ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme on Cybersecurity

Florina MUNTEANU
ECCC – Programme Officer
**26/11/2024**

#DigitalEU

Agenda

1. The ECCC and its network
2. Digital Europe Programme upcoming funding opportunities
3. Tips & tricks for writing a DEP Cybersecurity proposal
4. Q&A

The ECCC

The ECCC is the engine for the implementation of Europe's strategy in research, innovation, and industrial policy in the area of cybersecurity.

Proposed EU cybersecurity funding sources (2021-2027)
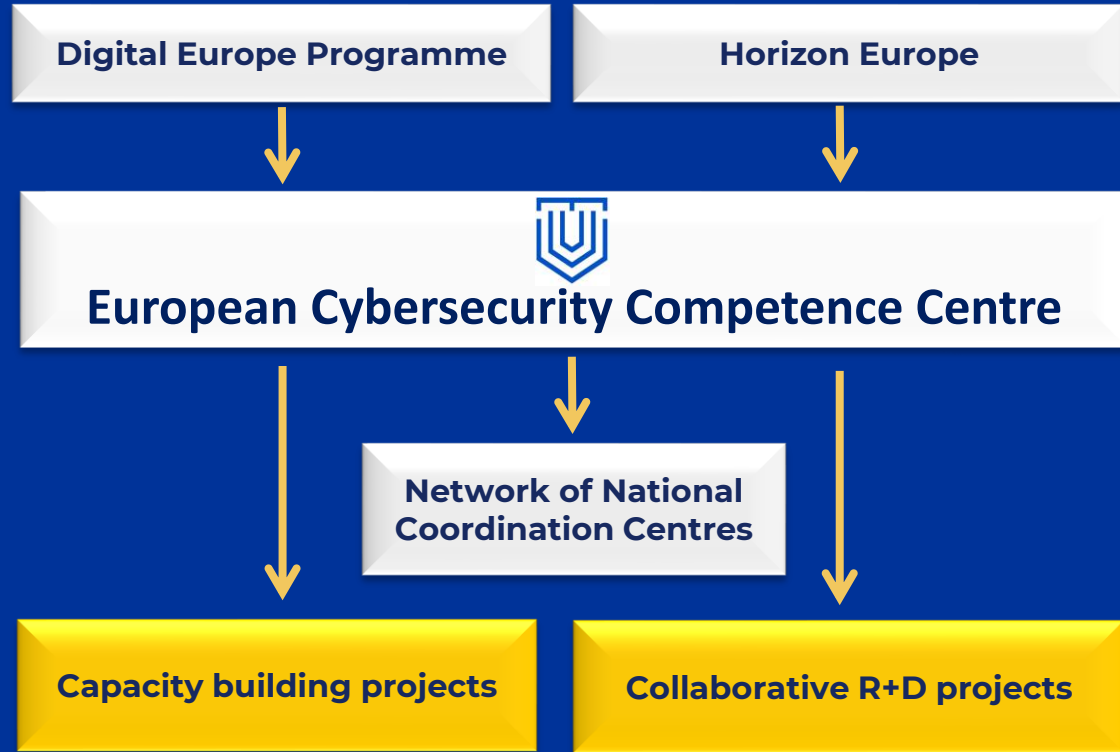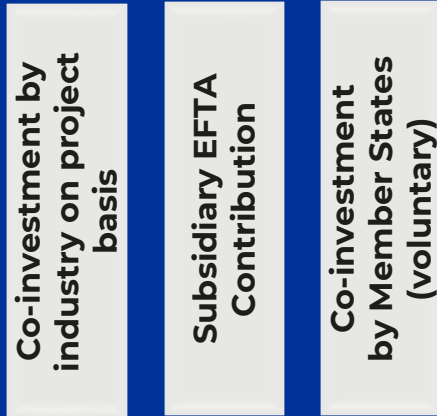
DIGITAL-ECCC-2024-DEPLOY-CYBER-07 - Topics call list

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC

• National SOCs (Joint Procurement budget 15M€)

EUR 5.800.000

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT

• Enlarging existing or Launching New Cross-Border SOC Platforms (Joint Procurement budget 17M€)

EUR 5.000.000

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS

• Strengthening the SOC Ecosystem

EUR 2.000.000

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

• Development and Deployment of Advanced Key Technologies

EUR 35.000.000

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

• Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

EUR 35.000.000

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02

• Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

EUR 20.000.000

Timetable and deadlines

Call opening:	**4 July 2024**
Deadline for submission:	**21 January 2025 – 17:00:00 CET (Brussels)**
Evaluation:	**February – March 2025**
Information on evaluation results:	**April – May 2025**
GA signature:	**October 2025**

National SOCs

Objective:

- **Create or strengthen National SOCs**, in particular with state-of-the-art tools for monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs;

- **benefit from information and feeds from other SOCs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis**.

