financiële draagkracht deel uit van de evaluatie van de haalbaarheid van de uitvoering. De volgende beginselen zijn van toepassing:

- De aanvrager moet aantonen dat hij de ontwikkeling van het project kan ondersteunen op basis van zijn financiële situatie;
- De beoordeling kan indicatoren omvatten zoals het beschikbare eigen vermogen, de afwezigheid van insolventie en een redelijke verhouding tussen de projectkosten en de omvang van de entiteit;
- Nieuw opgerichte of kleinere aanvragers worden niet automatisch uitgesloten als zij op geloofwaardige wijze kunnen aantonen dat zij het project kunnen uitvoeren.

f. Operationele capaciteit

Aanvragers moeten beschikken over de knowhow, kwalificaties en middelen om de projecten met succes uit te voeren en hun bijdrage te leveren (met inbegrip van voldoende ervaring met projecten op het gebied van cybersecurity bewustzijn of het creëren van infrastructuur voor kmo's). Deze capaciteit wordt beoordeeld samen met het toekenningscriterium 'Uitvoering', op basis van de competentie en ervaring van de aanvragers en hun projectteams, met inbegrip van de operationele middelen (menselijk, technisch en andere).

g. Uitsluiting

Aanvragers die onderworpen zijn aan een uitsluitingsbesluit van de EU of zich in een van de volgende uitsluitingssituaties bevinden waardoor zij geen EU-financiering kunnen ontvangen, kunnen niet deelnemen:

- Faillissement, liquidatie, een gerechtelijk akkoord, onder curatele van de rechtbank, akkoord met schuldeisers, opschorting van bedrijfsactiviteiten of andere soortgelijke procedures (inclusief procedures voor personen die onbeperkt aansprakelijk zijn voor de schulden van de aanvrager).
- Schending van sociale zekerheids- of belastingverplichtingen (inclusief door personen die onbeperkt aansprakelijk zijn voor de schulden van de aanvrager).
- Schuldig aan ernstig beroepsmatig wangedrag (ook indien gepleegd door personen met vertegenwoordigings-, beslissings- of controlebevoegdheid, uiteindelijke begunstigen of personen die essentieel zijn voor de toekenning/uitvoering van de subsidie).
- Fraude, corruptie, banden met een criminele organisatie, witwassen van geld,

- terrorisme-gerelateerde misdrijven (inclusief terrorismefinanciering), kinderarbeid of mensenhandel (ook indien gepleegd door personen met vertegenwoordigings-, beslissings- of controlebevoegdheid, uiteindelijke begunstigen of personen die essentieel zijn voor de toekenning/uitvoering van de subsidie).
- Aanzienlijke tekortkomingen vertonen bij het nakomen van de belangrijkste verplichtingen van een EU-aanbestedingscontract of overheidscontract, subsidieovereenkomst, prijs, deskundigencontract of iets dergelijks (ook indien gepleegd door personen met vertegenwoordigings-, beslissings- of controlebevoegdheid, uiteindelijke begunstigen of personen die essentieel zijn voor de toekenning/uitvoering van de subsidie).
 - Zich schuldig gemaakt aan onregelmatigheden in de zin van artikel 1, lid 2, van Verordening (EG) 2988/95 (ook indien gepleegd door personen met vertegenwoordigings-, beslissings- of controlebevoegdheid, uiteindelijke begunstigen of personen die essentieel zijn voor de toekenning/uitvoering van de subsidie).
 - Opgericht onder een andere jurisdictie met als doel om fiscale, sociale of andere wettelijke verplichtingen in het land van herkomst te omzeilen, of een andere entiteit met dit doel opgericht (ook indien gepleegd door personen met vertegenwoordigings-, beslissings- of controlebevoegdheid, uiteindelijke begunstigen of personen die essentieel zijn voor de toekenning/uitvoering van de subsidie).

