CIRCAT
Cybersecurity Infrastructure Resilience, Collaboration and Advanced Training

CIRCAT Open Call 1

FAQS

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project is supported by the European Cybersecurity Competence Center (ECCC) and its members.

Eligibility conditions

- **Are SMEs eligible to apply for the CIRCAT Open Call?**

Yes, SMEs are eligible to apply, provided they are registered in, and controlled by, an entity or person established in a Member State of the European Union or an EEA country. SMEs can apply if they operate as one of the targeted profiles, such as Operators of Essential Services (OES) or other relevant stakeholders with the capacity to aggregate demand.

- **Can a company legally registered in an EU/EEA country but ultimately owned by a non-EU/EEA national apply?**

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. CIRCAT does 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.

Eligibility conditions

- **How are sectors not explicitly listed classified within the prioritized verticals?**

Beneficiaries must design penetration testing scenarios within one of the explicitly prioritized verticals: Energy, Health, Public Administration, Digital infrastructure, ICT Service management (B2B), and Financial market infrastructure

Budget, cost and payments

- **What are the eligible costs for the grant, and is it paid as a fixed sum or based on hourly rates?**

The grant awards up to a maximum of EUR 40,000 per grantee, which is a fixed amount based on the total project budget outlined in the application form. The funding is paid as a lump sum upon the delivery of the agreed results, not upon the delivery of certain receipts. Applicants must co-finance the proposed activity by a minimum of 50% of the total project costs

- **Is subcontracting allow and what are the limtations?**

Yes, subcotracting is allow however with some limitations.

Best Value for Money: Beneficiaries must select subcontractors offering the best value for money or the lowest price, ensuring there is no conflict of interest.
Core Tasks: You cannot subcontract the core tasks of the action. Subcontracting is reserved for specific, ancillary, or technical implementation services. **In this specific Open Call, cybersecurity activities can not be subcontracted.**
Cybersecurity & Sovereignty Compliance: Subcontractors must comply with the Programme Security Instruction (PSI) for the Digital Europe Programme regarding protective security procedures.
Nationality and Ownership Restrictions: Participation and subcontracting are restricted to entities established in EU Member States or eligible associated countries. Subcontractors may be required to prove they are not controlled by non-eligible third countries.

Project technical implementation

- **Are activities such as acquiring IT infrastructure, software, or secure data storage eligible for funding?**

Eligible activities are strictly limited to vulnerability testing support (developing and documenting realistic penetration testing scenarios) and threat and risk assessment support (conducting customised risk scenario analyses). Advancing IT infrastructure by acquiring data handling systems, software, or secure data storage does not fall under the eligible activities

- **Do applicants need to own the targeted infrastructure, and is a formal letter of support from the operator required?**

Applicants without direct access to the required infrastructure are eligible and encouraged to apply. While direct involvement or access to a large operator is a "nice to have," it is not mandatory.

Project technical implementation

- **Does the funded activity require live testing on the target operator's production systems?**

Stage 2 of the support program focuses on identifying relevant threat vectors and detailing the technical steps, tools, and methodologies required to safely replicate these threats in a controlled environment.

- **Must applicants use the published scenario template for their application?**

No, the scenario template provided in Annex 1 is for your reference only, and you do not need to complete it now. Only selected companies that sign the Sub-Grant Agreement (SGA) will be required to work on it. You must solely use the online application form and ensure all mandatory sections are completed.

Evaluation and selection

- **Does the evaluation process rely on innovation?**

Yes, the evaluation process assesses the proposal's potential to generate significant benefits for society, industry, or public services, including increased competitiveness and innovation capacity under the "Impact" criteria.

- **Is there a specific number of scenarios to be proposed in the application?**

Beneficiaries must design "a Penetration Testing Scenario" within one of the prioritized verticals. The evaluation process assesses the scope of the proposal, such as how many targeted CIRCAT technologies and EU regulatory frameworks the scenario integrates, the proportion of targeted infrastructure assets it can detect and assess, and how many potential vulnerabilities it will expose and analyse.

Join the CIRCAT Initiative

Deadline:

July 9, 2026

Apply Online:
opportunities.getonepass.eu/open-opportunities/circat-opencalls/opencall1

Program Details & Docs: circat.eu
Helpdesk & Support: circat.help@fundingbox.com