OPEN CALL 3 - TERMS AND CONDITIONS
PENETRATION TEST AND VULNERABILITY ASSESSMENT

CYSSDE

CYBERSECURITY
DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

Submission deadline: April 28, 2026, at 15:00 (Brussels time)

Apply at:https://cyssde.eu/open-call-3/

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however, those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

PENETRATION TEST AND VULNERABILITY ASSESSMENT OPEN CALL 3

CYSSDE

CYBERSECURITY DEPLOYMENT SUPPORT

Preparedness Support, Capacity & Capabilities

cyssde.eu

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Document History

Version	Date	Comments	Author
V1	20/11/2025	First version	Rosa Villaronga FBOX
V2	12/01/2027	First partner review	CYSSDE partners
V3	16/02/2027	Approved version	CYSSDE Selection Committee

Table of Contents

About CYSSDE

CYSSDE (Cybersecurity Deployment Preparedness Support, Capacity and Capabilities) [cyssde.eu] is a Digital Europe Programme project focused on strengthening cybersecurity resilience across Europe, particularly for Critical Entities, and Essential and Important Service Operators and next to SMEs affected by NIS2 and other regulations such as the Cyber Resilience Act (CRA). The consortium, coordinated by LSEC and composed of seven European cybersecurity experts, including a National Coordination Centre, brings over 20 years of experience supporting critical infrastructure sectors such as energy, healthcare, transport, and water. Through this expertise, CYSSDE aims to address existing vulnerabilities and help organisations improve their cybersecurity posture.

The project contributes to Member States' preparedness efforts by organising Open Calls that provide support services such as vulnerability assessments, penetration testing, threat and risk assessments, and risk monitoring. CYSSDE also develops methodologies, scenarios, and use cases aligned with NIS2 requirements, and supports the use of digital tools and infrastructures for testing and exercises. Through these activities, the initiative facilitates systematic cybersecurity testing for NCCs, NCAs, essential entities, SMEs, and start-ups, ultimately helping increase cybersecurity maturity and resilience across the EU.

Open Call 3

Welcome to the CYSSDE Third Open Call Terms and Conditions (also Terms or Guide). This document outlines the rules for participation in the CYSSDE Third Open Call, including eligibility criteria, maximum grant amount, timeline, submission rules, and the evaluation process.

Please take a moment to read this document carefully to understand the requirements and process. For any questions, please contact us at helpdesk@cyssde.eu.

Good luck!

CYSSDE Team

1. Open Call 3 Fact Sheet (Basic Conditions)

Call opening date:	27 February 2026, at 10:00 (Brussels time)
Call deadline:	28 April 2026, at 15:00 (Brussels time)
Max. grant amount	The **maximum grant amount** is up to **€ 200.000,00** per selected proposal, **based on the budget included in the application form.** **The Project budget is part of the application form. The total amount you list will be fixed and will determine the maximum grant you'll receive. Changes can be made in the Execution Plan once the project is selected.** The co-funding rate is **50%** of the budget included in your application form. The grant will be paid as a lump sum.
Number of grants and total funding available	We will support up to 12 Projects in this Open Call, either as an indicative number or until the available budget is fully used. The total budget available for this Open Call is €2.353.000,00
How to apply?	**Submit your proposal via our online form** within the deadline. **All Open Call documents** - including the template of the Sub-grant Agreement can be found here. Your application **must be in English**, and **all mandatory sections must be completed**. Proposals **can be modified after submission**, but only **until the Open Call deadline.** **Multiple submissions for the same proposal are not allowed.** If more than one proposal was submitted, only the one submitted closer to the deadline will be considered.
Duration of the Support Programme:	The Grant is offered together with the CYSSDE Support programme. **CYSSDE Support Programme lasts 18 months.**
Who can apply?	We are looking for applications from **individual entities or consortia (up to two entities)** specialising in cybersecurity**.** Eligible applicants include **SMEs** (including micro-enterprises and start-ups), **mid-caps, large companies, research centres** (including universities), and **public bodies**. Applications have to be submitted by entities with a cybersecurity background and proven expertise. All entities must be registered in, and controlled by, an entity or person established in a Member State of the European Union or an EEA country. **Consortia may consist of up to two entitie**s, with one acting as the coordinator. **At least one entity must specialise in cybersecurity.** **The applicants have to perform at least 10 penetration tests for the end-users.**