Aanvragers worden ook geweigerd als:

- Zij tijdens de toekenningsprocedure onjuiste informatie hebben verstrekt die vereist is als voorwaarde voor deelname, of die informatie niet hebben verstrekt.
- Zij eerder betrokken waren bij de voorbereiding van de oproep, en dit leidt tot een verstoring van de mededinging die niet op een andere manier kan worden verholpen (belangenconflict).

h. Subsidiabele activiteiten

In aanmerking komende activiteiten zijn de activiteiten die uiteengezet zijn in deel 2 van het oproepdocument dat overeenkomt met oproep DIGITAL-2022-CYBER-03. Meer specifiek moeten de activiteiten gericht zijn op het versterken van kritieke digitale capaciteiten en het bevorderen van kennis en innovatie op het gebied van cybersecurity:

- Thema: Ontwikkeling van infrastructuur of digitale bewustmakingsinstrumenten met behulp van state-of-the-art technologieën die essentiële capaciteiten op het gebied van cybersecurity voor kmo's bieden, d.w.z. ondersteuning van de invoering en verspreiding van geavanceerde cybersecurity oplossingen door kmo's.
- Beschrijving: Ontwikkeling van infrastructuur of innovatieve digitale instrumenten die gericht zijn op het verbeteren van de cybersecurity capaciteiten van kmo's. De ontwikkelde oplossing moet praktisch, kosteneffectief, toegankelijk en gemakkelijk te integreren zijn in de activiteiten van kmo's.

Voorbeelden van projecten zijn:

- Infrastructuuroplossingen zoals soevereine cloud services, gratis back-ups, beveiligde DNS of multi-factor authenticatietools.
- Een AI-gestuurde app voor cybersecurity bewustzijn die gebruik maakt van interactieve lessen en/of gamified leertechnieken met voortgang tracking-functies.
- Projecten moeten in overeenstemming zijn met de beleidsbelangen en prioriteiten van de EU (zoals milieu-, sociaal, veiligheids-, industrieel en handelsbeleid, enz.).

Alle projectactiviteiten moeten plaatsvinden in in aanmerking komende landen³.

i. Ethiek

Projecten moeten voldoen aan:

- De hoogste ethische normen.
- Toepasselijke EU-, internationale en nationale wetgeving (met inbegrip van de Algemene Verordening Gegevensbescherming 2016/679).

Projecten die betrekking hebben op de ontwikkeling, het testen, de implementatie, het gebruik of de distributie van AI-systemen moeten voldoen aan de beginselen van menselijk handelen en toezicht, diversiteit/rechtvaardigheid, transparantie en verantwoorde sociale impact. De robuustheid van de AI-systemen moet voldoende hoog zijn om de betrouwbaarheid te garanderen en onbedoelde schade te voorkomen.

j. Veiligheid

Begunstigden moeten ervoor zorgen dat hun projecten niet onderworpen zijn aan nationale/derde-land veiligheidsvereisten die de uitvoering kunnen beïnvloeden of de toekenning van de subsidie in twijfel kunnen trekken (bijv. technologische beperkingen, nationale veiligheidsclassificatie, enz.). De subsidieverstrekkende instantie moet onmiddellijk op de hoogte worden gebracht van mogelijke veiligheidsproblemen.

k. Toelaatbare onderaanneming

Aanvragers moeten zorgen voor een optimale prijs-kwaliteitverhouding (best value for money) wanneer ze een onderaannemer inschakelen. Alle projectactiviteiten, inclusief werkzaamheden uitgevoerd door onderaannemers, moeten plaatsvinden in landen die voor subsidie in aanmerking komen.

l. Verwachte resultaten

Het thema van deze oproep is "Ontwikkeling van infrastructuur of digitale bewustmakingsinstrumenten met behulp van state-of-the-art technologieën die essentiële capaciteiten bieden op het gebied van cybersecurity voor kmo's". Het verwachte resultaat is de ontwikkeling van infrastructuur of innovatieve digitale instrumenten die gericht zijn op het verbeteren van de cybersecurity capaciteiten van kmo's. De ontwikkelde oplossing moet praktisch, kosteneffectief, toegankelijk en gemakkelijk te integreren zijn in de activiteiten van kmo's.

m. Beperkingen

Per bedrijf of project wordt slechts één subsidie goedgekeurd.

C. Aanvraag- en beoordelingsprocedure

1. Aanvraagformulier

Het aanvraagformulier is beschikbaar via de [NCC-BE pagina](#) van de CCB-website en via het EU Funding & Tenders Portal.