For this topics an expression of interest shall also be submitted no later than the 21 January 2025 at 17:00 Brussels time.
Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en.
Applications must be submitted in the correct form, duly completed and dated.

Scope (1/2):

The aim is capacity building for new or existing National SOCs. This can include for example:

- automation, analysis and correlation tools and data feeds covering Cyber Threat Intelligence (CTI) at various levels ranging from field data to Security Information and Event Management (SIEM) data to higher level CTI;
- leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context;
- use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information;
- the operations should be built upon live network data. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

Key elements:

- ✓ translation of advanced AI/ML, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real conditions in combination with access to supercomputing facilities;
- ✓ knowledge transfer, such as training of cybersecurity analysis;
- ✓ National SOCs must share information with other stakeholders in a mutually beneficial exchange of information and commit to apply to participate in a cross-border SOC platform within the next 2 years, with a view to exchanging information with other National SOCs.

European Commission

Scope (2/2):

To support the activities in scope of a National SOC, the following two work streams of activities are foreseen:

a)   [Procurement]

A Joint Procurement Action with the Member State where the national SOC is located: this will cover the procurement of the main equipment, tools and services needed to build up the National SOC.

b) [Building up and running the National SOC]
A grant will also be available to cover, among others, the preparatory activities for setting up the National SOC, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National SOC, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

- Applications shall be made to both work streams.
- Applications to the Call for Expression of Interest (CfEI) will be object of evaluations procedures.
- Grants will only be awarded to applicants that have succeeded the CfEI evaluation.

- Indicative duration of the action: 36 Months

- Type of Action: Simple Grant — 50% funding rate

- Grant amount: between 1 and 2 million EUR

- Type of Beneficiaries: public bodies acting as National SOCs

The target stakeholders under a) **[Procurement]** and b) **[Building up and running the National SOC]** are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU".

Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT

Enlarging existing or Launching New Cross-Border SOC Platforms

Objective:

This action **aims at new cross-border SOC platforms, as well as enlarging those that were already launched under the previous** DIGITAL work programme (2021-2022).

While the main focus of this action is on processes and tools for prevention, detection and analysis of emerging cyber-attacks, it also **foresees in particular the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU.**

In case of enlargement of an ongoing cross-border grant, the new consortium should be composed by the coordinator of the ongoing grant plus the new entities that want to join the cross-border SOC.

The new grant will work in close cooperation with the ongoing one.

For this topics an expression of interest shall also be submitted no later than the 21 January 2025 at 17:00 Brussels time.
Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en.
Applications must be submitted in the correct form, duly completed and dated.

Scope:

- Supporting the development of better performing data analytics, detection, and response tools, through the pooling of larger amounts of data, including new data generated internally;
- act as a central point allowing for broader pooling of relevant data and CTI, enable the spreading of threat information on a large scale and among a large and diverse set of actors;
- enhancing and consolidating collective situational awareness and capabilities in detection and CTI;
- support common situational awareness and effective crisis management and response by providing relevant information to networks and entities responsible for cybersecurity operational cooperation and crisis management.

Key elements:
- ✓ for cross-border SOC platforms, there is a crucial need for novel tools based on advanced Artificial Intelligence and machine learning (AI/ML), data analytics and other relevant cybersecurity relevant technologies, based on research results and further tested and validated in real conditions, in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms).