Additional conditions related to who can apply?	Applicants under EU restrictive measures are ineligible. National Coordination Centres (NCCS) that participated in OC1 are eligible to participate in OC3. The total maximum amount of funding (from CYSSDE) per participating organisation in all CYSSDE Support programmes, however, is € 200,000.00. Beneficiaries of the CYSSDE OC2 are not eligible. CYSSDE partners, its affiliates, and employees cannot apply due to the conflict of interest.

1.1. Project scope - type of activities that can be funded

The **CYSSDE Penetration Test Open Call 3 targets the performance of penetration testing and vulnerability assessmen**t for organisations aiming to enhance their operational capacity to deliver high-quality security testing services.

Selected beneficiaries will **conduct penetration tests and vulnerability assessments primarily for end users** (the minimum number of penetration tests/assessments is 10)**,** including **essential and important entities under the NIS2 Directive, operators of essential services, digital service providers, government bodies, and SMEs supporting NIS2-relevant sectors**.

Eligible activities (non-exhaustive) include:

- Hiring specialised personnel,
- Acquiring or developing tools and testing environments,
- Conducting applied research,
- Accessing intelligence services, and
- Delivering advisory or assessment services aligned with the needs of NIS2 entities.

The Open Call aims to strengthen the operational capabilities of security-testing providers to meet the needs of NIS2-covered sectors and enhance Europe's cyber-resilience.

1.2. Support programme

The CYSSDE Support Programme offers up to 18 months of tailored support alongside funding grants. Each selected beneficiary will be assigned a mentor, an expert from the CYSSDE partners, who will guide and support the implementation of their project. The programme is structured across four key stages:

- **Stage 1: Execution Plan (Month 1)**

The participant will create an execution plan (roadmap) based on their application. This plan will guide project implementation, outlining clear goals, KPIs, deliverables, and the required mentorship and resources.

- **Stage 2: Developing Testing Scenarios (Months 2–6)**

Participants will carry out preparatory activities for penetration testing, vulnerability assessments, and other supporting activities for the end user. This includes planning, system setup, designing testing scenarios, and installing/testing necessary tools and environments.

- **Stage 3: External Assessments with End Users (Months 7–15)**

At this stage, participants will perform penetration tests and vulnerability assessments for end users. Each beneficiary is expected to complete at least 10 assessments during this phase.

- **Stage 4: Outputs and Sustainability Services (Months 16–18)**

Participants will focus on generating outputs and promoting sustainability, including publications, mitigation services, and awareness creation. Mentors will assist with risk monitoring, vulnerability disclosure, communication with operators and manufacturers, and participation in CYSSDE-organised events, enabling beneficiaries to share insights and maximise the impact of their penetration testing activities.

1.3. Ground rules and formal requirements

When applying to the CYSSDE Open Call, please also note that the following conditions will be checked:

