



APPEL À PROJETS NCC-BE CYBERSÉCURITÉ 2025 « FUNDING FOR CYBER » – OUVERT DU 8 OCTOBRE 2025 AU 8 DÉCEMBRE 2025

Table des matières

APPEL À PROJETS NCC-BE CYBERSÉCURITÉ 2025 « FUNDING FOR CYBER »	1
Objet du document	1
A. Introduction	1
B. Description de l'appel « Funding for Cyber » et critères d'éligibilité	2
C. Processus de candidature et d'évaluation	9
D. Suivi, rapports et remboursement	11
E. Protection des données	12
F. Coordonnées	12

Objet du document

Ce document a pour objectif de décrire les termes de référence de l'appel à projets du financement en cascade 2025 du NCC-BE « Funding for Cyber ». Il présente le contexte de l'appel à projets, les critères d'éligibilité, la procédure de candidature, d'évaluation et d'attribution.

Il fournit aux candidats potentiels à une subvention toutes les informations pertinentes sur le programme de financement. Il décrit également les conditions générales à prendre en compte avant de postuler.

Ce document vise à définir, dans un langage clair, les lignes directrices à l'intention des participants au programme de subventions, afin de garantir l'équité, la transparence et l'égalité des chances.

A. Introduction

1. Le Centre National de Coordination pour la Cybersécurité en Belgique (NCC-BE)

Le Centre National de Coordination pour la cybersécurité (NCC-BE) a été créé par le gouvernement belge en vertu de l'article 6 du règlement (UE) 2021/887 au sein du Centre pour la Cybersécurité Belgique (CCB) par l'arrêté royal du 16 février 2022 (modifiant l'arrêté royal



du 10 octobre 2014 portant création du CCB).

Le gouvernement belge ambitionne que le NCC-BE devienne le partenaire privilégié de l'ensemble des parties prenantes, qu'elles soient issues des secteurs public ou privé, que ce soit au niveau local, régional ou national, dans le domaine de la cybersécurité. En outre, le NCC-BE joue un rôle proactif et dynamique dans le cadre du Centre de compétences européen en matière de cybersécurité (en anglais ECCC) et au sein du réseau des NCC. Cela renforcera l'écosystème belge de cybersécurité, contribuera à la collaboration transfrontalière avec d'autres NCC le cas échéant et favorisera une nouvelle croissance dans le domaine de la numérisation et de la sécurité. En outre, la compétitivité numérique de la Belgique et, par extension, celle de l'Union européenne en seront augmentées.

2. Digital Europe Programme

L'appel à projets « Funding for Cyber » est partiellement financé par « Digital Europe Programme » (DEP) et cofinancé par le Centre pour la Cybersécurité Belgique. Le DEP a accordé un financement au Centre pour la Cybersécurité Belgique dans le cadre de l'appel à projets DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION. Le NCC-BE œuvre à la création d'un paysage numérique sécurisé, au renforcement de la résilience nationale et à l'amélioration de la capacité à répondre aux cyberincidents. Chaque activité, étape et résultat escompté d'un projet proposé par un candidat doit être conforme aux objectifs définis dans le présent document d'appel.

Alignement stratégique

Ce programme de financement soutient les tâches et responsabilités assignées aux NCC en vertu du règlement (UE) 2021/887, en mettant l'accent sur le renforcement des capacités numériques essentielles et la promotion des connaissances et de l'innovation en matière de cybersécurité. En outre, le programme de financement s'aligne sur la stratégie belge en matière de cybersécurité et continuera d'évoluer en réponse aux nouvelles menaces et aux nouveaux défis cybernétiques.

B. Description de l'appel « Funding for Cyber » et critères d'éligibilité

1. Description de l'appel « Funding for Cyber »

L'objectif de ce soutien financier est d'aider les bénéficiaires belges, tels que les start-ups, les scale-ups, les PME¹ et/ou les mid-caps, à adopter ou à développer l'innovation numérique. La sous-convention de subvention entre le bénéficiaire du soutien financier et le CCB (NCC-BE) doit soutenir « l'adoption et la diffusion de solutions de cybersécurité de pointe par les PME ».

a. Thème du programme de financement

Le thème de cet appel sera « Développer des infrastructures ou des outils numériques de sensibilisation utilisant des technologies de pointe offrant des capacités essentielles en matière de cybersécurité pour les PME ». Ce thème peut englober, sans s'y limiter, les éléments suivants :

¹ Les petites et moyennes entreprises (PME) sont définies par la recommandation 2003/361/CE de la Commission et sont classées en fonction du nombre d'employés, du chiffre d'affaires annuel et du total du bilan. Une PME doit compter moins de 250 salariés et avoir soit un chiffre d'affaires annuel ne dépassant pas 50 millions d'euros, soit un bilan total ne dépassant pas 43 millions d'euros. Les catégories suivantes sont également distinguées: les petites entreprises (moins de 50 salariés, chiffre d'affaires ou bilan ≤ 10 millions d'euros) et les microentreprises (moins de 10 salariés, chiffre d'affaires ou bilan ≤ 2 millions d'euros).

- la création d'infrastructures offrant des services de cloud computing, des sauvegardes de données gratuites et/ou un système de noms de domaine fiable ;
- la création de solutions d'authentification multifactorielle ;
- la création de solutions informatiques pour la sensibilisation à la cybersécurité basées sur l'intelligence artificielle, utilisant des leçons interactives et/ou des techniques d'apprentissage ludiques et permettant aux utilisateurs de suivre leurs progrès.

b. Bénéficiaires ciblés

Les principaux bénéficiaires ciblés par ce programme de soutien financier sont les organisations (entreprises privées, PME, start-ups – liste non exhaustive) qui possèdent une expertise démontrable dans l'un des domaines suivants :

- (a) la création et la diffusion de contenus de sensibilisation à la cybersécurité, ou
- (b) le développement et le déploiement d'infrastructures liées à la cybersécurité adaptées aux petites et moyennes entreprises (PME).

Ces organisations bénéficiaires recevront un soutien pour concevoir, mettre en œuvre ou adapter des solutions visant à améliorer la posture des PME en matière de cybersécurité.

c. Utilisateurs finaux

Si les bénéficiaires directs du soutien financier sont les organisations expertes mentionnées ci-dessus, les bénéficiaires/utilisateurs finaux des solutions soutenues sont les PME belges. Ces PME devraient bénéficier :

- (a) d'un accès accru à des outils numériques de sensibilisation conviviaux, qui contribuent à former le personnel aux pratiques de cybersécurité ou
- (b) de l'adoption d'une infrastructure de cybersécurité essentielle qui renforce leur résilience numérique.

d. Budget et modalités de paiement

La subvention allouée par bénéficiaire s'élèvera à 60 000 EUR, avec un maximum de six subventions (une par demandeur), pour un montant total de 360 000 EUR. Le coût minimum du projet est de 60 000 EUR. Le budget est calculé sur la base des coûts directs éligibles estimés (coûts de personnel, coûts de sous-traitance, frais d'achat, autres catégories de frais).

Le paiement de la subvention prendra la forme suivante :

- une avance de 45 000 EUR après la décision d'attribution de la subvention et dans les 30 jours civils suivant la remise d'une copie signée de la décision d'attribution de la subvention,
- un paiement final ou un recouvrement correspondant aux coûts éligibles acceptés (effectué à compter de la date de publication du présent appel jusqu'au 11 décembre 2025) après la soumission du rapport complet, de la demande de remboursement et des pièces justificatives, à condition que les documents soumis soient approuvés par le CCB.

Le montant maximal de la subvention, fixé à 60 000 EUR, ne peut être dépassé. Dans le cas de projets dont le coût total est supérieur au montant maximal de la subvention, les bénéficiaires doivent financer eux-mêmes le montant dépassant ce montant maximal.

e. Dates d'ouverture et de clôture de la subvention

L'appel à projets « Funding for Cyber » est ouvert du 8 octobre 2025 et reste ouvert pendant une période de 60 jours calendaires, conformément aux exigences de la Commission européenne. La date limite de dépôt des candidatures est fixée au 8 décembre 2025. Tous les documents requis doivent être soumis avant cette date pour être évalués. Aucune candidature tardive ne sera prise en considération.

f. Mise en œuvre

Les actions relevant des projets financés dans le cadre de l'appel à projets de financement en cascade doivent au moins être menées pendant la période d'éligibilité des coûts. À la fin de cette période, les bénéficiaires doivent s'assurer que les actions décrites dans la description de l'action ont été exécutées conformément à la sous-convention de subvention. Les coûts correspondants doivent être réclamés avant le 31 décembre 2025. À cette date, les bénéficiaires doivent s'assurer que tous les rapports, demandes de remboursement et pièces justificatives ont été soumis.

g. Cadre réglementaire

Règlement (UE, Euratom) 2024/2509 du Parlement européen et du Conseil du 23 septembre 2024 relatif aux règles financières applicables au budget général de l'Union.

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

Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique. Ce règlement fixe l'enveloppe financière du « Digital Europe Programme » pour la période 2021-2027.

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

Le soutien financier sera accordé conformément au règlement (UE) 2023/2831 de la Commission du 13 décembre 2023 relatif à l'application des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne aux aides de minimis.

Arrêté royal du 1^{er} octobre 2025 fixant les conditions d'octroi de subsides pour la réalisation de projets de développement d'infrastructures ou de développement d'outils numériques qui permettent d'améliorer les capacités en matière de cybersécurité des PME.

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

2. Critères d'éligibilité

Les critères d'éligibilité pour le financement en cascade sont établis conformément aux critères d'éligibilité correspondant à l'appel DIGITAL-2022-CYBER-03.

a. Admissibilité et pièces justificatives

- Les propositions doivent être soumises avant la date limite de dépôt des candidatures. Toutes les candidatures et les pièces justificatives doivent être reçues avant le 8 décembre 2025.
- Les propositions doivent être soumises par voie électronique à l'adresse e-mail ncc@ccb.belgium.be en utilisant le modèle fourni, accessible via [la page NCC-BE](#) du site web du CCB et dans le cadre de l'appel à propositions de financement en cascade sur le EU Funding & Tenders Portal.
- Les propositions (y compris les annexes et les pièces justificatives) doivent être soumises conformément aux instructions fournies sur la page NCC-BE du site web du CCB et sur le EU Funding & Tenders Portal.
- Les propositions doivent être complètes et contenir toutes les informations demandées, toutes les annexes et tous les documents justificatifs requis, comme indiqué sur la page NCC-BE du site web du CCB et sur le EU Funding & Tenders Portal.

² Texte initial accessible via le lien suivant: <http://data.europa.eu/eli/reg/2021/694/oj>.

- La proposition doit inclure :
 - 1) une copie des statuts de l'entité;
 - 2) une déclaration de propriété et de contrôle dûment remplie et signée, permettant au NCC-BE de procéder à une évaluation de la propriété et du contrôle (« Ownership & Control Assessment », OCA) conformément à l'article 12, paragraphe 5, du règlement (UE) 2021/694 susmentionné ;
 - 3) une description du projet, en particulier son objectif, le groupe cible et la durée estimée de développement, conformément au modèle fourni sur la page NCC-BE du site web du CCB ;
 - 4) une estimation des coûts du projet, précisant les coûts éligibles (voir point c sur la capacité financière) ;
 - 5) une déclaration confirmant qu'aucun double financement n'est applicable aux activités du projet;
 - 6) toute information factuelle ou juridique permettant d'évaluer le niveau d'expertise de l'entité en matière de sensibilisation à la cybersécurité ou de la création d'infrastructures pour les PME ;
 - 7) toutes les données factuelles ou juridiques permettant d'évaluer la capacité financière de l'entité à soutenir le développement du projet visé au point 3), comme spécifié dans la section c. Capacité financière du présent document.
- La personne qui soumet la proposition doit être habilitée à agir au nom de l'entité (des entités) qui la soumette(nt).
- Les propositions doivent être lisibles, accessibles et imprimables.

b. Participants éligibles

Les bénéficiaires visés par l'appel « Funding for Cyber » sont des organisations disposant d'une expertise en matière de contenu de sensibilisation à la cybersécurité ou de mise en place d'infrastructures pour les PME. Les utilisateurs finaux qui devraient bénéficier de l'utilisation de l'outil numérique de sensibilisation ou de l'infrastructure sont les PME belges.

Pour être éligibles, les candidats et les participants doivent :

- être des entités juridiques.
- être établis dans l'un des pays éligibles, à savoir :
 - o les États membres de l'UE (y compris les pays et territoires d'outre-mer (PTOM)).
 - o les pays de l'EEE (Norvège, Islande, Liechtenstein).
- conformément à l'article 12, paragraphe 5, du règlement (UE) 2021/694 susmentionné, ne pas être contrôlés directement ou indirectement par un pays qui n'est pas un pays éligible.
- ne pas être soumis à des restrictions prévues par les dispositions en matière d'autonomie stratégique de l'UE.

Cas particuliers

- Les organisations internationales ne sont pas éligibles, sauf s'il s'agit d'organisations internationales d'intérêt européen au sens de l'article 2 du « Digital Europe Regulation ».
- Les entités qui ne sont pas dotées de la personnalité juridique en vertu de leur droit national peuvent participer à titre exceptionnel, à condition que leurs représentants aient la capacité de contracter des obligations juridiques en leur nom et offrent des garanties pour la protection des intérêts financiers de l'UE équivalentes à celles offertes par les personnes morales.

- Les organismes de l'UE (à l'exception du European Commission Joint Research Centre) ne peuvent pas participer.
- Des règles spéciales s'appliquent aux entités soumises à des mesures restrictives de l'UE en vertu de l'article 29 du traité sur l'Union européenne (TUE) et de l'article 215 du traité sur le fonctionnement de l'Union européenne (TFUE) ainsi qu'aux entités couvertes par les lignes directrices de la Commission n° 2013/C 205/0514). Ces entités ne sont éligibles à participer à aucun titre.

c. Capacité financière

Conformément à l'article 198 du règlement (UE, Euratom) 2018/1046 et aux articles 7 et 9 de l'arrêté royal du 1^{er} octobre 2025 fixant les conditions d'octroi de subsides pour la réalisation de projets de développement d'infrastructures ou de développement d'outils numériques qui permettent d'améliorer les capacités en matière de cybersécurité des PME qui établit le programme de subventions « Funding for Cyber », les candidats doivent démontrer qu'ils disposent d'une capacité financière stable et suffisante pour soutenir le développement du projet proposé. Il s'agit d'une condition d'éligibilité obligatoire et les candidatures qui ne remplissent pas cette condition seront rejetées.

La capacité financière est nécessaire pour garantir que le candidat peut soutenir la phase de développement du projet telle que décrite dans la demande, conformément à l'article 7, § 1^{er}, 6°, de l'arrêté royal. La capacité financière sera également évaluée dans le cadre du critère de mise en œuvre défini à l'article 10, § 1^{er}, 2°, de ce même arrêté royal.

d. Pièces justificatives

Aux fins de l'évaluation de sa capacité financière, chaque candidat doit joindre à son dossier de candidature (article 7, § 1^{er}) les documents suivants :

- Aperçu du budget du projet (à l'aide du modèle fourni).
- Toute information factuelle ou juridique permettant d'évaluer la capacité financière du candidat à soutenir le projet.

Liste non exhaustive des documents et informations pouvant être fournis :

- Compte de résultat approuvé.
- Bilan approuvé.
- Notes explicatives et/ou annexes faisant partie des états financiers ci-dessus.
- Rapport d'audit externe ou déclaration sur l'honneur.
- Dans le cas de filiales ne disposant pas de leurs propres états financiers : comptes consolidés et rapport d'audit/déclaration sur l'honneur de la société mère/du groupe dont elles font partie. Des documents supplémentaires peuvent être demandés pour prouver les conditions avec la société mère.
- Dans le cas de sociétés mères : un résumé simplifié du compte de résultat et du bilan non consolidés, respectant les exigences minimales en matière de reporting, daté et signé par la direction.
- Dans le cas de start-ups : données prévisionnelles pour un an (plan d'affaires).
- Dans le cas d'entités récemment créées, qui n'ont pas encore clôturé leurs comptes : documents relatifs au seul exercice clos ou données financières estimées (c'est-à-dire un plan d'affaires ou un document similaire comprenant des projections financières sur les actifs courants et non courants, les capitaux propres, les passifs courants et non courants, le chiffre d'affaires, les produits et charges d'exploitation et financiers).
- Dans le cas de personnes physiques : déclaration annuelle d'impôt sur le revenu contenant des détails sur les revenus et les dépenses liés aux activités

- commerciales.
- Dans le cas d'entités pratiquant la comptabilité de caisse : déclarations signées par le représentant légal autorisé de l'entité fournissant des informations sur les actifs immobilisés et courants ainsi que sur les revenus et les dépenses. En outre, il est recommandé de fournir toute preuve disponible à l'appui des montants déclarés (par exemple, des relevés bancaires confirmant le solde disponible à la date de clôture comptable, etc.)
- Dans le cas d'entités couvertes par un garant, les données financières du garant.

Si les informations financières fournies ne sont pas suffisamment claires, le NCC-BE peut contacter les participants pour obtenir des précisions supplémentaires.

e. Base d'évaluation

Conformément à l'article 10, § 1^{er}, 2°, de l'arrêté royal, l'évaluation de la capacité financière fait partie de l'évaluation de la faisabilité de la mise en œuvre. Les principes suivants s'appliquent:

- le candidat doit démontrer qu'il est en mesure de soutenir le développement du projet sur la base de sa situation financière ;
- l'évaluation peut inclure des indicateurs tels que les fonds propres disponibles, l'absence d'insolvabilité et la proportion raisonnable du coût du projet par rapport à la taille de l'entité ;
- les candidats nouvellement créés ou de petite taille ne doivent pas être automatiquement exclus s'ils peuvent démontrer de manière crédible qu'ils sont en mesure de mener à bien le projet.

f. Capacité opérationnelle

Les candidats doivent disposer du savoir-faire, des qualifications et des ressources nécessaires pour mener à bien les projets et apporter leur contribution (y compris une expérience suffisante dans des projets consacrés à la sensibilisation à la cybersécurité ou à la création d'infrastructures pour les PME). Cette capacité sera évaluée conjointement avec le critère d'attribution 'Mise en œuvre', sur la base des compétences et de l'expérience des candidats et de leurs équipes de projet, y compris les ressources opérationnelles (humaines, techniques et autres).

g. Exclusion

Ne peuvent participer les candidats qui font l'objet d'une décision d'exclusion de l'UE ou qui se trouvent dans l'une des situations d'exclusion suivantes les empêchant de bénéficier d'un financement de l'UE :

- faillite, liquidation, administration judiciaire, concordat avec les créanciers, suspension des activités commerciales ou autres procédures similaires (y compris les procédures concernant les personnes ayant une responsabilité illimitée pour les dettes du candidat).
- manquement aux obligations en matière de sécurité sociale ou fiscale (y compris par des personnes ayant une responsabilité illimitée pour les dettes du candidat).
- faute professionnelle grave (y compris si elle est commise par des personnes ayant des pouvoirs de représentation, de décision ou de contrôle, des bénéficiaires effectifs ou des personnes essentielles à l'octroi/à la mise en œuvre de la subvention).
- a commis une fraude, un acte de corruption, a des liens avec une organisation

criminelle, s'est livré à des activités de blanchiment d'argent, à des crimes liés au terrorisme (y compris le financement du terrorisme), au travail des enfants ou à la traite des êtres humains (y compris si cela a été commis par des personnes ayant des pouvoirs de représentation, de décision ou de contrôle, des bénéficiaires effectifs ou des personnes qui sont essentielles pour l'octroi/la mise en œuvre de la subvention).

- a présenté des lacunes importantes dans le respect des principales obligations découlant d'un contrat de marché public, d'une convention de subvention, d'un prix, d'un contrat d'expertise ou d'un contrat similaire de l'UE (y compris si cela a été commis par des personnes ayant des pouvoirs de représentation, de décision ou de contrôle, des bénéficiaires effectifs ou des personnes qui sont essentielles pour l'octroi/la mise en œuvre de la subvention).
- coupable d'irrégularités au sens de l'article 1^{er}, paragraphe 2, du règlement (CE) n° 2988/95 (y compris si cela a été commis par des personnes ayant des pouvoirs de représentation, de décision ou de contrôle, des bénéficiaires effectifs ou des personnes qui sont essentielles pour l'octroi/la mise en œuvre de la subvention).
- a créé sous une autre juridiction dans le but de contourner les obligations fiscales, sociales ou autres obligations légales dans le pays d'origine ou ayant créé une autre entité à cette fin (y compris si cela est fait par des personnes ayant des pouvoirs de représentation, de décision ou de contrôle, des bénéficiaires effectifs ou des personnes qui sont essentielles pour l'octroi/la mise en œuvre de la subvention).

Les candidats seront également refusés :

- si au cours de la procédure d'attribution, ils ont fourni des informations requises comme condition de participation inexactes ou n'ont pas fourni ces informations.
- s'ils ont déjà participé à la préparation de l'appel à propositions, ce qui entraîne une distorsion de concurrence qui ne peut être corrigée autrement (conflit d'intérêts).

h. Activités éligibles

Les activités éligibles sont celles énoncées à la section 2 du document d'appel correspondant à l'appel DIGITAL-2022-CYBER-03. Plus précisément, les activités doivent se concentrer sur le renforcement des capacités numériques essentielles et la promotion des connaissances et de l'innovation en matière de cybersécurité:

- Thème: développer des infrastructures ou des outils de sensibilisation au numérique à l'aide de technologies de pointe offrant des capacités essentielles en matière de cybersécurité pour les PME, c'est-à-dire soutenir l'adoption et la diffusion de solutions de cybersécurité de pointe par les PME.
- Description: développement d'infrastructures ou d'outils numériques innovants visant à renforcer les capacités des PME en matière de cybersécurité. La solution développée doit être pratique, rentable, accessible et facile à intégrer dans les activités des PME.

Exemples de projets possibles:

- des solutions d'infrastructure telles que des services cloud souverains, des sauvegardes gratuites, des DNS sécurisés ou des outils d'authentification multifactorielle.
- une application de sensibilisation à la cybersécurité basée sur l'IA qui utilise des leçons interactives et/ou des techniques d'apprentissage ludiques avec des fonctionnalités de suivi des progrès.

Les projets doivent être conformes aux intérêts et aux priorités politiques de l'UE (tels que l'environnement, la politique sociale, la sécurité, la politique industrielle et commerciale, etc.) Toutes les activités du projet doivent se dérouler dans les pays éligibles³.

i. Éthique

Les projets doivent respecter:

- les normes éthiques les plus élevées.
- la législation européenne, internationale et nationale applicable (y compris le Règlement Général sur la Protection des Données (UE) 2016/679).

Les projets impliquant le développement, le test, le déploiement, l'utilisation ou la distribution de systèmes d'IA doivent respecter les principes d'action et de contrôle humains, de diversité/équité, de transparence et d'impact social responsable. La robustesse des systèmes d'IA doit être suffisamment élevée pour garantir leur fiabilité et éviter tout préjudice involontaire.

j. Sécurité

Les bénéficiaires doivent s'assurer que leurs projets ne sont pas soumis à des exigences de sécurité nationales/de pays tiers qui pourraient affecter leur mise en œuvre ou remettre en cause l'octroi de la subvention (par exemple, restrictions technologiques, classification de sécurité nationale, etc.). L'autorité octroyant la subvention doit être immédiatement informée de tout problème potentiel en matière de sécurité.

k. Sous-traitance éligible

Les candidats doivent veiller à obtenir le meilleur rapport qualité-prix lorsqu'ils font appel aux services d'un sous-traitant. Toutes les activités du projet, y compris les travaux réalisés par des sous-traitants, doivent avoir lieu dans des pays éligibles.

l. Résultats escomptés

Le thème de cet appel sera « Développer des infrastructures ou des outils de sensibilisation au numérique utilisant des technologies de pointe offrant des capacités essentielles en matière de cybersécurité pour les PME ». Le résultat attendu est le développement d'infrastructures ou d'outils numériques innovants visant à renforcer les capacités des PME en matière de cybersécurité. La solution développée doit être pratique, rentable, accessible et facile à intégrer dans les activités des PME.

m. Restrictions

Une seule subvention sera approuvée par entreprise ou par projet.

C. Processus de candidature et d'évaluation

1. Formulaire de candidature

Le formulaire de candidature est disponible sur [la page NCC-BE](#) du site web du CCB ainsi que sur le Funding & Tenders Portal.

2. Soumission par e-mail

Les formulaires de candidature dûment remplis et les pièces justificatives doivent être envoyés

³ Les États membres de l'UE (y compris les pays et territoires d'outre-mer (PTOM)) et pays de l'EEE (Norvège, Islande, Liechtenstein).

en pièces jointes par e-mail à l'adresse ncc@ccb.belgium.be.

3. Critères d'attribution

Les demandes de projet doivent décrire clairement les activités à réaliser ainsi que les résultats à obtenir. Les critères d'attribution pour les demandes de projet de financement en cascade sont les suivants :

a. Impact

- Garanties / éléments suffisants démontrant que le projet a ou peut avoir un impact bénéfique sur la cybersécurité des PME belges et le respect de la législation en matière de cybersécurité.
- Mesure dans laquelle le projet est susceptible d'atteindre les résultats et les livrables attendus mentionnés dans l'appel à propositions « Funding for Cyber » et les plans de diffusion et de communication des résultats du projet.
- Mesure dans laquelle le projet renforcerait la compétitivité des bénéficiaires belges dans l'Union européenne et serait bénéfique pour la société.

b. Disponibilité

- Maturité commerciale : mesure dans laquelle la solution développée par le projet est prête à être déployée sur le marché.
- Accessibilité financière de la solution pour un large éventail d'utilisateurs, y compris les PME et les associations sans but lucratif.
- Accessibilité de la solution développée.
- Mesure dans laquelle la solution développée peut être intégrée dans les activités des PME ou des associations sans but lucratif avec un effort et des ressources limités.
- Évolutivité de la solution.

c. Pertinence

- Conformité avec le document d'appel « Funding for Cyber » et les objectifs poursuivis.
- Contribution aux objectifs politiques à long terme, aux politiques et stratégies pertinentes, et synergies avec les activités au niveau européen.
- Contribution à la stratégie belge en matière de cybersécurité, axée sur la sécurisation du paysage cyber à tous les niveaux et pour toutes les parties prenantes, et à ses objectifs stratégiques.
- Mesure dans laquelle le projet renforcerait et sécuriserait la chaîne d'approvisionnement des technologies numériques dans l'UE.

d. Mise en œuvre

- Maturité du projet.
- Solidité du plan de mise en œuvre et utilisation efficace des ressources.
- Capacité des candidats à mener à bien les travaux proposés, notamment en ce qui concerne leur expérience pertinente et leur capacité financière.

4. Processus d'évaluation

Les critères d'attribution du financement en cascade seront évalués et, pour chaque critère, une note individuelle sera attribuée comme suit :

Note	Description
0	Impossible à évaluer ou absent.
1	Très médiocre, la proposition de projet ne répond pas au critère d'attribution.
2	Médiocre, le critère d'attribution n'est rempli que dans une mesure limitée.
3	Bon, la proposition répond clairement au critère d'attribution.
4	Très bien, la proposition dépasse les critères d'attribution.
5	Excellent, la proposition est d'une qualité exceptionnelle.

Le nombre maximum de points pouvant être obtenus est de 5 points par critère d'attribution, et de 20 points au total pour l'ensemble des critères d'attribution. Les seuils individuels par critère sont de 3 points sur 5. Le seuil global est donc de 12 points. Les propositions qui dépassent les seuils individuels et le seuil global seront prises en considération pour un financement, dans les limites du budget disponible (c'est-à-dire jusqu'au plafond budgétaire). Les autres propositions seront rejetées. Si plusieurs projets obtiennent un score global identique, la priorité sera donnée aux projets ayant obtenu le score le plus élevé pour le critère d'attribution 'Impact'. En cas d'égalité pour le critère d'attribution 'Impact', la priorité sera donnée aux projets ayant obtenu le score le plus élevé pour le critère d'attribution 'Disponibilité', puis pour les critères d'attribution 'Pertinence' et 'Mise en œuvre'.

5. Notification des résultats et proposition de convention de subvention

Les candidats retenus seront informés des résultats par e-mail dans un délai d'un mois après la date limite de dépôt des candidatures et recevront ensuite une proposition de sous-accord de subvention. La proposition de sous-accord de subvention contiendra les conditions générales du financement de la subvention, y compris les dispositions relatives au suivi, à la rédaction de rapports et à l'audit. La proposition de sous-accord de subvention doit être examinée et complétée conformément aux demandes du NCC-BE, puis signée et renvoyée par e-mail. Le NCC-BE fournira aux bénéficiaires de la subvention une copie contresignée de la convention de subvention secondaire.

Les candidats non retenus seront informés du résultat. En outre, les résultats de l'appel seront publiés sur [la page NCC-BE](#) du site web du CCB, avec une description des projets sélectionnés, les dates d'attribution, la durée des projets, ainsi que les noms légaux et les pays des bénéficiaires finaux.

D. Suivi, rapports et remboursement

1. Suivi des projets

Le NCC-BE supervisera la mise en œuvre de tous les projets par l'intermédiaire du responsable des projets de subvention de l'entreprise et pourra demander des mises à jour sur l'avancement tout au long du cycle de vie du projet, afin de confirmer que les projets progressent comme prévu. Il incombe au bénéficiaire de la subvention de signaler au NCC-BE tout changement concernant le projet, en termes d'actions, de délais ou de coûts.

2. Rapports et demandes de remboursement

L'entreprise doit fournir au NCC-BE un ou plusieurs rapports confirmant les activités réalisées

et les coûts associés, comme stipulé dans la convention de subvention. Cela inclut la soumission d'une demande de remboursement accompagnée des pièces justificatives au NCC-BE. Pour le rapport et la demande de remboursement, l'entreprise doit utiliser le modèle fourni par le NCC-BE. Tous les documents, y compris les rapports, les demandes de remboursement et les pièces justificatives, doivent être soumis avant le 31 décembre 2025. Le NCC-BE examinera le rapport et la demande de remboursement et traitera les paiements dans l'ordre des demandes soumises. Seuls les coûts engagés entre la publication du présent appel et le 11 décembre 2025 et nécessaires à la mise en œuvre de l'action décrite dans la sous-convention de subvention sont éligibles. Les coûts éligibles peuvent inclure les frais de personnel, les frais de sous-traitance et les frais d'achat, conformément à la sous-convention de subvention. Les coûts acceptés et éligibles seront remboursés après soumission du rapport complet, de la demande de remboursement et des pièces justificatives, à condition que les documents soumis soient approuvés par le NCC-BE.

3. Publication des résultats

Les bénéficiaires de la subvention peuvent être tenus d'aider le NCC-BE à communiquer et à publier les résultats et les impacts de la subvention. Toute communication doit mentionner le soutien de l'Union européenne et du fonds concerné, conformément au règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021. Des orientations supplémentaires concernant les publications seront disponibles dans la proposition de sous-accord de subvention.

E. Protection des données

Les données collectées et stockées dans le cadre du processus de candidature seront protégées conformément au RGPD et à la législation nationale relative à la protection des données à caractère personnel. Pour plus de détails, veuillez consulter [la politique de confidentialité](#) du CCB.

F. Coordonnées

Pour toute question, veuillez contacter ncc@ccb.belgium.be.