Scope:

To support the above activities of a Cross-Border SOC platform, the following two workstreams of activities are foreseen:

a) [Procurement]
A Joint Procurement Action with the Member State participating in the Cross-Border SOC platform: this will cover the procurement of the main equipment, tools and services needed to build up the Cross-Border SOC platform.

b) [**Building up and running the Cross-Border SOC platform**] A grant will also be available to cover, among others, the preparatory activities for setting up the Cross-Border SOC platform, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Cross-Border SOC platform, e.g., using the equipment, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

- Applications shall be made to both work streams.
- Applications to the Call for Expression of Interest (CfEI) will be object of evaluations procedures.
- Grants will only be awarded to applicants that have succeeded the CfEI evaluation.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT

- Indicative duration of the action: 36 Months

- Type of Action: Simple Grant — 50% funding rate

- Grant amount: Between 2 and 3 million EUR

- Type of Beneficiaries: Public bodies acting as National SOCs

The target stakeholders under a) **[Procurement]** and **b)** [**Building up and running the Cross-Border SOC platform**] above are public bodies acting as National SOCs linked to a "call for expression of interest to deploy and operate Cross-border SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU".

Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

Strengthening the SOC Ecosystem

Objective:

- It will **empower SOCs which are linked to National SOCs, and to a stronger collaboration between local SOCs, National SOCs and Cross-Border SOC platforms**, leading to an increased data sharing and better detection capability for cyber threats.

- **Foster interoperability**, identifying what data can be shared, how this is shared and in what format, requirements and sharing agreements, and ways to enable better exchange.

- **Increased engagement**, including from the private sector, and to a better collaboration towards a common EU cyber threat knowledge base and technological independence.

- **Develop a comprehensive governance framework, with for example enrolment conditions and vetting procedures**. The aim is to foster discussion between such platforms, sharing best practices and identifying opportunities for collaboration.

✓ Links to the actions funded under the Cybersecurity Skills Academy (in the main Digital Europe work programme) can also be envisaged.

✓ One Coordination and support action will be selected, bringing together the largest possible network of National and Cross-Border SOC platforms.

European Commission

Scope:

Actions should address one or more of the following actions:

- **foster the collaboration and interconnection** between Cross-Border SOC platforms and National SOCs, as well as fostering the link between National SOCs and other SOCs at national level;
- support the **cooperation and coordination of Cross-Border SOC platforms**, both between different Cross-Border SOC platforms, and with relation to national SOCs and other SOCs;
- foster links between public sector and industry, and stimulate **mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities;**
- **foster links between SOCs and industrial stakeholders in artificial intelligence** and in other enabling technologies, fostering the adoption of such technologies;
- **engage stakeholders from the HPC stakeholder community and practitioners of breakthrough AI technologies, to develop a blueprint for the requirements of AI models that necessitate access to large or smaller HPC facilities**.

ENISA is tasked to develop guidelines on the **interoperability** of Cross-Border Cyber Hubs.
Therefore, the selected proposal shall be required to collaborate with ENISA on the aspect of the interoperability.

- Indicative duration of the action: 36 Months

- Type of Action: Coordination and Support Actions — 100% funding rate

- Grant amount: #1 proposal for up to 2 million EUR

- Type of Beneficiaries: National SOCs, Cross-Border SOC Platforms and other relevant stakeholders

Development and Deployment of Advanced Key Technologies

Objective:

- The objective is to enable European cybersecurity actors to **take advantage of new breakthroughs in *key digital technologies*** (*such as Artificial Intelligence Big Data Analytics, Quantum, Blockchain Technology, High Performance Computing and Software-Defined Networking*) **improving detection and prevention capabilities, efficiency, scalability, and facilitating data sharing and regulatory compliance.**

- In particular innovative technologies should allow for the **processing of larger amounts of data, automating real-time pattern recognition, log analysis, vulnerability scanning,** while enabling security professionals to focus on **higher level interpretation of data and response decisions**.

A priority is to create and strengthen capacity for original Cyber Threat Information (CTI), e.g., in the form of CTI feeds or services.

European Commission

Scope:

Activities should fortify cybersecurity capabilities using breakthrough technologies, encompassing various aspects of cybersecurity. In one or more of the following topics should be addressed:

- **Real-time Monitoring and Incident Response**

- **Malware Defence and Analysis**

- **Proactive Vulnerability Management**

- **Data Protection and Anomaly Detection**

- **Incident investigation**

- **Data Utilisation with Privacy**

✓ The systems, tools and services developed under this topic, where relevant, will be made available for licencing to National and/or Cross-Border SOC platforms under favourable market conditions.

✓ The deployment of such technologies must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.