2. Indiening per email

³ EU-lidstaten (met inbegrip van landen en gebieden overzee (LGO)); en EER-landen (Noorwegen, IJsland, Liechtenstein).

Ingevulde aanvraagformulieren en bewijsstukken moeten als bijlage per email worden verzonden naar ncc@ccb.belgium.be.

3. Toekenningscriteria

Projectaanvragen moeten een duidelijke beschrijving bevatten van de uit te voeren activiteiten en de te behalen resultaten. De toekenningscriteria voor projectaanvragen voor cascade financiering zijn de volgende:

a. Impact

- Voldoende garanties/elementen die aantonen dat het project een gunstige impact heeft of kan hebben op de cybersecurity van Belgische kmo's en op de naleving van de cybersecurity wetgeving.
- De mate waarin het project naar verwachting de beoogde resultaten en deliverables zal behalen, zoals vermeld in het oproepdocument "Funding for Cyber", alsmede de plannen voor verspreiding en communicatie van de projectresultaten.
- De mate waarin het project het concurrentievermogen van Belgische begunstigden in de Europese Unie zou versterken en de samenleving ten goede zou komen.

b. Beschikbaarheid

- Marktgereedheid: de mate waarin de door het project ontwikkelde oplossing klaar is voor implementatie op de markt.
- Betaalbaarheid van de oplossing voor een breed scala aan gebruikers, waaronder kmo's en non-profitorganisaties.
- Toegankelijkheid van de ontwikkelde oplossing.
- De mate waarin de ontwikkelde oplossing met beperkte inspanningen en beperkte middelen kan worden geïntegreerd in de bedrijfsvoering van kmo's of non-profitorganisaties.
- Schaalbaarheid van de oplossing.

c. Relevantie

- Afstemming met het oproepdocument "Funding for Cyber" en de nagestreefde doelstellingen.
- Bijdrage aan langetermijnbeleidsdoelstellingen, relevante beleidslijnen en strategieën, en synergie met activiteiten op Europees niveau.
- Bijdrage aan de Belgische Cybersecurity Strategy, met de nadruk op het beveiligen van het cyberlandschap op alle niveaus en voor alle belanghebbenden, en de strategische doelstellingen daarvan.
- Mate waarin het project de digitale technologie-toeleveringsketen in de EU zou versterken en beveiligen.

d. Uitvoering

- Maturiteit van het project.
- De degelijkheid van het uitvoeringsplan en het efficiënte gebruik van middelen.
- Capaciteit van de aanvragers om het voorgestelde werk uit te voeren, met name wat betreft hun relevante ervaring en financiële draagkracht.

4. Beoordelingsproces

De toekenningscriteria voor cascade financiering worden beoordeeld en voor elk toekenningscriterium wordt een individuele score in punten toegekend, volgens onderstaande schaal:

Score	Omschrijving
0	Onmogelijk te beoordelen of afwezig.
1	Zeer slecht, het projectvoorstel voldoet niet aan het toekenningscriterium.
2	Slecht, het toekenningscriterium is slechts in beperkte mate vervuld.
3	Goed, het voorstel voldoet duidelijk aan het toekenningscriterium.
4	Zeer goed, het voorstel overtreft het toekenningscriterium.
5	Uitmuntend, het voorstel is van uitzonderlijke kwaliteit.

Het maximum aantal punten dat kan worden behaald is 5 punten per toekenningscriterium en 20 punten in totaal voor alle toekenningscriteria samen. De individuele drempel per criterium is 3 van de 5 punten. De totale drempel bedraagt derhalve 12 punten. Voorstellen die de individuele drempels en de totale drempel halen, komen in aanmerking voor financiering, binnen de grenzen van het beschikbare budget (d.w.z. tot het budgetplafond). Andere voorstellen worden afgewezen. Bij gelijke totale scores van meerdere projecten, wordt voorrang gegeven aan projecten met de hoogste score voor het toekenningscriterium 'Impact'. Bij een gelijke score op het toekenningscriterium 'Impact', wordt voorrang gegeven aan projecten met de hoogste score voor het toekenningscriterium 'Beschikbaarheid', en vervolgens voor de criteria 'Relevantie' en 'Uitvoering'.