- **Submission deadline:** Only proposals submitted through the online form before the deadline will be considered.
- **Language requirement:** Proposals must be written in English. If mandatory sections are in another language, the proposal will be rejected. Non-mandatory sections in another language will not be evaluated, but the proposal will remain valid.
- **Data accuracy:** The information you provide must be correct, complete, and allow proper evaluation. Extra material provided by you that was not requested in the form will not be considered. Although we may use other resources to verify that the provided data is true.
- **Completeness:** Ensure all required fields are filled. You can edit your submission until the deadline, but no changes are allowed after that.
- **European dimension:** Your proposal should align with EU goals and contribute to creating a positive impact within the EU.
- **Conflicts of interest:** We will check for any conflicts of interest between applicants and Consortium partners. Partners, their affiliated entities, and their employees cannot participate. Each case of conflict will be reviewed individually.
- **Financial stability:** Entities under liquidation, in financial difficulty, or excluded from receiving EU funding are not eligible. We also exclude companies in bankruptcy.
- **Original work:** Execution of your project should not violate third-party IPR. It must be based on your intellectual property, or you must be allowed to use third-party rights. IPR to the project can not be subject to any dispute.
- **Ownership control and governance:** We only accept entities that are registered in the Member States of the European Union or EEA. **We do not accept entities that are directly or indirectly controlled by a person or entity established in a country that is not an eligible country (i.e. any country outside the EU Member States or EEA) or by an ineligible country entity**. This prohibition includes arrangements or coordination between shareholders from ineligible countries that would together exercise control, as well as any other financial or commercial links with ineligible countries or ineligible country entities conferring control.
- **Gender Equality Plan (GEP):** Public bodies, universities, and research organisations from EU or Associated countries must have a GEP.

Acceptance of rules: By applying, you agree to the Open Call Terms and Conditions outlined in this document.

1.4. More info about CYSSDE

You can find more information about the CYSSDE Project on https://cyssde.eu/

Open Call is managed by FundingBox Accelerator sp. z o.o. and organised by the CYSSDE Consortium partners.

2. Submission and evaluation process

Only proposals submitted through the online form before the Call Deadline will be considered. You will receive an email confirmation if the form is submitted correctly. If not, contact us immediately.

Our evaluation process is transparent, fair and equal to all participants. We will evaluate your project in a few phases described below. We will inform you about the results of the evaluation as soon as they become available.

2.1. Initial Check

After the closure of the Open Call, the system will review your proposal to ensure it meets the Call Terms and Conditions (section 1). This check will be based on the declarations in your proposal.

2.2. IN/OUT Screening

If we receive a high number of applications (more than 130 eligible applications), an additional IN/OUT screening step may be introduced. In this step, Consortium Partners will review the proposal's fit with the project scope and goals. A "Yes/No" approach will be used to assess those basic criteria, and non-compliant proposals will be rejected.

At least 1 technical partner will review the following aspects of your proposal:

- **Relevance to the Scope of the Open Call:** Proposals must clearly focus on **penetration testing and/or vulnerability assessment activities** and demonstrate the ability to deliver **a minimum of 10 assessments** for end users, including entities covered by the NIS2 Directive.
- **Alignment with NIS2 Target Sectors:** Projects must aim to engage with **end users** such as essential or important entities, operators of essential services, digital service providers, public-sector organisations, or SMEs supporting NIS2-relevant sectors.
- **Basic Technical Capability:** Applicants must show sufficient **technical competence** in penetration testing and vulnerability assessment. They should possess — or clearly plan to establish — the necessary **skills, tools, methods, and testing environments** required to carry out the proposed activities.

Please note that proposals that do not comply with the criteria described above will be rejected. Only those meeting all the criteria will proceed to the experts' evaluation phase.

Applicants will be informed about the results of this Phase 2 following the decision by the Selection Committee.

2.3. Expert Evaluation

Eligible proposals will be evaluated **by 2 independent evaluators from the pool of cybersecurity experts** using predefined award criteria:

- **Excellence**

This criterion focuses on the technical quality, relevance, and innovation of the proposed Penetration Testing or Vulnerability Assessment activities. Applicants should demonstrate:

- **Ambition and Innovation**. A clear alignment between the project proposal and the objectives of the Open Call, specifically regarding Penetration Testing and Vulnerability Assessments for (but not limited to) Critical Infrastructure, Essential and Important Services and their Operators or SMEs.
- **Technical Competence:** A high level of technical competence, showcasing the team's expertise and experience in conducting penetration tests and vulnerability assessments. Indicating previous experiences with similar projects or in this domain would be welcomed. This can also include research that led to publication or announcements of vulnerabilities, responsible disclosures made available to the public, under embargo or similar documentation.
- **Methodologies and Scenarios:** The use of established methodologies, tools, and innovative approaches for conducting assessments is recommended, but alternative approaches or combinations can equally be applied, as long as they are credible, properly presented and documented. The proposal should outline specific use cases and scenarios, including strategies for addressing challenges related to supply chain security, IoT, cloud, application, system, appliance and OT device vulnerabilities, if applicable.