European Commission

- Indicative duration of the action: 36 Months

- Type of Action: SME Support Actions — 50% and 75% (for SMEs) funding rate

- Grant amount: Between 3 and 5 million

- Type of Beneficiaries:

  - ✓ Technology companies, especially SMEs, working to provide and support other private and public organisations with cyber threat detection and CTI feeds.

  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

Objective:

- Complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for large industrial installations and infrastructures, by assisting Member States in their efforts to **improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise;**

- creation of platforms that serve as a reference point and provide services such as penetration testing and threat assessments for providers of essential services and critical infrastructures, as well as other actors.

- Preparedness actions should benefit entities in sectors indicated as critical infrastructure sectors in NIS2
- This involves data and operational measure regarding cybersecurity, including penetration tests and exploitable vulnerabilities

European Commission

Scope:

The provision of preparedness support services (ex-ante) shall include activities reported below, addressing for example large industrial installations or infrastructures, operators of essential services, digital service providers and governmental entities:

Support for testing for potential vulnerabilities:

- Development of penetration testing scenarios.
- Support for conducting testing of EE operating CI for potential vulnerabilities.
- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises Evaluation and/or testing of MS cybersecurity capabilities.
- Consulting services.

Support for threat assessment and risk assessment:

- Threat Assessment process implementation and life cycle.

- Customised risk scenarios analysis.

Risk monitoring service:

- Specific continuous risk monitoring such as attack surface monitoring, risk.
- Monitoring of assets and vulnerabilities.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- Indicative duration of the action: 36 Months

- Type of Action: Grants for Financial Support — 100% funding rate

- Grant amount: Between 3 and 5 million EUR

- Type of Beneficiaries:
  - ✓ This topic targets in particular industrial players, national cybersecurity authorities, national cybersecurity competence centres, National Coordination Centres (as defined in Regulation (EU) 2021/887), private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries, to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties.
  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

Objective:

Proposals should contribute to achieving at least one of these objectives:

- Development of trust and confidence between Member States.

- Supporting market surveillance authorities/notifying authorities/national accreditation bodies to **implement the CRA.**

- **Effective operational cooperation** of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs, or cooperation of OSE including public authorities.

- **Better security and notification processes** and means for Essential and Important Entities in the EU, including cross-border (automated) incident notification systems.

- **Better reporting of cyber-attacks to law enforcement authorities** in line with the Directive on attacks against information systems.

- Improved security of network and information systems in the EU.

- **More alignment of Member States' implementations of NIS2**.

- **Support cybersecurity certification in line with the amended Cybersecurity Act.**

Scope:

The action will focus on the support of at least one of the following priorities:

- Implementation, validation, piloting and **deployment of technologies**, tools and IT-based solutions, processes and methods **for monitoring and handling cybersecurity incidents.**
- **Increasing capacity** for market surveillance authorities/notifying authorities/national accreditation bodies in view of tasks as provided by the **CRA**.
- **Collaboration, communication, awareness-raising, knowledge exchange and training, on the implementation of NIS2.**
- **Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies for** effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.

- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.
- Ensure that manufacturers improve the security of products with digital elements and enhance **the transparency of security properties** of products with digital elements. **Facilitate compliance for hardware and software producers.**
- Enable **businesses across all sectors and consumers to use products with digital elements securely.**
- **Support to Cybersecurity certification.**

- Indicative duration of the action: 36 Months

- Type of Action: Simple Grants — 50% funding rate

- Grant amount: Between 2 and 4 million

- Type of Beneficiaries:
  - ✓ This topic targets relevant industrial stakeholders, including SMEs and start-ups in the scope of the upcoming CRA, concerned by the NIS2 Directive or that may benefit from the European cybersecurity certification schemes. It refers also to Member State competent authorities, which play a central role in the implementation of the NIS2 Directive, CSIRTs - including sectorial CSIRTs, SOC, OES, DSP, ISACs, actors that play a role in the implementation of the Cyber Resilience Act (including certification bodies), and any other actors within the scope of the legislations mentioned above.
  - ✓ Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation.

- For the topics:
  - ✓ SOC - National SOC
  - ✓ SOCPLAT - Enlarging existing or Launching New Cross-Border SOC Platforms
  - ✓ KEYTECH - Development and Deployment of Advanced Key Technologies
  - ✓ LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10).*

- For the topics:
  - ✓ SOCSYS - Strengthening the SOC Ecosystem
  - ✓ CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

following reimbursement option for equipment costs applies: depreciation only *(see section 10)*

Award criteria

Relevance
- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*

Implementation
- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work

Impact
- Achievement of the expected outcomes and deliverables, as well as communication and dissemination
- Competitiveness strengthen and contribution to society

*<u>Not applicable for topics</u>: NATIONAL SOCs, SOCPLAT, SOCSYS.
*<u>Applicable only for the topics</u>: KEYTECH, LARGEOPER, CYBERSEC-02

Criterion 1. RELEVANCE

Aspects to be taken into account (Items 3 and 4 may not be applicable to all topics see call document):

1. Alignment with the objectives and activities as described in the Call document:
- Proposal in line with the call objectives
- Proposal's objectives - clearly defined, justified/demonstrated, aligned with the objectives of the specific topic, with relevant measurable KPIs and target values

2. Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level:
- Sufficiently explained and substantiated
- Provide clear references to specific initiatives in terms of synergies and don't stay general

3. Extent to which the project would reinforce and secure the digital technology supply chain in the EU
- Sufficiently described
- Not checked for all topics

4. Extent to which the project can overcome financial obstacles such as the lack of market finance
- Not checked for all topics

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Aligned Clear Explained References

Criterion 2. IMPLEMENTATION (1/2)

Aspects to be taken into account:

1 - Maturity of the project

- Ensure the right maturity of the proposal with respect to the requirements of the call; maturity can touch upon tools, technology, and services, the experience of partners, standards, etc.
- Provide details on the involvement of the beneficiaries in the actions, the advancement compared to the current state of the art, and the topics to be addressed

3 - Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

- Description of the consortium participants
- Sufficient information on the background and specific expertise of team members
- Adequate experience to be sufficiently demonstrated (eg. List of previous projects relevant to the topic)
- By the time of the submission, all entities participating in a proposal should be fully operational

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Maturity   Added-value   State-of-the-art   Experience

Criterion 2. IMPLEMENTATION (2/2)

2 - Soundness of the implementation plan and efficient use of resources

- <u>Implementation plan</u> – clearly define the expected scope of the work and its connection to the objectives

- <u>Work plan</u> – provide sufficient explanation about
  - the rationale of each WP,
  - the work to be performed within each WP,
  - the connection between the different WPs,
  - how the activities outlined in the WPs will contribute to achieving the proposal's goal

- <u>Tasks</u>
  - if addressing testing and deployment – provide info on where deployment will take place
  - For proposals including FSTP activities, they should better define a concrete and feasible timeline.

- <u>KPIs</u> – relevant, well defined (including the baseline, connection to the objectives), including a progress evaluation methodology and quality assurance; best KPIs are quantitative and measurable.

- <u>Milestones</u> - scheduled over the duration of the project (and not at the end), with enough time for evaluation and corrective measures; avoid setting too many / too specific.

- <u>Deliverables</u> – provide detailed descriptions and always pay attention to potential requirements in the Call document

- <u>Use of resources</u> – realistic and detailed allocation per WP per partner, both in terms of workload but also of competencies required

- Make sure the Gantt chart provides a proper and logical sequencing of activities.

- <u>Risks</u> – describe impact and likelihood; provide clear mitigation strategies

Logic   Interlinked   Balanced   Controllable Measurable Complete

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Criterion 3. IMPACT

Aspects to be taken into account:

1 - Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements

- elaborate clearly the scale and significance, make clear how the project intends to improve with respect to current baselines.
- KPIs well defined (clear baseline, aligned to the project goals, ambitious)
- target audience, key messages, communication channels - well identified and defined; tailored to identified wider audience; credible and ambitious dissemination strategy

2 - Extent to which the project will strengthen competitiveness and bring important benefits for society

- provide concrete examples and sufficient details

!!!!!

IMPACT criterion will be considered in case of ties after RELEVANCE

Scale Impact   Audience   Impact

Questions?

1. Your NCC
2. Funding and Tender portal

General FAQ [link];

Topic Q&A [example link]

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

References

Digital Europe Programme website : https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Digital Europe Programme Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377

Funding & tender opportunities portal: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

Call document: call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf (europa.eu)

Keep in touch

[ECCC Newsletter](#)

[ECCC LinkedIn](#)

[ECCC Twitter/X](#)

[ECCC Instagram](#)

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Thank you!

Europe digitally secured