5. Kennisgeving van de resultaten en voorstel voor sub-subsidieovereenkomst

Succesvolle aanvragers worden binnen 1 maand na de uiterste aanvraagdatum per email op de hoogte gebracht van de resultaten en ontvangen vervolgens een voorstel voor een sub-subsidieovereenkomst. Dit voorstel bevat de voorwaarden en bepalingen van de subsidiefinanciering, waaronder monitoring-, rapportage- en auditbepalingen. Het voorstel voor de sub-subsidieovereenkomst moet worden beoordeeld en ingevuld zoals gevraagd door het NCC-BE, en ondertekend en per email worden teruggestuurd. Het NCC-BE zal de subsidieontvangers een medeondertekend exemplaar van de subsidieovereenkomst bezorgen.

Afgewezen aanvragers worden op de hoogte gebracht van hun resultaat. Daarnaast worden de resultaten van de oproep gepubliceerd op de [NCC-BE pagina](#) van de CCB-website, met een beschrijving van de geselecteerde projecten, de toekenningsdata, de projectduur en de officiële namen en landen van de uiteindelijke ontvangers.

D. Monitoring, rapportage en terugbetaling

1. Monitoring van projecten

Het NCC-BE zal de uitvoering van alle projecten monitoren via de subsidieprojectmanager van het bedrijf en kan gedurende de hele projectcyclus updates vragen over de voortgang om te bevestigen dat de projecten volgens plan verlopen. Het is de verantwoordelijkheid van de subsidieontvanger om eventuele wijzigingen in het project – met betrekking tot activiteiten, tijdschema's of kosten – aan het NCC-BE te melden.

2. Rapportage en terugbetalingsaanvraag

Het bedrijf moet aan het NCC-BE verslag(en) bezorgen waarin de uitgevoerde activiteiten en

de daarmee verband houdende kosten worden bevestigd, zoals bepaald in de sub-subsidieovereenkomst. Dit omvat het indienen van een terugbetalingsaanvraag, samen met de vereiste bewijsstukken, bij het NCC-BE. Voor het verslag en de terugbetalingsaanvraag moet het bedrijf de template gebruiken die door het NCC-BE wordt verstrekt. Alle documenten, inclusief verslagen, terugbetalingsaanvraag en bewijsstukken, moeten uiterlijk op 31 december 2025 worden ingediend. Het NCC-BE zal de verslagen en de terugbetalingsaanvraag beoordelen en de betalingen verwerken in de volgorde van de ingediende claims. Alleen kosten die zijn gemaakt vanaf de publicatie van deze oproep tot 11 december 2025, en die noodzakelijk zijn voor de uitvoering van de actie zoals beschreven in de sub-subsidieovereenkomst, komen in aanmerking. In aanmerking komende kosten kunnen personeels-, onderaannemings- en aankoopkosten omvatten, overeenkomstig de bepalingen van de sub-subsidieovereenkomst. Aanvaarde en in aanmerking komende kosten worden vergoed na indiening van het ingevulde verslag, de terugbetalingsaanvraag en de bewijsstukken, op voorwaarde dat de ingediende documenten door het NCC-BE zijn goedgekeurd.

3. Publicatie van resultaten

Subsidieontvangers kunnen worden verzocht het NCC-BE te ondersteunen bij de communicatie en bekendmaking van de resultaten en de impact van de subsidie. Alle communicatie moet ook vermelden dat de steun afkomstig is van de Europese Unie en het betreffende fonds, overeenkomstig Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021. Verdere richtlijnen voor publicaties zullen beschikbaar zijn in het voorstel voor de sub-subsidieovereenkomst.

E. Gegevensbescherming

Gegevens die in het kader van de aanvraagprocedure worden verzameld en opgeslagen, worden beschermd in overeenstemming met de AVG en de nationale wetgeving inzake de bescherming van persoonsgegevens. Voor meer informatie verwijzen wij u naar het [privacybeleid](#) van het CCB.

F. Contactgegevens

Voor hulp bij vragen kunt u contact opnemen via ncc@ccb.belgium.be.