- **Impact**

This criterion evaluates the expected benefits and contributions of the project. Applicants should:

- **Contribute to capabilities and capacities**. In relation to NIS2 Compliance and Resilience, define how the activities will serve the overall improvement, also at the level of European Member States. Indicate the number of additional Cybersecurity experts to be gained. Additional knowledge transfer has been done at the level of the essential entities or others. If appliances from Essential Service Operators are assessed, will the vulnerabilities found have a major impact on their operations?
- **Scope of planned actions**: provide a plan for delivering at least 10 external Penetration Testing and/or Vulnerability Assessments (see the definitions in section 2), specifying the target appliances, applications, end-users and the anticipated value these activities will bring to them (eg Penetration Testing a financial services app from a fintech company will impact 100 of its clients and provide additional security to the financial sector). This can also be described as the means to publish x-number of CVEs as a result of the actions.
- **Exploitation, market and social impact**: Demonstrate how the project supports the overall European Cybersecurity industry, the Critical Infrastructure security or impact on massive volumes of end-users, how the actions will provide an impact on the Capabilities and Capacity of the Member States or other societal benefits, emphasising the broader market and societal impacts of the activities and actions.

- **Implementation**

This criterion assesses the feasibility and practicality of the project plan. Applicants should present:

- **Resources and capabilities:** Evidence of sufficient resources and capabilities, including the necessary personnel, tools, and expertise to carry out the proposed activities. Any plans for acquiring additional resources or specialised equipment should be specified.
- **Appliance, system, application or end user engagement strategy:** a clear approach for the Penetration Testing activities or Vulnerability Assessment activities to be able to take place, by engaging with the manufacturers, developers, engineers, operators, system integrators, testing centres, end-users or others throughout the project. Any existing commitments or partnerships with Essential Service Operators or SMEs should be detailed as much as possible to support the credibility of the proposition.

- **Budget**: Applicants must provide a clear breakdown of how the requested funding (up to €200,000) will be allocated across the different budget categories. The proposal must include a credible estimation of the total project budget, explicitly detailing the required 50% co-funding contribution. All costs should be realistic, appropriate, and aligned with the successful implementation of the project.

Each criterion **will be scored on a scale from 0 to 5**, with evaluators providing individual reports and scores based on these criteria. Once the Evaluation Reports are submitted, the final score will be calculated as an average of the individual assessments provided by each evaluator on each criterion.

For each criterion, the minimum threshold is 3 out of 5 points. **The maximum total score will be 15 points, with a minimum total threshold of 10 points.**

Ties will be solved using the following criteria, listed in order of priority:

- The highest number of penetration tests planned.
- The highest number of Essential or Important Entities covered.
- The highest number of credible Letters of Intent /contracts signed.
- Applicants addressing the Space and/or Food domains.
- The highest number of end users covered.
- The highest score in the Impact section.

In cases where there is a significant divergence between the evaluators' scores (**3 points or greater discrepancy** in **two or more criteria)**, the experts will convene to establish a unified position on the evaluated proposals. If no consensus is reached, a third evaluator will be included to provide an additional assessment. In this case, the final score will be calculated by averaging the three individual scores provided by the experts.

2.4. Consensus Meeting

The Selection Committee, composed of LSEC, DNSC, TOREON, CEEYU, Cyber Ranges, INCIBE and FBA, will review and discuss the results of the previous evaluation stage, supported, if needed, by the outcome of the interviews (described below). They will reach a consensus or majority of ⅔ votes on the list of proposals to be selected, considering the evaluation scores and scope.

The final decision will be made based on the evaluation results. During the Consensus Meeting, the Selection Committee will review and discuss the 30 highest-ranked proposals. This process will result in a shortlist of 17 proposals. From this shortlist, up to 12 proposals will be selected as finalists, with 5 additional proposals placed on a reserve list. Keep in mind that although the highest-scoring proposals are usually chosen for funding, the Selection Committee can reject a candidate for valid reasons, such as not fitting CYSSDE goals and scope, limited potential impact, commercial competition issues, serious ethical concerns, or possible conflicts of interest. The exact number of proposals approved will be decided based on the overall **quality** of the proposals.

2.5. Interview (optional)

An optional final step may be added to the selection process: an interview stage. The purpose of this stage is to support the final decision on which shortlisted proposals will participate in the support programme. Interviews will be conducted by the Selection Committee only if, during the Consensus Meeting, the Committee identifies outstanding questions or requires further clarification to determine the finalists.

3. Formal check & Agreement signature

Finalists will undergo a formal check to confirm their legal status (e.g., company registration, financial documents, ownership structure, tax ID, etc.) and ownership control and governance. Therefore, we will ask you to provide documents to confirm all the details:

To confirm the ownership, control, and governance of your entity, you must submit the Ownership Control Declaration along with all required supporting documents.

To confirm your formal status, we may ask the applicants for: the company's registration document, the legal representation (optionally POA), tax ID number, ownership structure[1], financial statements, document/s confirming the staff headcount, Bank Identification form, and other documents in case of doubts raised during the checks (this list is not exhaustive)

Documents must be provided within the given deadline. If you don't deliver the requested documents on time, without a clear and reasonable justification, we will have to exclude you from further formal assessment.

After passing this check, we will invite you to sign the Sub-grant Agreement with the CYSSDE consortium to officially participate in the programme.

4. After the Sub-Grant Agreement signature

4.1. Payment conditions

The Grant will be paid as a lump sum. Payments depend on the successful and timely completion of each stage of the work planned and outlined in the Execution Plan developed at the beginning of the Support programme. Payments are scheduled in tranches as follows:

Stage 1: Up to 10,000.00€ (5%) of the Grant Amount by month 2

Stage 2: Up to 60,000.00€ (30%) of the Grant Amount by month 7

Stage 3: Up to 80,000.00€ (40%) of the Grant Amount by month 16

Stage 4: up to 50,000.00€ (25%) of the Grant Amount by month 19

A delayed payment mechanism will be applied to all payments. 20% of each tranche will be paid once the whole CYSSDE Project is completed. This should happen approximately 9 months after the end of the CYSSDE Project. The expected end of the CYSSDE is May 31, 2028. Relevant provisions will be included in the Sub-grant Agreement. Please consider that the CYSSDE Project might be extended.

4.2. Progress evaluation

We pay upon the delivery of the agreed results - not upon delivery of certain receipts. Therefore, Consortium Partners, gathered in the Selection Committee, will evaluate your progress regularly.

Payment milestone	Explanation

[1] If the ownership structure is not clear from the registration documents, additional documents confirming the ownership structure, e.g. statute, company deed, founding act, share register, in a joint-stock company - list of the company's shareholders; etc, may be requested.

Stage 1: Execution plan	Within the first month of the Support Programme, you will prepare an *Execution plan, based on the presented proposal,* outlining the final budget, KPIs, and deliverables for performance assessment. It will also cover any specific Ethics Assessment requirements (You will also be required to accept CYSSDE's Declaration Of Ethical Compliance And Data Protection Conformity. It can be found here) The *Execution plan* will be evaluated by the mentor assigned, taking into account the Deliverable quality (90%) and Deadline compliance (10%). Each criterion will be scored from 0 to 10, and the final score will be calculated based on the weights indicated. A score of **7 points** or more is required to continue in the program.
Stage 2 to 4	Before each payment, the Selection Committee will review your progress. Performance will be evaluated by the mentor assigned based on: - Deliverables quality (30%) - KPIs (60%) - Deadline compliance (10%) Each criterion will be scored from **0 to 10**, and the final score will be calculated based on the weights indicated. A score of **7 points** or more is required to continue in the program. For more details, please check the template of the Sub-grant Agreement.

5. Contact us

If you have any questions about our application process, feel free to reach out to our helpdesk at the CYSSDE Helpdesk or email us at helpdesk@cyssde.eu.

Please note that responses are given individually and do not change these Terms; they are provided for informational purposes only.

In case of any technical issues or problems, please include the following information in your message:

- your username, phone number and email address;
- details of the specific problem (e.g. error messages you encountered, bug description, i.e. if a dropdown list isn't working, etc.); and
- screenshots of the problem.

6. Complaints

If you believe there was an error in one of the evaluation phases, you may submit a complaint within three (3) calendar days after sending the results to you. Send it to helpdesk@cyssde.eu in English and include:

- your contact details (including email),
- the subject of your complaint,
- evidence of the specific issue.

Please note that we will review only complaints related to:

- errors in the process caused by our staff,
- technical issues beyond the applicant's control,
- clear human or mechanical errors made by our staff,
- incorrectly marked statements, minor clerical errors, and obvious typographical mistakes.

Please note that we will not review complaints related to the content of the expert evaluations.

Complaints will be reviewed within seven (7) calendar days. If more time is needed, we will inform you via email. Anonymous complaints or those with incomplete information will not be considered.

7. Final provisions

Any issues not covered by these Terms and Conditions are governed by Polish law, Digital Europe Programme rules, and EU grant regulations.

We make our best effort to keep all provided data confidential; however, for the avoidance of doubt, you are solely responsible for indicating your confidential or sensitive information as such. Please be aware that your application form will be shared with the external evaluators and CYSSDE Consortium partners.

You retain ownership of your intellectual property rights (IPR).

The signature of the Sub-grant Agreement is the initial condition to establish any obligations among applicants and any Consortium partners (with respect to the obligation of confidentiality of the application). The Sub-grant Agreement will include a set of obligations towards the European Commission (for example: promoting the project and giving visibility to the EU funding, maintaining confidentiality, and understanding potential controls by the EC/ECA, EPPO, and OLAF).

Please be aware that eligibility criteria will be checked throughout the process, including a final review and support programme.

In the event of any discrepancies between these Terms and their Annexes, the Terms shall prevail.

The CYSSDE Consortium reserves the right to cancel or modify the call at any time, informing applicants accordingly.

Need more help? Contact us at helpdesk@cyssde.eu, and we'll be happy to assist.

Annex 1: Glossary of Acronyms

Acronym	Definition/Meaning
CVEs	Common Vulnerabilities and Exposures
CRA	Cyber Resilience Act
CYSSDE	Cybersecurity Deployment Preparedness Support, Capacity and Capabilities
EEA	European Economic Area
EU	European Union
GA	Grant Agreement
GEP	Gender Equality Plan
IoT	Internet of Things
IPR	Intellectual Property Rights
KPIs	Key Performance Indicators
NCAs	National Cybersecurity Authorities
NCC	National Coordination Centre
NIS2	Network and Information Security 2 (Directive)
OT	Operational Technology
SMEs	Small and Medium-sized Enterprises

Terms and Conditions
Penetration Test and Vulnerability Assessment Open Call

Do you have questions or want to know more?

Contact us

Managed by:

FundingBox

https://fundingbox.com/

PENETRATION TEST AND VULNERABILITY ASSESSMENT OPEN CALL 3

CYSSDE

CYBERSECURITY DEPLOYMENT SUPPORT

Preparedness Support, Capacity & Capabilities

cyssde.eu

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE