ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme (DIGITAL)

Call for proposals

Strengthening European Cybersecurity Technologies, Capacities and Preparedness

(DIGITAL-ECCC-2027-DEPLOY-CYBER-11)

Version 1.0
01 09 2026

HISTORY OF CHANGES			
Version	Publication Date	Change	Page
1.0	01.09.2026	Initial version.	

CALL FOR PROPOSALS

0. Introduction

This is a call for proposals for EU **action grants** in the field of Cybersecurity under the **Digital Europe Programme (DIGITAL)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2024/2509 (EU Financial Regulation)[1]
- the basic act (Digital Europe Regulation 2021/694[2]).

The call is launched in accordance with the ECCC Digital Europe Cybersecurity 2025-2027 Work Programme[3] and will be managed by the European Cybersecurity Competence Centre (ECCC).

⚠ Please note that this call is subject to possible amendments of the ECCC Digital Europe Cybersecurity 2025 - 2027 Work Programme. In case there are substantial changes, the call may be modified. All updates will be reflected in the call document.

The call covers the following **topics**:

- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI – Cybersecure tools, technologies and services relying on AI**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME – Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP – Coordinated preparedness testing and other preparedness actions**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH – Regional Cable Hubs**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC – Enhancing the NCC Network**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG – Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements**
- **DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE – Dual-use technologies**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call document, the Model Grant Agreement, the EU Funding & Tenders Portal Online Manual and the EU Grants AGA — Annotated Grant Agreement.

---

1 Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) ('EU Financial Regulation') (OJ L, 2024/2509, 26.9.2024).

2 Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme (OJ L 166, 11.5.2021, p. 1).

3 Adopted by the GB of ECCC in Decision No 2026/07 concerning the adoption of the work programme for 2025-2027 and the financing decision for the implementation of the Digital Europe Programme.

These documents provide clarifications and answers to questions you may have when preparing your application:

- the Call document outlines the:
  - background, objectives, scope, outcomes and deliverables, KPIs to measure outcomes and deliverables, targeted stakeholders, type of action and funding rate and specific topic conditions (sections 1 and 2)
  - timetable and available budget (sections 3 and 4)
  - admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)
  - criteria for financial and operational capacity and exclusion (section 7)
  - evaluation and award procedure (section 8)
  - award criteria (section 9)
  - legal and financial set-up of the Grant Agreements (section 10)
  - how to submit an application (section 11).
- the Online Manual outlines the:
  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
  - recommendations for the preparation of the application.
- the AGA — Annotated Grant Agreement contains:
  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc)*.

You are also encouraged to visit the EU Funding & Tenders Portal to consult the list of projects funded previously.

1. Background

The accelerated evolution of digital transformation is reshaping economies, societies, public services and industrial value chains worldwide, while redefining how citizens, businesses, and administrations interact, operate, and safeguard information. As digital technologies become increasingly embedded in critical infrastructures, public authorities, businesses, and essential services, they create new opportunities for innovation and competitiveness, but also increase exposure to evolving cyber threats affecting information and communication technologies, operational technologies, supply chains, and digital services.

Recent geopolitical developments, hybrid threats and cyber incidents underline the need for the Union to strengthen its cybersecurity capacities, operational preparedness and resilience. Cybersecurity is therefore, a key condition for protecting Europe's digital sovereignty, strengthening resilience and ensuring trust in digital technologies and services.

In response to these challenges, the EU strategically invests in cybersecurity deployment through the Digital Europe Programme. The third Work Programme (2025-2027), implemented by the European Cybersecurity Competence Centre (ECCC),

supports actions that strengthen cybersecurity capacities and capabilities across the Union, in alignment with the EU Cybersecurity Strategy, The Cyber Solidarity Act, the ECCC Strategic Agenda, and relevant EU Cybersecurity Legislation.

The 2027 Call 11 focuses on the key following areas of cybersecurity deployment:

- **Cybersecure tools, technologies and services relying on AI:** This action addresses AI-based technologies, including generative AI, for national authorities, competent authorities, National and Cross-Border Cyber Hubs, CSIRTs, public bodies, NIS 2 entities and other relevant stakeholders. It supports the development and deployment of AI-based cybersecurity systems, tools and services for threat detection, vulnerability detection, threat mitigation, incident recovery, data analysis and data sharing, while also addressing the cybersecurity, robustness and trustworthiness of AI solutions.

- **Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions:** This action supports the market uptake and dissemination of innovative AI-powered cybersecurity solutions for SMEs and aims to improve knowledge and auditing of cybersecurity preparedness. It supports the development and deployment of AI-powered solutions, tools and services for European SMEs, including user-friendly tools for risk management, threat detection, incident response and notification.

- **Coordinated preparedness testing and other preparedness actions:** This action covers two actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism: coordinated preparedness testing of entities operating in sectors of high criticality across the Union, and other preparedness actions for entities operating in sectors of high criticality and other critical sectors. It supports activities including penetration testing, threat assessment, vulnerability monitoring, risk monitoring, coordinated vulnerability disclosure, exercises and training courses.

- **Regional Cable Hubs:** This action supports the progressive establishment of Regional Cable Hubs, one per sea basin of the EU, to enhance threat detection and operational security around undersea cable infrastructures. It supports the set-up of processes, tools and services for the detection and analysis of emerging threats, near real-time situational awareness, incident reporting and information sharing between relevant national authorities.

- **Enhancing the NCC Network:** This action supports the operation of the National Coordination Centres and enables them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and the strengthening of cybersecurity capacities. It also supports activities related to the Cybersecurity Competence Community, cybersecurity awareness, safer digital behaviours, cybersecurity skills, start-ups and SMEs, and the promotion of market-ready cybersecurity solutions.

- **Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements:** This action supports the European ecosystem in strengthening its cybersecurity capacities and in implementing the regulatory framework in line with Cyber Resilience Act, the NIS 2 Directive, GDPR, DORA, the Cybersecurity Act, specific requirements of the AI Act, and other relevant EU cybersecurity legislation. It supports stakeholders in addressing new responsibilities and obligations linked to EU cybersecurity legislation, including through financial and organisational support where relevant.

- **Dual-use technologies:** This action supports cooperation between the civil and defence spheres regarding dual-use projects, services, competences, and applications in cybersecurity. It aims to enhance operational cooperation through the development of dual-use working prototypes, ready-to-market products and operational infrastructures related to cybersecurity technologies, applications, and tools that have relevance in both civilian and defence contexts

These initiatives are subject to Article 12(5) of the Digital Europe Programme Regulation, ensuring that entities involved meet EU security requirements.

Together, these actions aim to strengthen European cybersecurity capacities and operational preparedness, while supporting a more secure, sovereign and resilient digital Europe. They will promote the deployment and uptake of advanced cybersecurity technologies, tools and services, enhance cooperation and information sharing between relevant actors, and support the resilience of public and private entities across the Union.

2. Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action and funding rate — Specific topic conditions

Guidance on milestones, deliverables and KPIs

Applicants shall define milestones, deliverables and Key Performance Indicators (KPIs) that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities. Milestones, deliverables and KPIs should be designed to support effective monitoring of the action's implementation, progress, performance, and results.

Milestones

Milestones should represent meaningful decision points, implementation achievements or validation steps in the action. Routine project management events, such as the kick-off meeting, periodic meetings, or the submission of progress reports, should not be proposed as milestones.

 Applicants should carefully consult the Proposal Template when preparing the list of milestones, as it contains additional guidance and requirements regarding their structure, content and timing.

Deliverables

Deliverables should provide concrete and substantive outputs of the action, such as technical specifications, methodologies, tools, services, deployment reports, validation reports, pilot results, training materials, guidelines, operational procedures, dissemination and exploitation plans, or other outputs directly linked to the action's objectives and expected outcomes. Deliverables should not include administrative or progress reporting, unless such reporting is explicitly required in the call conditions.

In addition, the ECCC is required to monitor programme-specific Key Performance Indicators (KPIs) as part of the regular project reporting process. This obligation is established under the Digital Europe Programme legal framework and supports the monitoring, evaluation and assessment of the Programme's performance, achievements and impact. The collection of these indicators also contributes to measuring progress towards the Programme's objectives and provides evidence for reporting, benchmarking and future policy development.

To fulfil this obligation, applicants shall include a mandatory yearly deliverable to be submitted every 12 months throughout the lifetime of the project. These deliverables shall be named using the following terminology:

- Project Outputs and KPIs M12 (Y1)
- Project Outputs and KPIs M24 (Y2)
- Project Outputs and KPIs M36 (Y3)
- Etc., as applicable to the project duration.

The dissemination level of Project Outputs and KPIs deliverables shall be set to **SEN (Sensitive)**.

Applicants should carefully consult the Proposal Template when preparing the list of deliverables, as it contains additional guidance and requirements regarding their structure, content and timing.

KPIs

KPIs should be measurable, verifiable and proportionate to the scale and scope of the proposed action. They should allow the assessment of both implementation progress and the achievement of results.

All proposals shall report against the following Digital Europe Programme cybersecurity indicators, where applicable:

- **Number of cybersecurity infrastructures/services/tools your organisation has deployed as part of the project**
  - Definitions:
    - *Infrastructures:* Research or experimentation infrastructure such as a testbed, cyber range, or computing/communication facility. This may be data and/or software-based only or may include physical facilities.
    - *Tools:* A physical device and/or software/algorithm used to increase the security of ICT systems.
    - *Services:* The provision of expertise to help organisations deploy, manage, optimise, or access cybersecurity capabilities.

Applicants must report the total number of cybersecurity infrastructures, tools and services deployed as part of the project and provide a breakdown by category, as follows:

Total number deployed, out of which:

- Infrastructures:
- Tools:
- Services:

Each item must be reported under the category that best reflects its principal nature and must not be counted more than once under this indicator. Applicants should briefly identify the infrastructures, tools and services included in the reported figures. The examples below are illustrative and non-exhaustive:

- **CYBERAI**: AI-enabled cybersecurity experimentation environment may be reported as an infrastructure; AI-powered threat or vulnerability detection software as a tool; AI-supported cyber threat intelligence as a service;

- **AI4SME:** shared environment through which SMEs access and test AI-powered cybersecurity solutions may be reported as an infrastructure; AI-powered SME cyber-risk assessment toolkit as a tool; managed incident-support or risk-assessment for SMEs as a service.

- **COORDPREP:** cyber range or testing facility used for preparedness activities may be reported as an infrastructure; vulnerability scanning or risk-monitoring application as a tool; penetration testing; threat-assessment or preparedness-testing as a service.

- **REGCABH:** technical environment established or upgraded for the operation of a Regional Cable Hub may be reported as an infrastructure; automated threat-detection or situational-awareness applications as a tool; cyber-threat intelligence, monitoring or incident-reporting services supporting undersea cable protection as a service.

- **NCC:** cybersecurity platform made available to the national cybersecurity community may be reported as an infrastructure; software supporting early threat detection or community management as a tool; technical assistance or cybersecurity support provided to stakeholders, including SMEs, as a service.

- **EULEG:** platform supporting cybersecurity certification, conformity assessment or incident reporting may be reported as an infrastructure; compliance self-assessment or vulnerability-reporting application as a tool; certification conformity-assessment or legislative implementation support as a service;

- **DUALUSE**: cyber range or operational environment serving both civilian and defence cybersecurity use cases may be reported as an infrastructure; a quantum-safe cryptography, Zero Trust, AI-driven threat detection or SOAR solution as a tool; joint civilian-defence threat-monitoring or secure information-sharing as a service

Applicants must classify their outputs according to the definitions above and the actual nature of the proposed activities. The reported figures must cover only infrastructures/services/tools deploy as part of the project.

- **Number of users and user communities getting access to cybersecurity facilities including cybersecurity infrastructures service and/or tools.**

- **Number of entities supported in strengthening preparedness for and response to major cybersecurity incidents.**

- **Number of communication and dissemination, knowledge-sharing, capacity-building and awareness-raising outputs and activities implemented to promote the project and its results, reported by type, such as conferences, workshops, information days, training activities, best-practice exchanges, technical workshops, webinars, publications, newsletters, etc.**

Where one of the above indicators is not applicable to the proposed action, applicants shall indicate this clearly and provide a justification.

Applicants must provide, where applicable, baseline values, target values, units of measurement, measurement methods, data sources, reporting frequency, responsible entities and supporting evidence.

Applicants shall present their KPIs using a structured table, such as the template below:

Table 1 KPI Template

I D	Name	Description	Linked activity/outcome/ deliverable	Baseline	Target	Unit	Measurement method	Data source	Responsible Entity	Means of verification

The fields in the KPI table should be completed as follows:

- **ID**: A unique identifier for the KPI.
- **Name**: A concise name describing the indicator.
- **Description**: A clear explanation of what is being measured and why it is relevant to the action.
- **Linked activity / outcome / deliverable:** The activity, expected outcome or deliverable to which the KPI relates.
- **Baseline**: The starting point against which progress will be measured. Where applicable, baseline values should be based on scientifically sound, evidence-based or otherwise robust and verifiable data sources. If no baseline exists or a baseline is not applicable, applicants shall provide a clear justification.
- **Target**: The expected value or result to be achieved by a specified point in time, normally be the end of the project or by an identified milestone. Targets should be realistic, measurable and aligned with the action's objectives. Where a target value is not applicable, applicants shall provide a clear justification.
- **Unit**: The unit of measurement used for the KPI (e.g., number, percentage, users, organisations reached).
- **Measurement method**: The methodology, calculation approach or assessment process used to determine the KPI value.
- **Data source**: The source of the information used to measure and verify the KPI.
- **Responsible entity:** The beneficiary, partner or other entity responsible for collecting, monitoring and reporting the KPI.
- **Means of verification**: The documentation, records, datasets, reports or other means that will be used to verify the reported KPI values.

KPIs may be quantitative or qualitative, provided that they are objectively verifiable. Quantitative KPIs should use clear units of measurement, while qualitative KPIs should be supported by transparent assessment criteria and verifiable evidence. Where applicable, KPI baselines and targets should be supported by scientifically proven,

evidence-based or otherwise robust methodologies and data sources. Applicants may include additional KPIs beyond the indicators listed under each topic, provided that they are duly justified and relevant to the proposed action.

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI – Cybersecure tools, technologies and services relying on AI

Objectives

This topic addresses AI-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies and private entities from the NIS 2 directive, NCCs[4], etc. They play a key role in providing central operational capacity to European cybersecurity ecosystems. They may also provide primary input data for AI/ML-based cybersecurity tools and solutions, which can strengthen such authorities' capacity to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats. In particular, the adoption of generative AI[5] could be a challenge and an opportunity for cybersecurity[6] processes and applications.

These enabling technologies should allow for more effective creation and analysis of Cyber Threat Intelligence (CTI), automation of large-scale processes, as well as faster and scalable processing of CTI and identification of patterns that allow for rapid detection and decision making.

The security of AI itself, especially for the systems in the learning phase, also needs to be addressed, including the misuse of AI by malicious actors. This includes carrying out risk assessments and mitigation of cybersecurity risks inherent to AI technologies, implementing supply chain security, etc., and complying with the AI Act, intellectual property legislation and the GDPR.

In addition to being secure, the AI technologies being developed should perform well, and be robust and trustworthy. In particular, having trustworthy AI solutions will help in the deployment phase, where social acceptance is essential.

Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity[7], based on AI technologies[8], addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. These activities must also comply with intellectual property rights (IPR) and the GDPR, depending on the type of information handled. The AI solutions proposed should also be cybersecure.

Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that can potentially indicate emerging threats, recognising new attack vectors and

[4] If applicable and in line with individual national strategies.
[5] Cybersecurity in the age of generative AI, September 2023, available at: https://www.mckinsey.com/featured insights/themes/cybersecurity-in-the-age-of-generative-ai
[6] The Need For AI-Powered Cybersecurity to Tackle AI-Driven Cyberattacks, April 2024, available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered cybersecurity-to-tackle-ai-driven-cyberattacks
[7] Multilayer Framework for Good Cybersecurity Practices for AI, ENISA, June 2023, available at: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai
[8] Cybersecurity of AI and Standardisation, ENISA, March 2023, available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

enabling advanced detection in an evolving threat landscape, including in ICT or in Operational Technology infrastructures using open technologies.
- Creation of CTI based on novel threat detection capabilities.
- Enhancing speed of incident response through real-time monitoring of networks to identify security incidents and generating alerts or triggering automated responses.
- Mitigating malware threats by analysing code behaviour, network traffic, and file characteristics, reducing the window of opportunity for attackers to exploit malware.
- Identification of vulnerabilities and support for management considering multiple sources of information.
- Cybersecure tools and solutions that provide risk-reduction in the crossover between AI, IoT and smart grids or other manufacturing chains.
- Support for recovery from incidents through self-healing capacities.
- Reducing the chances of attacks and pre-emptively identifying weaknesses through automated vulnerability scanning and penetration testing.
- Protecting business sensitive data through the analysis of access patterns and detection of abnormal behaviour.
- Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymisation.
- Tools and solutions that provide product security or cybersecurity by design/default in line with CRA requirements.
- Tool and service providers are welcome to apply for this topic, also when in a consortium with Cyber Hubs. Links with stakeholders in the area of High-Performance Computing should be made where appropriate, as well as activities to foster networking with such stakeholders. In well justified cases, access requests to the EuroHPC high-performance computing infrastructure could be granted.
- The systems, tools and services developed under this topic will be made available for licensing to National and/or Cross-Border Cyber Hubs platforms, CSIRTs, competent authorities, and other relevant authorities under favourable market conditions.
- These actions aim at providing AI-powered cybersecurity capabilities for National and/or Cross-Border Cyber Hubs and for national authorities encompassing Cyber Hubs, CSIRTs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. These entities are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of their crucial operative role in ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, Cyber Hubs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.
- Tools to protect and secure AI solutions in line with the EU legislative framework and considering integration of requirements for robustness, performance, trust and balanced AI autonomy.
- Contribute to the cybersecurity certification of AI-driven cybersecurity solutions and systems. The primary objective of cybersecurity certification for AI systems within the EU is twofold: to mitigate cybersecurity risks inherent in AI technologies and to demonstrate compliance with the EU's comprehensive legislative framework, including the AI Act. By establishing a standardised, transparent, and rigorous certification process, the EU seeks to foster trust in AI technologies among users, developers, and regulators alike.

Expected Outcome

- Deployment of Artificial Intelligence and various AI-powered technologies as enablers for Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Novel cybersecurity tools based on AI that have been developed, tested and validated in relevant conditions and made available to Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Enhanced information sharing and collaboration amongst National and Cross-Border Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others relevant stakeholders, supported by CTI produced by AI-powered tools.
- Tools for automation of cybersecurity processes such as the creation, analysis and processing of CTI, to enhance operations of the Cyber Hubs.
- Original European CTI feeds or services.
- Ensure that the most advanced and innovative secure AI solutions are developed and implemented for NIS sectors.
- Secure AI solutions and tools, complying with EU legislation. Promote the mitigation of risks associated with the misuse of AI by malicious actors, with a focus on AI ethics and secure deployment.
- Contribution to the standardisation and certification of cybersecure, trustworthy AI technologies.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.

- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of entities benefitting from the development, testing, validation, deployment or uptake of AI-powered cybersecurity technologies, tools, and services.
- Number of AI-powered cybersecurity technologies and capabilities provided for National and/or Cross-Border Cyber Hubs and for national authorities encompassing Cyber Hubs and CSIRTs.

Topic optional KPIs

- Number of AI services and enabling technologies deployed for rapid detection of cybersecurity incidents and more effective decision making.

- Number of tools for automated threat detection and incident response.
- Number of cybersecure tools and solutions that provide risk-reduction in the crossover between AI, IoT and smart grids or other manufacturing chains.
- Number of original Cyber Threat Information (CTI) feeds created and deployed in operational environment.
- Number of tools and solutions that provide product security or cybersecurity by design/default in line with CRA requirements. Number of tools to protect and secure AI solutions in line with the EU legislative framework.

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

Technology providers, operators of Cyber Hubs, Research and academia, cybersecurity entities, public sector, NIS 2 Directive entities, private sector, Other relevant stakeholders supporting the deployment of cyber-secure AI solutions.

Type of action and funding rate

Simple Grants — 50% funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply *(see sections 6 and 10 and Annex 2)*
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME – Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions

Objectives

To support the market uptake and dissemination of innovative AI-powered cybersecurity solutions (notably in SMEs, possibly using results stemming from Horizon Europe projects or similar) and improve knowledge and auditing of cybersecurity preparedness.

SMEs often lack the resources to assess cyber risks, develop cybersecurity strategies and implement solutions, leaving them vulnerable to cyberattacks. The resilience of organisations that fall into this category is key to the prosperity of the EU single market.

Cyber risk assessment and management can be significantly enhanced and simplified with the application of AI-based tools and solutions. However, this requires an understanding of the evolving technology landscape, of the benefits of technology integration and of deployment prioritisation. Faced with organisational and financial constraints, the SMEs may be missing the opportunity to fully harness AI-powered solutions to advance their cybersecurity and resilience.

Cybersecurity is the precondition for reliable, secure and resilient AI models and algorithms. Cybersecurity of AI is not just about protecting AI systems against threats such as poisoning and evasion attacks, as it also involves ensuring they have trustworthiness features such as human oversight and robustness – the ability to resist cyberattacks, as required by the EU's AI Act for high-risk AI systems. The need for human oversight of AI has also been emphasised by experts. Also, the use of AI at the SME level supporting the integration of predictive algorithms can greatly support to a bottom-up approach when dealing with vulnerability detections, threat mitigation and more efficient coordinated incident response.

Scope

This action aims to increase the maturity of cyber risk management and improve the cyber resilience and ultimately foster a technologically advanced culture of cybersecurity for SMEs in the EU. Actions in this topic should develop and deploy AI-powered products, tools and services for European SMEs, also enabling the detection/discovery of attack patterns.

Proposals should cover the development or adaptation of the software/hardware and the validation of the solutions.

It foresees the automation of fundamental cybersecurity processes, in particular in small market organisations, through a SaaS toolkit tailored to the needs of SMEs. This toolkit should allow SMEs to improve the key aspects of their cybersecurity by providing user-friendly tools for risk management[9], threat detection, incident response and notification, to improve their cyber hygiene and mitigate potential threats while protecting personal data. The cyber toolkit should also provide cyber-incident prediction and response functions to improve SMEs' resilience.

Activities should include at least one of the following:

- Uptake/adoption of AI-powered cybersecurity tools in organisations where this has not yet taken place.
- Development of user-friendly sets of tools (e.g. toolkit) based on AI to automate main cybersecurity processes in SMEs. Such a toolkit could provide automated functions such as:
  - A function that supports the assessment and management of an SME's cybersecurity risks. This function should perform a risk assessment, provide recommendations for risk mitigation, and identify options.
  - An interface to existing tools that support the analysis and assessment of the extent of an SME's cyber risk based on information gathered from digital infrastructure scanning and data provided by authorised users.

[9] Interoperable EU Risk Management Framework, ENISA, 2023, available at: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

  - A function that issues alerts on relevant vulnerabilities and threats based on the information collected by the risk management function.
  - A function that connects SMEs to a Cyber Hub to report an incident and assist with recovery if possible.
- SME user interface for incident reporting associated with the cyber toolkit. Users can report an incident, get instructions on how to react and obtain information on how to obtain support for the response, with the use of AI assistants.

Expected Outcome

- Support the adoption of market-ready innovative AI-powered cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date AI-powered tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.
- Integrate AI technologies into cybersecurity processes to improve the security of ICT solutions, including providing innovative approaches to training employees to use AI solutions for cybersecurity.
- Deployment of cybersecure tools and technologies relying on trustworthy AI; AI-driven cybersecurity tools; Integration of tools to protect and secure AI solutions.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.

- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of entities benefitting from project activities, in particular SMEs.

- Number of AI-powered cybersecurity infrastructures, tools and services developed, adapted, tested and validated for use by SMEs, such as AI-powered cyber-risk assessment and management tools, digital infrastructure scanning tools, vulnerability and threat alerting tools, cyber-incident prediction and response tools, incident-reporting interfaces, AI assistants providing incident-response guidance, and SaaS-based cybersecurity toolkits tailored to SMEs.

Topic optional KPIs

- Number of innovative tools and services that support SMEs in reporting incidents, assisting with recovery and exchanging information with competent authorities.
- Number of AI-powered solutions or functions supporting cyber incident prediction, incident response or incident notification for SMEs.
- Number of training, awareness-raising or onboarding activities delivered to SMEs for the use of AI powered cybersecurity solutions

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

SMEs, start-ups, research and academia public sector, NIS 2 Directive entities, Other industry actors and related stakeholders (including providers of AI-assisted functionalities)

Type of action and funding rate

SME Support Actions — 50% and 75% (for SMEs) funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP – Coordinated preparedness testing and other preparedness actions

This action covers two actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism, and the support to the Member States namely through (1) coordinated preparedness testing of entities operating in sectors of high criticality across the Union, selected in advance according to Article 12 (4) of the Cyber Solidarity Act and (2) other preparedness actions for entities operating in sectors of high criticality and other critical sectors according to Article 13 of the Cyber Solidarity Act.

Objectives

These actions aim to complement and not duplicate **efforts by the Member States** and those at Union level to increase the level of protection and resilience to cyber threats, in particular for critical industrial installations and infrastructures, by assisting Member States in their efforts to improve their preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving at least one of the following objectives:

- (part 1) Coordinated preparedness testing of entities operating in sectors of high criticality across the Union, selected in advance according to Article 12 (4) of the Cyber Solidarity Act (including penetration testing and threat assessment) considering ICT as well as Operational Technology/Industrial Control Systems.
- (part 2) Other preparedness actions for entities operating in sectors of high criticality and other critical sectors (i.e. vulnerability monitoring, exercises and training courses).

Scope

[Part 1 Coordinated preparedness testing]

In accordance with Article 12 (4) of the Cyber Solidarity Act, the Commission has identified three sectors eligible for supporting the Member States through grants for the purposes of Coordinated preparedness tasting:

1. The energy sector and in particular the electricity sub-sector;

2. The transport sector and in particular the rail and water (ports) sub-sectors;

3. The public administration sector.

Call for proposals submitted by Member States under Part 1 of this topic (Coordinated preparedness testing) must refer to a risk-scenario that was conducted by the NIS Cooperation Group for the purpose of this call (baseline, medium, high). A proposal by a Member State shall include at least the baseline risk scenario (i.e., low stress level). All of the developed scenarios for each of the identified sectors are included in Annex 3 of the present document.

The provision of preparedness support services shall include the activities listed below, for entities in the sector or sub-sector, identified by the Commission, in line with the selected risk scenario from Annex 3 and specified in the call for proposal document.

Support for testing for **potential vulnerabilities:**

- Development of penetration testing according to a scenario from Annex 3 (at least baseline).

- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.
- Support for the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g. energy sector, transport sector, etc.) or others affected by NIS 2 to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.
- Evaluation and/or testing of cybersecurity capabilities of MS entities and MS sectors (including capabilities to prevent, detect and respond to incidents and stress test of the entire sectors), evaluation and compliance activities aimed at increasing maturity, e.g. on the basis of established maturity models and/or relevant evaluation and compliance schemes.
- Evaluation and/or testing of cybersecurity capabilities of entities in scope (including for the evaluation and management of risks concerning the supply chain).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities as a result of the conducted risk scenario/s.

Support for **threat assessment and risk assessment, such as:**

- Threat Assessment process implementation and life cycle
- Customised risk scenarios analysis.

The support will target the competent authorities in the Member States, which play a central role in the implementation of the NIS 2 Directive, such as Computer Security Incident Response Teams (CSIRTs) and National Cybersecurity Authorities.

[Part 2 Other preparedness actions]

For the second part, in addition to the services already listed for Part 1 (support for testing for potential vulnerabilities and support for threat assessment and risk management), the provision of preparedness support services included below addresses entities operating in highly critical and other critical sectors of all the sectors referred to in Annex I and II of the NIS 2 Directive. Namely, those actions are aimed for entities in sectors not identified for coordinated preparedness testing pursuant to Article 12 of the Cyber Solidarity Act (Part 1). The actions are again aiming at supporting the preparedness efforts of the Member States and support shall be provided to the Member States in the form of grants as in Part 1.

Support for **threat assessment and risk assessment**:

- Supply chain risk management within the risk assessment services.
- Risk monitoring service:
  - Specific continuous risk monitoring such as attack surface monitoring, risk monitoring of assets and vulnerabilities.
- Support coordinated vulnerability disclosure and management:
  - Promote the adoption of national CVD Policies[10] and the EU Vulnerability Database.
  - Coordinate the disclosure of vulnerabilities and timely dissemination of security patches. Standardisation of the way information is shared between different stakeholders in the vulnerability handling process.

[10] Coordinated Vulnerability Disclosure Policies in the EU, ENISA, 2022, available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

  - CVD applications that manage multiple sources of vulnerability information using open standards or technologies. (e.g. researchers, vendors, CSIRTs).
  - Raise awareness on the adoption of vulnerability management best practices.
- Dedicated exercises and training courses:
  - Develop[11] comprehensive training programmes and workshops, including international ones, for cybersecurity professionals that will cover the latest trends in cyber threats, attack methodologies, and best practices for pre-threat management and prevention. Maturity checks, evaluation of cybersecurity capabilities.
  - Encourage the development of cybersecurity continuous learning activities[12] to keep up with the cybersecurity requirements driven by EU cybersecurity-related regulations and directives, including the NIS 2 Directive, CSA, CSoA, DORA, EECC, GDPR, CRA.

The support aims to complement the efforts of the national competent authorities in the Member States, which play a central role in the implementation of the NIS 2 Directive, Computer Security Incident Response Teams (CSIRTs) including national sectorial CSIRTs, national Security Operation Centres (SOC)/Cyber Hubs

The COORDPREP topic covers two categories of actions under the Cybersecurity Emergency Mechanism:

- **Part 1** – Coordinated preparedness testing of entities operating in sectors of high criticality across the Union, selected in advance according to Article 12 (4) of the Cyber Solidarity Act; and
- **Part 2** – Other preparedness actions for entities operating in sectors of high criticality and other critical sectors according to Article 13 of the Cyber Solidarity Act.

The Cyber Solidarity Act provides that coordinated preparedness testing (Part 1) should be conducted using common risk scenarios and methodologies developed by the NIS Cooperation Group, in cooperation with the Commission, the European External Action Service (EEAS), The European Union Agency for Cybersecurity (ENISA), and within the remit of its mandate, the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe).

Risk scenarios are a key component for engaging in coordinated preparedness testing activities. Building on risks and vulnerabilities previously identified in sectoral, national and/or Union-level risk assessments, risk scenarios support and guide coordinated preparedness testing providing "what-if" situations where the effects of risks materialising are measured. Risk scenario development typically incorporates features such as severity, likelihood, and escalation levels over a baseline. Aggravation levels are key to realistically assessing resilience under increasing pressure. A gradual aggravation of severity can be delivered either by scaling the impact of a single scenario or layering either multiple sub-scenarios or attack vectors together for each variation.

The proposed risk scenarios for this call cover the following critical sectors and sub-sectors:

- The **energy sector** and in particular the **electricity** sub-sector;
- The **transport sector** and in particular the **rail** and **water (ports)** sub-sectors;

[11] Based on the European Cybersecurity Skills Framework (ECSF)
[12] Based on ECSF: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

- The **public administration sector**.

The risk scenarios are detailed in Annex 3. They adopt a multi-layer approach using a baseline scenario with a low stress level and two additional scenarios with medium and high stress levels, each compounding on the previous one. Annex 3 also proposes a methodology that could be used for coordinated preparedness testing in the relevant sectors and sub-sectors. The methodology could differ between sectors and sub-sectors and may be adapted to the applicable national context and needs.

Each applicant may choose among the proposed risk scenarios for the relevant sector or sub-sector to be used for the national action and included in the proposal. Each applicant may choose among the proposed risk scenarios what they would use for the national action (included in the proposal). However, the proposals must include at least one baseline scenario (which is the first one for each three sub-sectors in annex 3). Applicants may adapt the scenarios and include elements based on their national context, on top of the general EU-wide risk scenarios. Member State may choose to include higher intensity scenarios proposed in Annex 3.

For the national action, applicants:

- Are encouraged to explore systemic risks by covering supply-chain and interdependency-related issues;
- May expand the proposed risk scenarios to reflect the cumulative effects of multiple, possibly smaller, incidents occurring simultaneously within a defined timeframe, including incidents affecting individual organisations and supply-chain disruptions;
- Are encouraged to balance the focus across different types of incidents, including system failures, human error, malicious acts and natural phenomena, or combinations thereof;
- May refine the risk scenarios based on the specific national context and the needs and maturity levels of the selected sectors or sub-sectors.

A. Systemic Risk Analysis Phase

In this phase, applicants should undertake the planning and preparation of the coordinated preparedness testing activities, including:

- Identifying key stakeholders;
- Defining the scope and the primary and secondary objectives of the activities;
- Selecting the type of test evaluation;
- Designing the test structure
- Refining the risk scenarios based on specific needs;
- Conducting pilot tests to ensure reliability and validity

B. Testing Phase

In this phase, the coordinated preparedness testing takes place. Testing may take the form of:

- Vulnerability scanning;
- Security audits;
- Penetration testing;
- Exercises;
- Cyber resilience stress tests;

C. Gap Analysis Phase

In this phase, the results of the coordinated preparedness testing are converted into actionable follow-up measures, including:

- Identifying gaps and areas for improvement;
- Developing recommendations;
- Defining an action plan;

The results of the coordinated preparedness testing should be integrated into the remediation plan of the tested entity and should be sent to the relevant Member State authority for review. Lessons learned should be shared with the Commission in anonymised and aggregated form. A follow-up discussion may take place in the relevant workstreams of the NIS Cooperation Group.

Expected Outcomes

The types of deliverables are presented in two parts.

The first part covers:

- Enhanced cooperation, preparedness and cybersecurity resilience in the EU; preparedness support services;
- Threat assessment and risk assessment services.

The second part covers:

- Risk monitoring services;
- Better compliance, coordinated vulnerability disclosure and monitoring;
- Improved skills, via exercises and training courses, organisation of events, workshops. Stakeholder consultations and white papers.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.

- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of essential and important entities supported through coordinated preparedness testing or other preparedness actions.

Topic optional KPIs

The indicative KPIs below relate to the activities covered under both parts of this topic. Applicants should select and report the KPIs relevant to the part or parts addressed by their proposal.

- Number of penetration tests provided
- Number of essential and important entities supported
- Number of threat assessments / risk scenario analyses carried out
- Number of risk monitoring services provided
- Number and nature of vulnerabilities discovered
- Number of cross-border actions/exercises

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

For coordinated preparedness [Part 1] testing:

The action is targeted at public bodies that have been designated or entrusted by the relevant Member State with responsibilities in the area of cybersecurity, including cybersecurity competent authorities and CSIRTs designated under NIS2 Directive. Other relevant public or private partners may also participate in the consortium to support the implementation of the preparedness activities.

For other preparedness [Part 2] actions:

The action is targeted at public bodies that have been designated or entrusted by the relevant Member State with responsibilities in the area of cybersecurity, including cybersecurity competent authorities and CSIRTs designated under NIS 2 Directive.

Other relevant public or private partners may also participate in the consortium to support the implementation of the preparedness activities.

Type of action and funding rate

Simple Grants — 50% funding rate

 For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11- REGCABH – Regional Cable Hubs

As part of the EU Action Plan on Cable Security, it was announced that the Commission, together with voluntary Member States, will work on Cable Integrated Surveillance Mechanisms per sea basin ('Regional Cable Hubs') to enhance the detection capacity against threats to undersea cables as they are critical infrastructure.

Taking into account the fact that these cables are covered by the scope of NIS2 Directive that follows an all-hazards approach, it is crucial to protect their physical environment from events such as malicious acts, including cuts as integral part of the cable cybersecurity measures.

Objectives

The objective is to support the progressive establishment of Regional Cable hubs, one per sea basins of the EU, whose role will be to concretely enhance threats detection and operational security around these strategic infrastructures.

This action is therefore aimed at supporting the set-up of processes, tools and services for detection and analysis of emerging threats, to establish a near real time situational awareness to protect the undersea cables. It includes the capacity to aggregate data and security information from all available sources (including established systems such as the Integrated Maritime System, or CISE, or National Cyber Hubs) and analyse them in an automated way. The action will support also the establishment of a reporting incident function and a procedure for information sharing between relevant national authorities.

Regional Cable Hubs should be established as cooperative cross-border structures. Each Hub should involve a consortium of authorities from at least two Member States concerned by the relevant sea basin, including competent public authorities such as ministries, agencies or other public entities responsible for cable security, maritime security, resilience, or the protection of critical infrastructure. The involvement of a larger number of Member States is preferable. Other relevant public or private partners may also participate in the consortium to support the Hub's technical and operational implementation.

Additionally, structured partnership with private sector to enhance the voluntary information sharing for cable security as well as the potential and progressive integration of the relevant defence dimension capacities – in a dual use approach – could be considered in the action.

Should the participating Member States so decide, the regional cable hubs could coordinate the deployment and activation of modular repair equipment across a sea basin. Finally, the scope could also cover the acquisition of additional capacities, equipment, tools, instruments or services useful for the enhancing the resilience and security of undersea cables.

Expected Outcomes

The Regional cable hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection, supporting the development of an operational capacities to ensure the security and resilience of undersea cables.

The hubs should act as a central point allowing for broader pooling of data and information relevant for the security environment of the cables, enabling the dissemination of threat information and incident detection on a regional scale and among a diverse set of national actors as designated by each Member States (e.g. National Hubs, CSIRTs.)

The Hubs should allow a rapid exchange of information, even if classified among participating authorities in a given hub. To that end, the participating authorities shall set procedural arrangements on cooperation and information sharing.

Furthermore, regional cable hubs could also benefit from additional solutions for the surveillance and protection of submarine cables, and the detection of malicious activities. For instance, situational awareness performed through the collection and analysis of in-situ, sea-based sensor data as well as relevant satellite imagery or undersea drones capacities.

The Hubs could make use of existing systems which were not developed necessarily for Cable Security, such as the Integrated Maritime Systems, the Common Information Sharing Environment (CISE), the EU Copernicus Space Programme, and the Maritime Surveillance System. (MARSUR).

The Hubs should also integrate direct cooperation with private entities, especially cable operators to increase access – in a highly secured framework - to information on ongoing and future threats and voluntary incident reporting.

The Hubs should progressively also integrate the defence dimension, as any defence capacities is likely to increase the situational awareness as well as the capacity to respond fast in case of incident against these strategic critical infrastructures. To that end, Member States can integrate in the operations of the Hubs their defence capacities (e.g. navy or surveillance system) and operational command while building on international partnerships.

To support the above activities of a Regional Cable Hub, a grant will be available to cover, among others, the preparatory activities for setting up the Regional Cable Hub, its interaction and cooperation between its members and with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Regional Cable Hub. The grant could also be used to cover the acquisition of the infrastructures, tools and services needed to build-up the Regional Cable Hub but also to equip it with the necessary capacities to enhance the security and resilience of undersea cables, such as detection capacities.

These actions aim at creating or strengthening Regional Cable Hubs, which occupy a central role in ensuring the Security and resilience of strategic and critical infrastructures, providers of essential services such as global connectivity and power supply. As previously noted, Regional Cable Hubs will have a crucial operative role in ensuring the security of undersea cables in the Union and will handle sensitive information.

Actions may address:

a) the establishment of new Regional Cable Hubs.

b) the expansion to new Member States of existing Regional Cable Hubs projects funded under previous calls of this Topic.

c) the capability upgrade (extension of scope (e.g. defence aspect), application of new technologies enabling more predictive, automated, interoperable and operationally actionable situational awareness).

Pursuant to Article 12 of Regulation (EU) 2021/694, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.
- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of cybersecurity infrastructure, tools, and services developed or acquired to establish, operate, or upgrade the Regional Cable Hub and enhance the security and resilience of undersea cables.
- Number of processes established and implemented for threat detection and analysis, incident reporting and information sharing between relevant authorities for the protection of undersea cables.

Topic optional KPIs

- Number of solutions for the surveillance and protection of submarine cables and the detection of malicious activities.
- Number of active collaborations to increase access to information on cyber threats and voluntary incident reporting.
- Number of cyberthreat intelligence and situational awareness services developed.
- Number of tools for automated threat detection and incident response.

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

Competent public authorities from at least two Member States concerned by the relevant sea basin. Other relevant public or private entities may join where necessary for implementation.

Proposals may include the **expansion of existing Regional Cable Hubs projects funded under previous calls** of this topic to additional Member States.

Type of action and funding rate

Simple Grants — 70% funding rate co-funding

The funding rate of this action is exceptionally increased due to the geopolitical importance of the activities funded under this topic.

 For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6)
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC – Enhancing the NCC Network

Objectives

The National Coordination Centres (NCCs) set up by the Regulation (EU) 2021/887 are designed to work together through a network and to contribute to achieving the objectives of the regulation and to foster the Cybersecurity Competence Community in each Member State, by contributing to the acquisition of the necessary capacity. National Coordination Centres can also support priority areas such as the implementation of EU legislation (Directive (EU) 2022/2555, the proposed Cyber Resilience Act and the Cybersecurity Act).

The objective of this topic is to support the operation of the NCCs and to enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities. This could also be achieved by using Financial Support for Third Parties (FSTPs)[13]. Based on the financing received in previous years and on the different operational start dates in the Member States, this activity aims to continue providing support for NCCs.

In this regard, it is important to stress that individual NCC can choose from the list of activities and deliverables included in this topic depending on their interest and mandate. There is no obligation for NCCs to execute all actions.

This topic also considers providing support for the uptake of EU cybersecurity technologies and products, commercialisation and scale-up of the European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European and ongoing national and regional initiatives, such as accelerator and incubation programmes and technology transfer programmes. Such a strategy should also include support for scale-ups, considering the use of public procurement and private investment.

An essential aspect of this action is to create a framework for the emergence of such incubators and accelerators in the Member States, based on best practices and considering the specific needs and requirements arising from EU legislation (such as the Cyber Resilience Act, NIS 2 Directive).

In addition, this topic could contribute to cybersecurity awareness. It is becoming increasingly important to inform and educate EU citizens on cybersecurity topics in their daily use of digital technologies. Cybersecurity awareness helps individuals and organisations to identify threats and take appropriate action. By promoting awareness, the likelihood of incidents and data breaches can be reduced. Within this topic, NCCs are encouraged to build upon ongoing initiatives, including for example the ones from the EC and ENISA, to improve the awareness of EU citizens, businesses and organisations about cybersecurity risks and threats and to support Europe-wide actions to increase the number of students in cybersecurity courses, students engaged in cybersecurity research activities and students and young professionals choosing a career in cybersecurity.

Furthermore, European companies are innovative and develop highly competitive products, but the still underdeveloped Digital Single Market confines most of these companies (especially SMEs and start-ups) to their home country. A platform that can open the European market for small and medium-sized enterprises would also act as a springboard into international markets. This platform will ensure the competitiveness of European cybersecurity solutions. As such, this topic could also support the EU market's growth in cybersecurity products and services by providing a platform on

[13] For the use of FSTPs, the GB will prepare a dedicated procedure before the launch of the call.

which European SMEs and start-ups can post their (market-ready) products and solutions and on which businesses, public authorities and private individuals can search for the best solution for their needs, regardless of the country.

Scope

The National Coordination Centre should carry out, depending on their decision, one or more of the following tasks:

- Acting as contact points at the national level for the Cybersecurity Competence Community to support the ECCC in achieving its objectives and missions.
- Providing expertise and actively contributing to the strategic tasks of the ECCC, taking into account relevant national and regional challenges for cybersecurity in different sectors and deliver tasks supporting the implementation of the Cyber skills Academy.
- Promoting, encouraging and facilitating the participation of civil society and industry, in particular start-ups and SMEs, academic and research communities and other actors at Member State level in cross-border projects and cybersecurity actions funded through all relevant Union programmes.
- Providing technical assistance to stakeholders by supporting stakeholders in their application phase for projects managed by the ECCC, and in full compliance with the rules of sound financial management, especially on conflicts of interests. This should be done in close coordination with the relevant NCPs set up by the Member States.
- Seeking to establish synergies with relevant activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of those policies stated in the national cybersecurity strategies. Where relevant, implementing specific actions for which grants have been awarded by the ECCC, including through the provision of financial support to third parties in accordance with Article 204 of the Financial Regulation under the conditions specified in the grant agreements concerned, in particular aimed at strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs).
- Supporting the scaling-up of start-ups by finding other funding to implement existing projects.
- Promoting and disseminating the relevant outcomes of the work of the Network and the ECCC at national, regional or local level.
- Assessing requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the NCC.
- Advocating and promoting involvement by relevant entities in the activities arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments and deployments.
- Supporting the Cybersecurity Competence Community registration (on platforms such as ATLAS) and contributing to the development of suitable community management tools.

In addition, this action aims to promote safer digital behaviours, grow talents and attract more youth to cybersecurity careers; the NCCs could also, depending on their national context, carry out one or more of the following tasks:

- Provide support to innovative ideas towards market-readiness.
- Promote cybersecurity awareness, best practices, and careers in schools, universities, and community events (for instance by launching a pan-European programme where young individuals will be trained as ambassadors to promote cybersecurity.)

- Strengthen collaboration between institutions for higher education, e.g. by jointly organising events, by teaching students and working together on cutting-edge research. Support activities in primary and secondary levels of education to increase cybersecurity awareness and hygiene, through educating the teachers and educators.
- Build stronger partnerships with established SMEs, tech companies, and government agencies to develop and distribute software tools and services that assist in early threat detection, actor identification, and threat evolution monitoring. These collaborations can ensure that cybersecurity professionals have access to the latest tools and technologies for effective threat management.
- In collaboration with other entities, as needed, organise periodic cybersecurity boot camps, challenges, awareness campaigns and training courses across Europe, specifically for SMEs or students (e.g. focusing on equipping participants with hands on skills to manage prevalent cyber threats through training sessions, workshops, and simulation activities tailored to their industry). Organise periodic awareness raising campaigns, at national and regional level, to increase cybersecurity awareness and hygiene aimed at different demographics. Organise national and regional cyber exercises to enhance the security and resilience of critical sectors as well as SMEs.
- Foster a community of cybersecurity professionals who can share their experiences, challenges, and solutions.
- Support and encourage the uptake of cybersecurity educational policy goals in national (cybersecurity) strategies.
- Promote safer digital behaviours and more youth considering cybersecurity careers.

The action could also aim to:

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect (e.g. network security, advanced two-factor or passwordless authentication) and respond to cybersecurity threats.

This topic targets exclusively National Coordination Centres which have been recognised by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. These actions aim at the operation of National Coordination Centres, which occupy a central role in the cybersecurity landscape as foreseen in Regulation (EU) 2021/887. Due to the synergetic role they play with regard to the activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of those policies stated in the national cybersecurity strategies, they must be able to handle sensitive information, and be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt undue foreign influence and control.

As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions are subject to Article 12(5) of the DEP Regulation (2021/694).

Expected Outcomes

Depending on the decision of each NCC, one or more of the following should be covered:

- Network of national initiatives to accelerate the cybersecurity industry and facilitate Access-to-Market.
- European frameworks for establishing cybersecurity incubators and accelerators.
- Cybersecurity Community Observatory to inform subsequent policy interventions by the ECCC and NCCs.
- Matchmaking events to create connections and build trust; platforms and events for Access-to-Finance and Access-to-Market including in the area of dual-use technologies.
- Strengthened Cybersecurity Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre; Maintained technical registration possibilities for candidates for the Cybersecurity Competence Community; Technical assistance for potential applicants for ECCC calls.
- Uptake of cybersecurity solutions.
- Strengthened cybersecurity capacities of stakeholders.
- Synergetic activities that strengthen the role of NCC.
- Centralised the many initiatives focusing on raising awareness and work together with other NCCs to support a cross European approach covering education, studies, training courses and awareness campaigns[14]; Share and provide best practices related to the awareness topic.
- Support the transfer of best practices related to cybersecurity teaching for primary and secondary school and other activities for children and youngsters (including camps, materials, games, etc.).
- Support for teachers and professors to have access to best practices available in the EU and facilitate dialogue.
- Support the development of cross-over educational solutions for SMEs, for example by gamification.
- Cyber campaign material focused on young professionals and students of all ages and gender to pursue and advance in cybersecurity careers, where the NCCs can build on in view of regional differences.
- Cyber campaign material focused on parents and teachers of future students of all ages and gender to raise the number of cybersecurity students.
- Platform supporting a network of young cybersecurity ambassadors spreading awareness and fostering a culture of cybersecurity among Europe's youth.
- Common services to be provided within national cyber campuses.
- Hybrid events for the cybersecurity competence community to increase awareness of cybersecurity threats, threat actor modus operandi and potential impact, potentially in collaboration with existing initiatives and platforms.
- Deliverables supporting the implementation of the Cyber skills Academy.
- Support for activities dedicated to the EU Cybersecurity Challenges.

In addition, activities could cover setting up a platform integrating all other existing platforms, hosted and maintained at the European level under the .eu domain, so as to:

- Establish and maintain a marketplace for cybersecurity products and services.
- Allow the retrieval of information on entities adhering to the 27 NCC communities.

[14] The activities should consider other ongoing projects, activities, campaigns as well as the mandate of ENISA and other EU or national bodies. These actions should ensure synergies at EU level and should not duplicate efforts at EU or national levels.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.
- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of entities supported through NCC project activities to uptake state-of-the-art cybersecurity solutions.
- Number of entities supported in the uptake and dissemination of state-of-the-art cybersecurity solutions and in strengthening their cybersecurity capacities, out of which SMEs
- Number of entities receiving financial support to third parties.

Topic optional KPIs

- Number of users and user communities getting access to EU cybersecurity facilities;
- Number of entities supported in strengthening preparedness for and response to major cybersecurity incidents;
- Number of registered candidates for the Cybersecurity Competence Community;
- Number of Matchmaking events organised and promotion of available funding opportunities;
- Number of events organised for the cybersecurity competence community to increase awareness of cybersecurity threats, threat actor modus operandi and potential impact, potentially in collaboration with existing initiatives and platforms;
- Number of interactions (requests of clarifications, questions or call/topic related questions, etc.) with the local Cybersecurity Competence Community for assistance to apply for funding opportunities;
- Number of actions to promote the expertise and achievements of the members of the cybersecurity community;
- Number of collaboration actions with other NCCs and with the ECCC;

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Financial support to third parties and Ownership Control Assessments (OCAs)

Where Financial Support to Third Parties (FSTP) is implemented under this topic, beneficiaries responsible for managing FSTP schemes must ensure that third-party recipients comply with the applicable eligibility, establishment, geographic location, ownership and control, and security restrictions set out in the call conditions and the grant agreement.

Beneficiaries implementing FSTP are invited to consult the EU services' guidance on participation in restricted calls with ownership and control restrictions[15] when preparing and implementing their OCA arrangements.

Beneficiaries implementing FSTP schemes shall ensure that adequate administrative, operational and technical arrangements are in place to perform ownership and control assessments (OCAs) of third-party recipients before the award of financial support and before the signature of any sub-grant agreement or equivalent arrangement with the selected recipient.

Operational Capacity for FSTP and OCA implementation

Applicants implementing FSTP must demonstrate, at proposal stage, that they possess operational capacity necessary to manage the FSTP scheme and to perform the required OCAs. This should be described in the relevant part of the application under Section 2 "Implementation", subsection 2.3 "Capacity to carry out the proposed work".

In accordance with the EU services' guidance on participation in restricted calls with ownership and control restrictions, applicants shall describe the measures and arrangements they will put in place throughout the lifecycle of the FSTP scheme. The description should cover, as appropriate, aspects such as governance, implementation, assessment, ownership and control verification, award procedures and record-keeping, and explain how these measures and arrangements ensure:

- Clear allocation of responsibilities for the design, management and supervision of the FSTP scheme;
- Sufficient human resources, expertise and administrative capacity to manage FSTP open calls and perform the required checks;
- Sufficient expertise and administrative capacity to assess eligibility, establishment, geographic location, ownership and control, and security-related requirements;
- Internal governance arrangements for preparing, reviewing and approving OCA conclusions;
- Transparent and documented procedures for launching and managing FSTP open calls, including application, evaluation, award and contracting arrangements;
- Procedures for collecting, checking and retaining declarations, supporting documents and other evidence required from FSTP applicants and recipients;
- Procedures for requesting clarification or additional supporting documents from FSTP applicants where needed;
- Safeguards to prevent and manage conflicts of interest throughout the FSTP selection and OCA process;
- Arrangements to ensure that OCA checks are completed before financial support is awarded and before the signature of any sub-grant agreement or equivalent arrangement;

[15] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/guidance-on-participation-in-eu-calls-with-ownership-and-control-restrictions_en.pdf

- Record-keeping and audit trail arrangements enabling the beneficiary to demonstrate how each OCA conclusion was reached;
- Access-to-file arrangements and cooperation with checks, reviews, audits or sample-based verification by the granting authority.

Ownership Control Assessment (OCA) Methodology

Applicants implementing FSTP must provide, at proposal stage, an appropriate OCA methodology. The methodology must be proportionate to the scale and nature of the FSTP scheme and sufficiently detailed to demonstrate that the beneficiary will be able to perform the required checks in a reliable, consistent, traceable and auditable manner.

In accordance with the EU services' guidance on participation in restricted calls with ownership and control restrictions, applicants shall describe the methodology and procedures they will apply to assess the ownership and control of Financial Support to Third Parties (FSTP) recipients. The methodology shall address, as appropriate, the following elements:

- The assessment workflow, from receipt of the FSTP application and supporting documents to the documented OCA conclusion;
- The written methodology, checklists or assessment template to be used;
- The declaration and supporting documents to be requested from FSTP applicants and recipients;
- The procedure for assessing direct and indirect ownership structures, including intermediate ownership layers and ultimate ownership;
- The procedure for assessing control relationships, including voting rights, veto rights, special rights and other rights affecting strategic decisions;
- The procedure for assessing de jure and de facto control;
- The procedure for assessing corporate governance arrangements, including board composition, appointment rights, quorum and majority rules;
- The procedure for assessing commercial links, financial links or other arrangements that may confer decisive influence;
- The decision-making process, including how OCA conclusions are reviewed, approved and linked to the award decision;
- Confidentiality, record retention, and audit-trail arrangements;

The FSTP open calls, application forms, evaluation procedures and sub-grant agreements or equivalent arrangements must include the applicable eligibility and security restrictions, including ownership and control requirements. They must also require FSTP applicants to provide the declarations and supporting documents necessary for the beneficiary to perform the required assessment.

OCA checks must be completed before financial support is awarded and before the signature of any sub-grant agreement or equivalent arrangement. Selected recipients must have a complete OCA file before signature. Where an FSTP applicant or recipient does not comply with the applicable restrictions, financial support must not be awarded or must not proceed.

The granting authority may request additional information during grant preparation and throughout project implementation in order to obtain reasonable assurance regarding the beneficiary’s capacity to perform these checks and the methodology followed. The granting authority may also request access to OCA files and perform checks, including on a sample basis, covering the application of the OCA methodology, the supporting documentation retained by the beneficiary and the consistency of the assessment

conclusions. Beneficiaries must therefore ensure that OCA conclusions are supported by complete, consistent, and auditable records.

Targeted stakeholders

This call targets National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and other private and other private and public entities in consortium with NCCs, including academia and research entities.

Type of action and funding rate

Simple Grants — 50% funding rate

The maximum EU funding rate for this topic is 50% of the total eligible costs of the action, **including any budget allocated to Financial Support to Third Parties (FSTP).**

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, following reimbursement option for equipment costs applies: depreciation only *(see section 10)*
- For this topic, financial support to third parties is allowed *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG – Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

Objectives

The objective of this topic is to support the European ecosystem to strengthen its cybersecurity capacities and to support the implementation of the regulatory framework in line with the Cyber Resilience Act (CRA), NIS 2 Directive, GDPR, DORA, Cybersecurity Act, specific requirements of the AI Act, etc. in a homogeneous approach. Additionally, and in alignment with the Digital education plan, which emphasises the development of digital skills crucial for the modern economy, and in support of initiatives like the Cybersecurity Skills Academy, activities related to cybersecurity challenges should also be promoted. These initiatives aim to address the skills shortage in cybersecurity and develop a workforce capable of meeting regulatory and operational demands. By providing practical training, attracting young professionals, and encouraging diversity

within the field, these efforts are vital to Europe's ability to respond to evolving cyber threats and to comply with new legislation. Additionally, these activities foster equal opportunities and raise cybersecurity awareness among future generations, contributing to Europe's broader strategic goals in the digital domain.

The implementation of EU cybersecurity legislation needs to be supported to achieve a higher level of cybersecurity in the EU, especially in a constantly changing threat landscape. Cybersecurity maturity levels are different depending on each sector. This means that efforts and investments are needed to ensure and continuously improve cyber security in both the public and private sectors. Such efforts and investments are crucial in each Member State and therefore require increased focus and joint efforts at European level. Empowerment and self-assessment tools can be the most effective.

All the above efforts should consider that data security and protection must be promoted during the design and development of ICT products and services.

Scope

EU cybersecurity legislation brings new responsibilities and imposes obligations on key stakeholders, ICT systems, Operational Technology and IoT manufacturers. For instance, the cost of obtaining a cybersecurity certification for an ICT or digital product, service or process is often an insuperable barrier for EU start-ups and SMEs.

Support must be provided for the implementation of these obligations. The activities under this action require various types of support, including financial and organisational. Applications should address at least one of the eligible pieces of cybersecurity legislation but can also address more.

The focus will also be on fostering cross-border collaboration and promoting diversity within the cybersecurity workforce, encouraging participation from women and other underrepresented groups. In conjunction with initiatives like the Cybersecurity Skills Academy, these activities will contribute to building capacity, raising awareness, and supporting the uptake of the aforementioned regulatory framework. By integrating these challenges into a broader capacity-building framework, they will ensure that stakeholders across sectors are equipped to address evolving cybersecurity threats and comply with the new legislative landscape.

Aligned with the goals of the Digital Education Action Plan which focuses on enhancing digital skills across Europe, activities related to cybersecurity challenges will play a crucial role in developing the next generation of cybersecurity professionals. These challenges will provide hands-on experience for young professionals and students, helping to close the cybersecurity skills gap and ensuring they are well-prepared to meet the demands of new legislative requirements.

The assessment of products and services is an essential step in the EU cybersecurity certification process. As cybersecurity threats are rapidly evolving and attacks are becoming more sophisticated, it is important to find a way to address these challenges. In addition, the EU needs to cope with the continuous growth of information systems (in terms of size and complexity) and the significant expansion of the digital space by enabling fast but secure replication of assessments. Furthermore, it is a great opportunity for the EU to develop interoperable solutions that will increase its competitiveness. In doing so, the Union can rely on a large and dynamic number of players who have already developed high-quality offerings.

The certification process is also very formal in terms of the documentation that is later used as proof for issuing the certificate. There is currently no platform to help proponents overcome the challenges posed by the use of many different and complex documents by all parties.

This action involves building capacity of national cybersecurity certification authorities to undertake market surveillance and supervise conformity assessment bodies and conformity assessments of essential requirements for cybersecurity products, services and processes. It should ensure the mutual recognition across Member States.

Furthermore, the action is also about building up capabilities of conformity assessment bodies and certification laboratories to meet the requirements of the Cyber Security Act and the Cyber Resilience Act, as regards verifying declarations of conformity from suppliers and vendors.

The action involves also the development of supporting tools for certification and evaluation processes, including a 'Certification and Evaluation as a Service' software platform to assist conformity assessment as well as support in creating national or cross-regional expert hubs to assist with these processes. Its development should involve relevant stakeholders such as CBs, CABs, and client representatives.

The 'Certification and Evaluation as a Service platform' could facilitate and streamline the management of all documentation used in the certification process. It could also help to speed up the information exchange between the bodies taking part in the process. The platform could help to harmonise and standardise the documentation and tools to be used across Europe.

The main areas considered under the scope of this action could include:

- The implementation of EU legislation in cybersecurity to be supported to achieve a higher cybersecurity level in Europe.
- Provide support to SMEs aiming to enhance cybersecurity resilience with a particular focus on legal requirements deriving from EU legislation such as NIS 2, Cyber Resilience Act, Cybersecurity Act, etc., including practical guidelines and user-friendly tools allowing the company to check whether its solutions are compliant with the requirements of the new legislation considering open standards.
- Develop reporting platforms for NIS 2 (e.g. incident reporting platform) and CRA (e.g. vulnerability single reporting platform).
- Establish short-term and long-term actions to prepare professionals to properly implement the requirements of new EU regulations in entities covered by those regulations.
- Develop programmes to promote diversity and equal opportunities for all young Europeans, providing tailored onboarding programmes for youth. These programmes will offer resources and easy access to educational content, ensuring that participants from various backgrounds can engage with cybersecurity training. By supporting non formal education and offering participation opportunities, such as cybersecurity challenges, these efforts will help equip the next generation with the skills needed to thrive in the sector.
- Creation and development of cooperation initiatives in cross-border and cross-sector contexts. Encourage collaboration between national and regional authorities to enhance cyber resilience and raise cybersecurity maturity levels through development and implementation of common methodologies.
- The design and evaluation of platforms for training programmes and tools for cross country exchange will support these efforts. Additionally, benchmarking and assessment programmes will help optimise performance, enhancing participants' skills. These initiatives, including training materials, with cybersecurity challenges as one example, will also include peer exchange and fellowship opportunities, fostering a connected community of cybersecurity professionals. By encouraging cross-border collaboration and ongoing engagement, these programmes aim to strengthen Europe's cybersecurity workforce and support long-term talent development.

- Support the development of cross-border collaboration programmes, enabling pan European teams to participate in international cybersecurity competitions, enhancing visibility and competitiveness on the global stage. These initiatives will provide teams with access to advanced tools, mentorship, and leadership training, fostering the growth of a European cybersecurity talent pipeline. By promoting excellence, skills development, and leadership, this support will ensure that Europe's top talent remains competitive, well-prepared, and collaborative in facing global cybersecurity challenges.

In addition to providing supports for national cybersecurity certification authorities, conformity assessment bodies and national accreditation bodies with certification, the implementation of the NIS 2 Directive will continue in the coming years. In particular, competent authorities will need to build up capacity in audit and compliance to ensure that essential and important entities are meeting their responsibilities. Training and awareness raising activities along with trust and confidence building activities to facilitate information sharing and knowledge building should be provided.

Overall, this action is intended to increase collaboration between national authorities, supporting or supplementing the structures under the NIS Directive that need to comply with CRA (e.g. Software Bill of Materials, CRA Single Reporting Platform contributions and open prototypes, CVD processes or security advisory automation, like the CSAF), as well as between national authorities and stakeholders, especially SMEs, to raise cybersecurity maturity levels through the development and implementation of common methodologies to enable the deployment of cybersecurity processes and the uptake of products and services by entities.

This action involves the creation and deployment of common tools for regulation and enforcement, including targeted security audits and incident notifications to national competent authorities to facilitate information exchange.

Under information exchange, the action can also include:

- At national level, federate national actors working on cyber threat intelligence and national competent authorities around a common platform. Including facilitating and centralising the notification process for NIS 2 entities.
- At vertical level within the EU, organise or support cyber threats intelligence (CTI) unclassified information sharing in confidence between stakeholders of the given vertical.
- At EU level, enabling and organising collaboration between countries and information sharing.
- Collaborate on and implement a framework of guidelines - in the EU or multiple EU MS - to ensure and continuously improve cybersecurity both within the public and private sectors through better protection of their data, a significant reduction of the risk of the most common cyberattacks, and an increase of cyber resilience in general.

In addition, this topic promotes security and privacy 'by design' in existing and emerging technologies, applications and hardware, including IoT, Operational Technology, Identity and e-government systems, by supporting and/or funding research and innovation opportunities. Privacy-enhancing technologies aim to minimise the risks to the privacy of data subjects. Implementing security and privacy features in emerging technologies, applications and hardware from the outset – in the design and implementation phase[16] – ensures that potential vulnerabilities and risks are recognised

[16] Data Protection Engineering, ENISA, 2022, available at: https://www.enisa.europa.eu/publications/data protection-engineering.

and addressed early in the development process. In addition, to be in line with data protection regulations, this approach can be more cost effective and would reduce the likelihood of security and personal data breaches.

Consortia should consider including at least one representative of each of the following categories to reflect the whole value chain: privacy-enhancing technology researchers, privacy-enhancing technology providers, developers of ICT products and services integrating privacy-enhancing technologies, and ICT product and services user organisations.

Expected Outcomes

One or more of the following should be covered:

- Implementation of guidelines, standardised processes, or manuals – in the EU or multiple EU MS – concerning the most challenging issues, supporting specific stakeholders and sectors addressed by cybersecurity legislation.
- Develop and implement tools, raise awareness and encourage and facilitate industry uptake, with a focus on SMEs, of conformity assessments of essential cybersecurity requirements for products with digital elements (hardware and software) under the CRA.
- Support for mechanisms reducing the administrative burden for entities, like single entry point for incident notification.
- Establish secure communication channels allowing for cooperation and information sharing initiatives.
- Support the organisation of regular meetings/workshops to identify good practices within specific sectors or emerging areas and facilitate collaborative efforts between different sectors.
- Support the development of training courses, on the basis of the ECSF and exercises that promote capacity building and internal awareness.
- **Contribution to CR standardisation:** Training materials and training actions on cybersecurity certification for national authorities and conformity assessment bodies.
- **Fostering certification:** Educational and supporting materials and an explanatory press campaign using interactive material such as 'Do I comply with CRA?'. Information campaign through various channels such as conferences, meetings, etc. Website dedicated to the mandatory certification and conformity assessments of essential requirements.
- Development of training programmes and materials, including tools for cross-country collaboration and exchange, aimed at enhancing participants' skills and readiness for real-world threats. These programmes can also support non-formal education for high school students and teachers, enhancing digital literacy and cybersecurity awareness at early educational levels.
- Creation of benchmarking and assessment programmes to evaluate and optimise the performance of participants in cybersecurity training programmes, ensuring continuous improvement and alignment with industry standards.
- Implement peer exchange and fellowship programmes, aimed at fostering a connected, resilient community of cybersecurity professionals across Europe. These programmes will also include support for cross-border training initiatives and non formal education activities, ensuring that both students and educators can participate in hands-on cybersecurity learning experiences and contribute to long-term talent development.
- Establishment of cross-border collaboration programmes to support the development of pan-European teams in cybersecurity competitions. These programmes will provide access to mentorship, advanced tools, and leadership training, ensuring European teams remain competitive on the global stage. Additionally, the programmes will foster the growth of a European cybersecurity

leadership pipeline, enhancing Europe's visibility and effectiveness in international cybersecurity challenges.
- Support organisations, including SMEs, in assessing the robustness, applicability and relevance of security- and privacy-enhancing technologies to be integrated in the ICT products and services they develop.
- Set-up pilot projects to test CRA compliance, use open-source software and libraries for conformity assessment and testing; develop assessment methodologies for the purpose of CRA compliance/requirements.
- Develop best practices or guidelines for setting-up and operating market surveillance authorities in MSs; develop awareness of CRA requirements.
- Support organisations, including SMEs, in commercialising privacy-enhancing technologies and demonstrate how they can address security and privacy risks from emerging technologies.
- Facilitate cooperation between the producers of emerging technologies, the users of those technologies and regulators. Such cooperation would make it possible to identify which requirements can be met by which privacy-enhancing technology, in which use cases, to what extent they could facilitate compliance or reduce the cost thereof, and how to engineer it in practice, during the early phases of design and development of ICT products and services.
- Strengthen cooperation in the whole privacy-enhancing technology value chain, including between researchers, providers, integrators and users, and GDPR national authorities/European supervisors.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.

- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of stakeholders supported in understanding, preparing for or implementing requirements under relevant EU cybersecurity legislation, out of which:
  - SMEs and start-ups;
  - competent authorities and CSIRTs;
  - market surveillance and notifying authorities;
  - national cybersecurity certification authorities;
  - conformity assessment bodies and certification laboratories;

- other entities subject to or supporting the implementation of relevant EU cybersecurity legislation.

Topic optional KPIs

- Number of technologies and IT-based solutions, processes and methods for handling cybersecurity incidents implemented, validated, piloted or deployed.
- Number of activities organised for collaboration, communication, awareness-raising, knowledge exchange or training on the implementation of EU cybersecurity legislation.
- Number of twinning schemes implemented between at least two Member States for effective cross-border collaboration in preventing, detecting and countering cybersecurity incidents.
- Number of tools and IT-based solutions, processes and methods for monitoring and handling exploited vulnerabilities in products with digital elements in the scope of the Cyber Resilience Act.
- Number of products or services made available that simplify and/or automate compliance with the Cyber Resilience Act.
- Number of SMEs using open-access or low-cost tools to support the implementation of the Cyber Resilience Act for public authorities and economic operators.
- Number of tools supporting market surveillance authorities and notifying authorities appointed under the Cyber Resilience Act in the implementation of their respective mandates.
- Number of communication, awareness-raising, knowledge exchange and training activities organised on the rules and requirements of the Cyber Resilience Act.
- Number of activities organised to promote the sharing of technical specifications, best practices and use cases among actors that have obligations under the Cyber Resilience Act.
- Uptake of Cyber Resilience Act-compliant products across sectors.
- Number of tools, processes or services supporting stakeholders in meeting requirements under the NIS2 Directive.
- Number of activities supporting cooperation between competent authorities, CSIRTs, SOCs, ISACs, essential and important entities, and other stakeholders concerned by EU cybersecurity legislation.
- Number of cybersecurity certification-related tools, processes, guidance materials or support activities made available to relevant stakeholders.
- Number of stakeholders supported in understanding, preparing for or implementing obligations under relevant EU cybersecurity legislation.

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

This topic targets all relevant stakeholders, including industrial stakeholders, SMEs and start-ups in the scope of the Cyber Resilience Act, stakeholders concerned by the NIS2 Directive, and stakeholders that may benefit from European cybersecurity certification schemes.

It also targets Member State competent authorities, Computer Security Incident Response Teams (CSIRTs), including sectoral CSIRTs, Security Operation Centres (SOCs), Operators of Essential Services (OES), digital service providers (DSPs), Information Sharing and Analysis Centres (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 relevant EU cybersecurity legislation.

Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.

Type of action and funding rate

Simple Grants — 50% funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, following reimbursement option for equipment costs applies: depreciation only (see section 10)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union
  - extent to which the proposal can overcome financial obstacles such as the lack of market finance
  - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE – Dual-use technologies

Objectives

Dual-use technologies have emerged as a cornerstone in addressing both cybersecurity threats and broader cyber defence needs. The integration of advanced civilian and military technologies under a unified framework is critical to bolstering resilience across critical infrastructure, ensuring data security. In addition, addressing cybercrime and hybrid threats will contribute to maintaining societal stability.

Cross fertilisation and spill-over effects from synergies between the civil and defence spheres have proven to be an important driver for innovation, industrial deployment and market uptake. Such effects should also be fostered for cybersecurity and cyber defence. The results could lead to increased resilience to cyber threats and better protection of both civilian and defence critical infrastructures.

Building on Digital Europe Programme, Horizon Europe, and the European Defence Fund, the EU must prioritise collaborative pilot projects. These projects results can bridge civilian and defence sectors, fostering innovations in relevant key technologies such as quantum-safe cryptography, Zero Trust Architectures (ZTA), and AI-driven

threat detection systems. Such efforts are essential to addressing emerging cyber threats while ensuring interoperability and scalability across sectors.

The objective is to enhance cooperation between the civil and defence spheres regarding dual use projects, services, competences and applications in cybersecurity in line with Article 6.1(f) of the DEP Regulation and Article 5.3(g) of the ECCC Regulation.

Scope

The objective is to enhance operational cooperation between the civil and defence spheres through the development of dual-use working prototypes, ready-to-market products and operational infrastructures related to cybersecurity technologies, applications and tools that have relevance in both civilian and defence context.

Examples of domains of interest for this call topic are:

- Quantum-Safe Cryptography: Develop encryption methods resistant to quantum computing attacks. These solutions will ensure secure communication and data protection for critical civilian and military infrastructures.
- Zero Trust Architectures (ZTA): Implement ZTA frameworks to enhance endpoint security and prevent unauthorised access to critical systems. These architectures can serve both civilian applications (e.g. healthcare, finance) and defence systems.
- AI-Driven Threat Detection and Response: Deploy advanced AI tools for real-time threat detection, mitigation and response. AI can be leveraged for anomaly detection in critical networks, adaptive defence mechanisms, and predictive risk assessments. AI-driven threat detection systems can enhance the ability of stakeholders, including law enforcement authorities, to analyse large datasets and identify patterns of malicious activity. These systems also enable real-time prioritisation of actionable intelligence and can support investigations across sectors. Ethical considerations, including compliance with the GDPR and AI Act, must guide their deployment.
- Cyber Ranges including Digital Twins for Cybersecurity: Use Cyber Ranges solutions and Digital Twin technology to simulate potential cyberattacks on civilian and military systems and networks. This enables proactive identification of vulnerabilities and the development of effective response strategies. This would enhance the capacities of a wide range of stakeholders, including Law Enforcement Authorities.
- Advanced SOAR Tools: Develop Security Orchestration, Automation, and Response (SOAR) platforms to streamline incident response across sectors.

Other cybersecurity domains where the civil and defence spheres have a common interest in developing working systems together will also fall within the scope of this call topic.

The above domains are expected to be demonstrated and deployed for (but not limited to):

- Critical Infrastructure Protection: For example, deploy dual-use AI-driven tools to monitor and secure critical infrastructures such as undersea critical infrastructure, transportation networks, communication networks, energy grids, and healthcare systems against cyber and physical threats and investigate incidents.
- Secure Communications: For example, utilise quantum-safe communication protocols to protect sensitive data exchanges between civilian and defence stakeholders.
- Hybrid Threat Management: For example, design systems capable of countering hybrid threats, such as GPS jamming and spoofing, cable sabotage, ransomware attacks combined with disinformation campaigns, ensuring operational continuity.

- Extension of SOC/CSIRT functionalities and operations that are compatible with military requirements. The defence community can benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure.
- Digital Fraud and Digital Violence Prevention for Public Safety: For example, dual-use technologies for the prevention of digital fraud, disinformation and identity theft through real-time monitoring and advanced digital forensics. These solutions can enhance the ability to collect and analyse digital evidence across jurisdictions, supporting victim protection and law enforcement efforts.

Upon request from the ECCC, project consortia will participate in clustering activities to define common actions and to enhance synergies between the civilian and defence communities.

Expected Outcomes

- Secure Data Sharing Framework: Develop standardised and encrypted communication mechanisms to facilitate seamless data exchange between civilian and military stakeholders. These mechanisms should align with GDPR and other EU regulatory requirements.
- Early Warning Systems (EWS): Establish a European-level EWS for cyber and hybrid threats. These systems should integrate real-time monitoring tools and predictive analytics to pre-emptively identify and neutralise cyber and hybrid threats targeting critical infrastructure.
- Collaborative Training Programmes: Design joint training programmes that incorporate AI and cybersecurity scenarios for both civilian (including law enforcement) and military personnel. These programmes should address sector specific needs and hybrid threat scenarios.
- Integrated Threat Detection Systems: Deploy unified threat detection systems leveraging AI, ZTA, and Digital Twins for cross-sectoral application, targeting current and emerging cyber and hybrid threats.
- Cross-Sector Security Standards: Develop harmonised cybersecurity standards for dual-use technologies to ensure interoperability and scalability across EU Member States and propose EU-wide frameworks for harmonising cybersecurity standards, ensuring seamless integration of civilian and military technologies.
- Stakeholder Collaboration and Integration: Facilitate partnerships among diverse stakeholders, including national authorities, SMEs, academia, and industry stakeholders to foster innovation and deployment of dual-use solutions.

KPIs to measure outcomes and deliverables

In addition to the common indicators set out in Section 2, under "Guidance on milestones, deliverables and KPIs ", subsection KPIs, proposals shall report against the topic-specific KPIs set out below, where applicable.

Applicants shall assess the relevance of each topic-specific KPI to their proposed action:

- Where a KPI is applicable, applicants shall include it in their proposal and provide the required information.

- Where a KPI is not applicable because the corresponding activity, output or expected outcome is not part of the proposed action, applicants shall clearly indicate this and provide an appropriate justification.

Proposals may also include topic-optional KPIs from the indicative list below, where relevant to their proposed activities, outputs and expected outcomes. Applicants may propose additional KPIs where duly justified.

All KPIs must be measurable, verifiable, and clearly linked to the proposed activities, expected outcomes and deliverables. For each KPI included in the proposal, applicants must provide the information required in Table 1 KPI Template set out in Section 2, under "Guidance on milestones, deliverables and KPIs", subsection KPIs.

Topic mandatory KPIs

- Number of stakeholders from the civilian and defence cybersecurity communities involved in project activities
- Number of dual-use cybersecurity use cases, scenarios or good practices identified and documented

Topic optional KPIs

- Number of industrial stakeholders participating in cybersecurity activities directly relevant to both the defence and civilian sectors
- Number of white papers, guidelines, recommendations, reports or policy briefs produced
- Number of common activities, knowledge-transfer or best-practice exchange actions implemented between the two communities.

Milestones and deliverables

Applicants shall define milestones and deliverables that are specific to the proposed action and clearly linked to the topic objectives, scope, expected outcomes and planned activities.

Applicants shall prepare milestones and deliverables in accordance with the guidance set out at the begging of Section 2 "Guidance on milestones, deliverables and KPIs".

Targeted stakeholders

Stakeholders in either Cybersecurity Civilian (including law enforcement) and Defence Sphere, aiming at fostering joint collaborations targeting the delivery of concrete systems, tools and technologies, such as industrial players, Defence Ministries and Agencies, Ministries of Interior, SMEs and start-ups and relevant actors that play a role in the European Cybersecurity Civilian and Defence Spheres. Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.

Type of action and funding rate

Simple Grants — 50% funding rate

For more information on Digital Europe types of action, *see Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see sections 6 and 10 and Annex 2)
- For this topic, following reimbursement option for equipment costs applies: depreciation only and full cost for listed equipment *(see section 10)*
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:

- extent to which the project would reinforce and secure the digital technology supply chain in the Union
- extent to which the proposal can overcome financial obstacles such as the lack of market finance
- extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects
-

3. Available budget

The estimated available call budget is EUR **96 000 000**.

Specific budget information per topic can be found in the table below:

Topic	Topic budget
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI	**EUR 15.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME	**EUR 20.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP	**EUR 15.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH	**EUR 5.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC	**EUR 11.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG	**EUR 20.000.000**
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE	**EUR 10.000.000**

The availability of the call budget still depends on the final adoption of the 2025-2027 Work Programme amendment.

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	01 September 2026
Deadline for submission:	14 January 2027 – 17:00:00 CET (Brussels)
Evaluation:	February-March 2027
Information on evaluation results:	April 2027

GA signature:	October 2027

5. Admissibility and documents

Proposals must be submitted before the **call deadline** *(see timetable section 4)*.

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the Calls for proposals section link in the invitation letter). Paper submissions are NOT possible.

Proposals (including annexes, supporting documents and additional non-mandatory documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project *(to be filled in directly online)*
- Application Form Part B — contains the technical description of the project *(template to be downloaded from the Portal Submission System, completed, assembled and re-uploaded)*
- **mandatory annexes and supporting documents** *(templates to be downloaded from the Portal Submission System, completed, assembled and re-uploaded)*:
  - detailed budget table/calculator: not applicable
  - CVs of core project team: not applicable
  - activity reports of last year: not applicable
  - list of previous projects: not applicable
  - ownership control declarations including for associated partners and subcontractors:

    Additional non-mandatory document:

    In addition, applicants are encouraged to apply for membership to the Cybersecurity Competence Community through the National (NCCs) and attach proof of the request to the application (see Annex 4).

    Registration to the Cyber Community is not mandatory but encouraged for those entities that would like to be further engaged with the ECCC and NCC community.

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that all participants comply with the conditions for receiving EU funding *(especially eligibility, financial and operational capacity, exclusion, etc)*. Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable**, **accessible and printable** (please check carefully the layout of the documents uploaded).

Proposals are limited to maximum **70 pages** (Part B). Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents *(for legal entity validation, financial capacity check, bank account validation, etc)*.

For more information about the submission process (including IT aspects), consult the Online Manual.

6. Eligibility

Applications will only be considered eligible if their content corresponds wholly (or at least in part) to the topic description for which they are submitted.

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
  - EU Member States (including overseas countries and territories (OCTs))
  - EEA countries (Norway, Iceland, Liechtenstein)

Beneficiaries and affiliated entities must register in the Participant Register — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other consortium roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc *(see section 13)*.

Please be aware that all topics of this call are subject to restrictions due to security, therefore entities must not be directly or indirectly controlled from a country that is not an eligible country. **All entities[17] will have to fill in and submit a declaration on ownership and control.**

Moreover:

- participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is limited to entities established in and controlled from eligible countries
- project activities (included subcontracted work) must take place in eligible countries (see section geographic location below and section 10)
- the Grant Agreement may provide for IPR restrictions (see section 10).

For more information, *see Annex 2*.

[17] Except for entities that are validated as public bodies by the Central Validation Service.

Specific cases and definitions

Natural persons — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations — International organisations are NOT eligible, unless they are International organisations of European Interest within the meaning of Article 2 of the Digital Europe Regulation (i.e. international organisations the majority of whose members are Member States or whose headquarters are in a Member State).

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons[18].

EU bodies — EU bodies (with the exception of the European Commission Joint Research Centre) can NOT be part of the consortium.

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[19].

⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Countries currently negotiating association agreements — Beneficiaries from countries with ongoing negotiations for participating in the programme *(see list of participating countries above)* may participate in the call and can sign grants if the negotiations are concluded before grant signature and if the association covers the call (i.e. is retroactive and covers both the part of the programme and the year when the call was launched).

EU restrictive measures — Special rules apply for entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[20]. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

EU conditionality measures — Special rules apply for entities subject to measures adopted on the basis of EU Regulation 2020/2092[21]. Such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties, etc). Currently such measures are in place for Hungarian public interest trusts established under the Hungarian Act IX of 2021 or any entity they maintain (see Council Implementing Decision (EU) 2022/2506, as of 16 December 2022).

For more information, *see Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

18 See Article 200(2)(c) EU Financial Regulation 2024/2509.

19 For the definitions, see Articles 190(2) and 200(2)(c) EU Financial Regulation 2024/2509.

20 Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.

21 Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 325, 20.12.2022, p. 94).

Consortium composition

Consortium composition requirements vary by topic and are set out below. Unless otherwise specified, there is no minimum consortium composition requirement. Although proposals may be submitted by a single applicant where permitted, applicants are encouraged to form consortia where appropriate, as collaboration between complementary entities can strengthen the implementation and expected impact of the action.

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC: N/A

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH – Regional Cable Hubs: a minimum of 2 independent applicants (beneficiaries; not affiliated entities) form 2 different eligible countries. The consortium must include competent public authorities from at least two Member States concerned by the relevant sea basin, such as ministries, agencies or other public entities responsible for cable security, maritime security, resilience or the protection of critical infrastructure.

Proposals may include the expansion of existing Regional Cable Hubs projects funded under previous calls of this topic to additional Member States.

Eligible activities

Applications will only be considered eligible if their content corresponds wholly (or at least in part) to the topic description for which they are submitted.

Eligible activities are the ones set out in section 2 above.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

Projects must comply with EU policy interests and priorities *(such as environment, social, security, industrial and trade policy, etc)*. Projects must also respect EU values and European Commission policy regarding reputational matters (*e.g. activities involving capacity building, policy support, awareness raising, communication, dissemination, etc*).

Financial support to third parties is allowed in topic DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC for grants under the following conditions:

- the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality
- the calls must be published on the Funding & Tenders Portal, and on the participants' websites
- the calls must remain open for at least two months
- if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change

- the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries
- the calls must have a clear European dimension.

Geographic location (target countries)

Due to restrictions due to security:

- for all topics: the proposals must relate to activities taking place in the eligible countries (see above)

Ethics

Projects must comply with:

- highest ethical standards and
- applicable EU, international and national law (including the General Data Protection Regulation 2016/679).

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

For proposals involving development, testing, deployment, use or distribution of AI systems, the ethics review will in particular check compliance with the principles of human agency and oversight, diversity/fairness, transparency and responsible social impact, while the experts performing the technical evaluation will assess the robustness of the AI systems (i.e. their reliability not to cause unintentional harm).

Security

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Decision 2015/444[22] and its implementing rules and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
  - created or accessed only on premises with facility security clearance (FSC) from the competent national security authority (NSA), in accordance with the national rules
  - handled only in a secured area accredited by the competent NSA
  - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know

[22] See Commission Decision 2015/444/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)
- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearance may have to be provided before grant signature. The granting authority will assess the need for clearance in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearance.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables *(e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc)*.

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant *(e.g. technology restrictions, national security classification, etc)*. The granting authority must be notified immediately of any potential security issues.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the Participant Register during grant preparation *(e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc)*. The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities (see below, section 10)
- prefinancing paid in instalments
- (one or more) prefinancing guarantees (see below, section 10)
  or
- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

For more information, *see* *Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment*.

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the 'Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project
- description of the consortium participants

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate[23]:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct24 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

[23] See Articles 138 and 143 of EU Financial Regulation 2024/2509.

[24] 'Professional misconduct' includes, in particular, the following: violation of ethical standards of the profession; wrongful conduct with impact on professional credibility; breach of generally accepted professional ethical standards; false declarations/misrepresentation of information; participation in a cartel or other agreement distorting competition; violation of IPR; attempting to influence decision-making processes by taking advantage, through misrepresentation, of a conflict of interests, or to obtain confidential information from public authorities to gain an advantage; incitement to discrimination, hatred or violence or similar activities contrary to the EU values where negatively affecting or risking to affect the performance of a legal commitment.

- guilty of irregularities within the meaning of Article 1(2) of EU Regulation 2988/95 (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- intentionally and without proper justification resisted[25] an investigation, check or audit carried out by an EU authorising officer (or their representative or auditor), OLAF, the EPPO, or the European Court of Auditors.

Applicants will also be rejected if it turns out that[26]:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each topic) against the operational capacity and award criteria *(see sections 7 and 9)* and then ranked according to their scores.

For proposals with the same score (within a topic or budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:

1) Proposals focusing on a theme that is not otherwise covered by higher ranked proposals will be considered to have the highest priority.

2) The ex aequo proposals within the same topic will be prioritised according to the scores they have been awarded for the award criterion 'Relevance'. When these scores are equal, priority will be based on their scores for the criterion 'Impact'.

3) If this does not allow to determine the priority, a further prioritisation can be done by considering the overall proposal portfolio and the creation of positive synergies between proposals, or other factors related to the objectives of the call. These factors will be documented in the panel report.

4) After that, the remainder of the available call budget will be used to fund projects across the different topics in order to ensure a balanced spread of the

[25] 'Resisting an investigation, check or audit' means carrying out actions with the goal or effect of preventing, hindering or delaying the conduct of any of the activities needed to perform the investigation, check or audit, such as refusing to grant the necessary access to its premises or any other areas used for business purposes, concealing or refusing to disclose information or providing false information.

[26] See Article 143 EU Financial Regulation 2024/2509.

geographical and thematic coverage and while respecting to the maximum possible extent the order of merit based on the evaluation of the award criteria.

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

 No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc*.

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Full compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access *(see also Funding & Tenders Portal Terms and Conditions)*. Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

1. Relevance

- Alignment with the objectives and activities as described in section 2
- Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*****
- Extent to which the project can overcome financial obstacles such as the lack of market finance*****

2. Implementation

- Maturity of the project
- Soundness of the implementation plan and efficient use of resources
- Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

3. Impact

- 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

- Extent to which the project will strengthen competitiveness and bring important benefits for society
- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects ***.**

**May not be applicable to all topics (see specific topic conditions in section 2).*

Award criteria	Minimum pass score	Maximum score
Relevance	3	5
Implementation	3	5
Impact	3	5
Overall (pass) scores	**10**	**15**

Maximum points: 15 points.

Individual thresholds per criterion: 3/5, 3/5 and 3/5 points.

Overall threshold: 10 points.

Proposals that pass the individual thresholds AND the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on Portal Reference Documents.

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement *(Data Sheet, point 1)*. Normally the starting date will be after grant signature. A retroactive starting date can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration:

- for topic DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP the indicative duration of the action is 24 months, other durations are not excluded.
- for topics DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG, and DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE the indicative duration of the action is 36 months, other durations are not excluded.

Extensions are possible, if duly justified and through an amendment.

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal

The following deliverables will be mandatory for all projects:

- additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project
- additional deliverables (yearly) on achievement of relevant KPIs and project outputs.

Applicants must consult the information provided in Section 2, under *"Guidance on milestones, deliverables and KPIs"*, in particular the subsection *"Milestones" and "Deliverables"*

Form of grant, funding rate and maximum grant amount

The grant parameters *(maximum grant amount, funding rate, total eligible costs, etc)* will be fixed in the Grant Agreement *(Data Sheet, point 3 and art 5)*.

Project budget (requested grant amount):

Topic	Requested grant amount
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI	The requested EU contribution is expected to be between **EUR 3 million and EUR 5 million per project.** However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME	The requested EU contribution is expected to be between **EUR 3 million and EUR 5 million per project.** However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG	The requested EU contribution is expected to be between **EUR 3 million and EUR 5 million per project.** However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE	The requested EU contribution is expected to be between **EUR 3 million and EUR 5 million per project**. However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP	The requested EU contribution is expected to **be EUR 1.5 million per project**. However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH	The requested EU contribution is expected to be **EUR 2.5 million per project.** However, proposals requesting different amounts may also be considered, provided this is duly justified.
DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC	The requested EU contribution is expected to be **between EUR 2 million and EUR 3 million per project**. However, proposals requesting different amounts may also be considered, provided this is duly justified.

⚠ The grant awarded may be lower than the amount requested.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted*

costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement *(see art 6 and Annex 2 and 2a)*.

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of action which applies to the topic *(see section 2)*.

Grants may NOT produce a profit (i.e. surplus of revenues + EU grant over costs). For-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount *(see art 22.3)*.

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement *(e.g. improper implementation, breach of obligations, etc)*.

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement (Data Sheet, point 3 and art 6).

Budget categories for this call:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties (for topic DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC)
  - D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices)[27]: Yes
  - SME owner/natural person unit cost[28]: Yes
- travel and subsistence unit costs[29]: No (only actual costs)
- equipment costs:

[27] Decision of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

[28] Commission Decision of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7115).

[29] Commission Decision of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

  - depreciation (for topics DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG,
  - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-COORDPREP, DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH, and DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE))
- other cost categories:
  - costs for financial support to third parties allowed for grants
    - for topic DIGITAL-ECCC-2027-DEPLOY-CYBER-11-NCC: maximum amount per third party EUR 100 000; amounts of more than 60 000 EUR per third party are necessary because of the nature of the actions under this call is such that their objectives would otherwise be impossible or overly difficult to achieve;
  - internally invoiced goods and services (unit cost according to usual cost accounting practices)[30]: Yes
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).
- VAT: non-deductible/non-refundable VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
  - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
  - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
  - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
  - restrictions due to security:
    - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries (for all topics)
    - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible (for all topics)
  - other ineligible costs: No.

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement *(Data Sheet, point 4 and art 21 and 22)*.

After grant signature, you will normally receive a **prefinancing** to start working on the

[30] Decision of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

project (float of normally **80%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/10 days before starting date/financial guarantee (if required) – whichever is the latest.

There will be one or more **interim payments** (with cost reporting through the use of resources report).

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All ppayments will be made to the coordinator.

⚠ Please be aware that payments will be automatically lowered if you or one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement *(see art 22)*.

Please also note that you are responsible for **keeping records** on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement *(Data Sheet, point 4)*. The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are normally requested from the coordinator, for the consortium. They must be provided during grant preparation, in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement *(art 23)*.

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement *(Data Sheet, point 4 and art 24)*.

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement *(Data Sheet, point 4.4 and art 22).*

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up* to their maximum grant amount

- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*

or

- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes
- protection of results: Yes
- exploitation of results: Yes
- rights of use on results: Yes
- access to results for policy purposes: Yes
- access to results in case of a public emergency: Yes
- access rights to ensure continuity and interoperability obligations: No
- special IPR obligations linked to restrictions due to security:
  - exploitation in eligible countries: Yes (for all topics)
  - limitations to transfers and licensing: Yes (for all topics)

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- communication and dissemination plan: Yes
- dissemination of results: Yes
- additional dissemination obligations: No
- additional communication activities: Yes
- special logo: Yes – both EU and European Cybersecurity Competence Centre

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for PAC Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No

- special obligations linked to restrictions due to security
    - implementation in case of restrictions due to security or EU strategic autonomy: Yes

Other specificities

Consortium agreement: Yes – in case of more than one beneficiary

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

 For more information, *see AGA — Annotated Grant Agreement*.

11. How to submit an application

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) **create a user account and register your organisation**

To use the Submission System (the only way to apply), all participants need to create an EU Login user account.

Once you have an EULogin account, you can register your organisation in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) **submit the proposal**

Access the Electronic Submission System via the Topic page in the Calls for proposals section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 3 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and upload it as a PDF file
- Annexes (*see section 5*). Upload them as PDF file (single or multiple depending on the slots). Excel upload is sometimes possible, depending on the file type.

The proposal must keep to the **page limits** *(see section 5)*; excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System, otherwise the proposal may be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the IT Helpdesk webform, explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the Online Manual. The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- Online Manual
- Portal FAQ (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the IT Helpdesk.

For guidance and support related to this call, we recommend that you first contact the National Cybersecurity Coordination Centres (NCC) in your country, where available. The Network of NCCs includes one national centre from each of the 27 EU Member St ates plus Iceland and Norway. You may also address your questions to the ECCC Appli cants Direct Contact Centre at applicants@eccc.europa.eu Please indicate clearly the reference of the call and topic to which your question relates (see cover page).

13. Important

IMPORTANT

- **Don't wait until the end —** Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions *(e.g. congestion, etc)* will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System —** By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the Portal Terms & Conditions.
- **Registration —** Before submitting the application, all beneficiaries, affiliated entities and associated partners must be registered in the Participant Register. The participant identification code (PIC) (one per participant) is mandatory for the Application Form.
- **Consortium roles —** When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

  The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting, in very exceptional cases, may go beyond 30% of the total eligible costs must be justified in the application.
- **Coordinator —** In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any). If affiliated entities participate in your project, please do not forget to provide documents demonstrating their affiliation link to your organisation as part of your application.
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget —** Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully *(e.g. own contributions, income generated by the action, financial contributions from third parties, etc)*. You may be requested to lower your estimated costs, if they are ineligible (including excessive).

- **Completed/ongoing projects** — Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).

- **No-profit rule** — Grants may NOT give a profit (i.e. surplus of revenues + EU grant over costs). This will be checked by us at the end of the project.

- **No cumulation of funding/no double funding** — It is strictly prohibited to cumulate funding from the EU budget (except under 'EU Synergies actions'). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances be declared under two EU grants; projects must be designed as different actions, clearly delineated and separated for each grant (without overlaps).

- **Combination with EU operating grants** — Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice *(see AGA — Annotated Grant Agreement, art 6.2.E).*

- **Multiple proposals —** Applicants may submit more than one proposal for *different* projects under the same call (and be awarded funding for them).

  Organisations may participate in several proposals.

  BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw the others (or they will be rejected).

- **Resubmission —** Proposals may be changed and re-submitted until the deadline for submission.

- **Rejection —** By submitting the application, all applicants accept the call conditions set out in this this Call document (and the documents it refers to). Proposals that do not comply with all the call conditions will be rejected. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, they must be replaced or the entire proposal will be rejected.

- **Cancellation —** There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.

- **Language —** You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, *see section 12*).

Annex 1

Digital Europe types of action

The Digital Europe Programme uses the following actions to implement grants:

Simple Grants

Description: Simple Grants (SIMPLE) are a flexible type of action used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.

Funding rate: 50% Simple Grants — The funding rate may be exceptionally changed in very specific cases and always in accordance with the approved Work Programme.

Payment model: Prefinancing – (x) interim payment(s) – final payment

SME Support Actions

Description: SME Support Actions (SME) are a type of action primarily consisting of activities directly aiming to support SMEs involved in building up and the deployment of the digital capacities. This type of action can also be used if SMEs need to be in the consortium and make investments to access the digital capacities.

Funding rate: 50% except for SMEs where a rate of 75% applies

Payment model: Prefinancing – (x) interim payment(s) – final payment

Coordination and Support Actions (CSAs)

Description: Coordination and Support Actions (CSAs) are a small type of action (a typical amount of 1-2 Mio) with the primary goal to support EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure and may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Grants for Procurement

Description: Grants for Procurement (GP) are a special type of action where the main goal of the action (and thus the majority of the costs) consist of buying goods or services and/or subcontracting tasks. Contrary to the PAC Grants for Procurement *(see below)* there are no specific procurement rules (i.e. usual rules for purchase apply), nor is there a limit to 'contracting authorities/entities'. Personnel costs should be limited in this type of action; they are in general used to manage the grant, coordination between the beneficiaries, preparation of the procurements.

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

PAC Grants for Procurement

Description: PAC Grants for Procurement (PACGP) are a specific type of action for procurement in grant agreements by 'contracting authorities/entities' as defined in the EU Public Procurement Directives (Directives 2014/24/EU , 2014/25/EU and 2009/81/EC) aiming at innovative digital goods and services (i.e. novel technologies on the way to commercialisation but not yet broadly available).

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

Grants for Financial Support

Description: Grants for Financial Support (GfS) have a particular focus on cascading grants. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations.

Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria.

In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third party costs.

Funding rate: 100% for the consortium, co-financing of 50% by the supported third party

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance sub-grants) – payment of the balance

Lump Sum Grants

Description: Lump Sum Grants (LS) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature). on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented only part of the lump sum will be paid.

Funding rate: 100%/50%/50% and 75% (for SMEs)

Payment model: Prefinancing – (x) interim payment(s)– final payment

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators ; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Annex 2

Eligibility restrictions under Articles 12(5) and (6) and 18(4) of the Digital Europe Regulation

Security restrictions Article 12(5) and (6)

If indicated in the Digital Europe Work Programme, and if justified for security reasons, topics can exclude the participation of legal entities *established* in a third country or DEP associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including DEP associated countries)[31].

This restriction is applicable for SO1 (High Performance Computing), SO2 (Artificial Intelligence) and SO3 (Cybersecurity), but at different levels.

- In the case of SO3, the provision is implemented in the strictest way. When activated, only entities established in the EU AND controlled from the EU will be able to participate; entities from associated countries (which are normally eligible) can NOT participate — unless otherwise provided in the Work Programme.

- In SO1 and SO2, entities established in associated countries and entities controlled from non-EU countries may participate, if they comply with the conditions set out in the Work Programme (usually:

  - for the associated countries: be formally associated to Digital Europe Programme and receive a positive assessment by the Commission on the replies to their associated country security questionnaire.

  - for the participants: submission of a guarantee demonstrating that they have taken measures to ensure that their participation does not contravene security or EU strategic autonomy interests).

 EEA countries (and participants from EEA countries) are exempted from these restrictions (and additional requirements) because EEA countries benefit from a status equivalent to the Member States.

In order to determine the ownership and control status, participants[32] will be required to fill in and submit an ownership control declaration* as part of the proposal (and later on be requested to submit supporting documents) *(see Guidance on participation in EU restricted calls with ownership and control restrictions*)*.

In addition, where a guarantee is required, the participants will also have to fill in the guarantee template*, approved by the competent authorities of their country of establishment, and submit it to the granting authority which will assess its validity.

The activation of these restrictions will also make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

---

31 See Article 12(5) and (6) of the Digital Europe Regulation 2021/694.

32 Beneficiaries and affiliated entities, associated partners and subcontractors — except for entities that are validated as public bodies by the Central Validation Service.

Thus:

- participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is also limited to entities established in and controlled from eligible countries
- project activities (included subcontracted work) must take place in eligible countries
- the Grant Agreement provides for specific IPR restrictions.

Strategic autonomy restrictions Article 18(4)

If indicated in the Digital Europe Work Programme, calls can limit the participation to entities *established* in the EU, and/or entities established in third countries associated to the programme for EU strategic autonomy reasons[33].

The activation of these restrictions will make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

 For more information, *see* *Guidance on participation in EU restricted calls with ownership and control restrictions**.

[33] See Article 18(4) of the Digital Europe Regulation 2021/694.

Annex 3

Coordinated Preparedness Testing under the Cyber Solidarity Act

Introduction

The Regulation (EU) 2025/38 (hereafter 'Cyber Solidarity Act' or 'CSoA'), in force since 4 February 2025, lays down measures that aim at strengthening capabilities in the European Union (EU) to detect, prepare for and respond to significant and large-scale cyber threats and incidents.[34] More specifically, the Regulation provides for the establishment of a Cybersecurity Emergency Mechanism to support and complement Member States' both proactive and reactive efforts against significant, large-scale and large-scale-equivalent cyber incidents.[35]

As part of the preparedness actions, the Cyber Solidarity Act states that **the Cybersecurity Emergency Mechanism shall support the voluntary coordinated testing of entities operating in sectors of high criticality** across the Union as defined in Annex I to Directive (EU) 2022/2555 (NIS 2 Directive). Support may consist of such preparedness activities as penetration testing and threat assessment and shall be provided to Member States[36] upon request, primarily **in the form of grants managed by the European Cybersecurity Competence Centre (ECCC)**.[37]

More specifically, according to the Regulation, the European Commission, after consulting the NIS Cooperation Group (NISCG), the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) and the European Union Agency for Cybersecurity (ENISA), shall identify – among those listed in Annex I of the NIS 2 Directive – the sectors or sub-sectors that would mostly benefit from coordinated preparedness testing (CPT) support and for which a call for proposals to award grants may thus be issued.

At the outset of 2026, the Commission – in agreement with the relevant stakeholders above – identified the following sectors and/or sub-sectors to be subject of coordinated preparedness testing:

1. The **energy sector** and in particular the **electricity** sub-sector;
2. The **transport sector** and in particular the **rail** and **water (ports)** sub-sectors;
3. The **public administration sector**.

CPT work arrangements and approach

According to the Cyber Solidarity Act, **common risk scenarios and methodologies shall be developed to guide the coordinated preparedness testing.[38]**

In line with the Regulation, after receiving positive feedback on the sectors selected for the 2026 edition of coordinated preparedness testing, the Commission and ENISA have commenced the process of drafting the common risk scenarios in close cooperation with relevant stakeholders and expert groups. More precisely, consultations occurred with

[34] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). http://data.europa.eu/eli/reg/2025/38/oj

[35] Regulation (EU) 2025/38, *Article 10*.

[36] According to the Regulation, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU and 2014/25/EU of the European Parliament and of the Council.

[37] Regulation (EU) 2025/38, *Article 12*.

[38] Regulation (EU) 2025/38, Article 12.

the NISCG Work Stream on Energy, the European Union Agency for Railways (ERA) and the European Maritime Safety Agency (EMSA), the informal group of public administration sector experts recently established by ENISA and the NISCG Work Stream on Risk Assessment and Supply Chain Security.

The common risk scenarios have been developed according to a dedicated methodology that not only carefully considers Member States' specific needs and the maturity levels of the selected sectors, but is also guided by national and/or EU level risk assessments to provide "what-if" situations where the effect of risks materialising is measured.

Each participating **Member State may choose – among those proposed in the present document – the risk scenarios that they intend to use as a reference** during the national coordinated preparedness testing activities.

Member States may adapt and tailor the proposed scenarios according to specific national contexts and needs. More specifically, Member States:

- are encouraged to adopt a **risk-based approach** that considers – and possibly integrates within a certain risk scenario – system failures, human error, malicious acts, natural phenomena and/or combinations thereof;
- are encouraged to explore **systemic risks** by covering also supply chain and interdependencies-related issues since the impact of a cybersecurity incident may significantly increase when an organisation is heavily dependent on affected services and lacks alternative services;
- may consider expanding the proposed risk scenarios to reflect the **cumulative effects of multiple (possibly unsophisticated and/or unrelated) incidents occurring simultaneously** within a defined timeframe and thus raise the intensity and overall complexity of the scenarios (e.g., incidents affecting individual organisations, supply chain disruptions);

However, **the proposal submitted by Member States to request for supporting grants shall include at least the baseline risk scenario** (i.e., low stress level).

Phases of coordinated preparedness testing

The coordinated preparedness testing activities shall be conducted by participating Member States following a common illustrative methodology, articulated in three primary phases as outlined below.

A. Systemic risk analysis phase

The first phase consists in the planning of the testing activities via a systemic risk assessment whereby Member States shall, *inter alia*:

- identify key stakeholders;
- define the scope and (primary and secondary) objective(s) of the activities;
- select the type of test evaluation;
- design the test structure;
- refine the risk scenarios based on specific needs;
- conduct pilot tests to ensure reliability and validity.

B. Testing phase

The second phase marks the launch of the testing activities, which may include, *inter alia*:

- Vulnerability Scanning;
- Security Audits;
- Penetration Testing;
- Exercises;
- (Cyber Resilience) Stress Tests.

C. Gap analysis phase

The third and final phase provides for, *inter alia*:

- the identification of gaps and areas of improvement;
- the elaboration of recommendations;
- the definition of an Action Plan.

The results of the coordinated preparedness testing should be integrated in the remediation plan of the tested entity and should be sent to the Member State authority to review the results of the activity. Lessons learned should be shared, in an anonymised and aggregated form, with the Commission. A follow-up discussion could take place in the relevant workstreams of the NIS Cooperation Group.

CPT risk Scenarios 2026

Risk scenarios serve as the foundation for reflecting specific risks in the identified sectors and, accordingly, the needs for testing based on Member States comments and the overall threat landscape.

The scenario building process for the CPT risk scenarios is based on the methodology adopted by the NISCG WS on Risk Assessments and Supply Chain Security. This methodology aims at supporting resilience building initiatives through a structured approach where building blocks are utilised for designing realistic scenarios and to incorporate an all-hazard approach to cyber incidents.

Therefore**, the following risk scenarios adopt a multi-layer structure by using a baseline scenario and two additional scenarios (with aggravation levels), each compounding on the previous one.** For each risk scenario, we provide a short description of the scenario together with its primary impacts.

1. Energy sector: electricity

RISK SCENARIOS OVERVIEW:

RS.1 – Low stress level

Supply-chain compromise affecting RES market platforms and grid stakeholders

RS.2 – Medium stress level

Ransomware attack affecting Renewable Energy Sources (RES) aggregators and grid operations

RS.3 – High stress level

Supply-chain–enabled destructive attack on RES platforms and grid-supporting systems

Risk scenario 1 – Low stress level (baseline scenario)

Scenario 1: Supply-chain compromise affecting RES market platforms and grid stakeholders Exploitation of vulnerabilities in third-party suppliers and information and communication technology (ICT) systems used by RES operators and aggregators. Core grid operations remain unaffected but some operational and market processes are degraded and a hidden risk is introduced into the interconnected ICT systems supporting electricity generation, markets and grid operations.	
Scenario steps	**Impact**
1. A cybercriminal group exploits a known but unpatched vulnerability in a cloud-based software platform[39] provided by a third-party supplier and widely used by RES operators and aggregators to monitor production, manage assets and exchange data with Distribution (DSOs) and Transmission System Operators (TSOs). The platform is compromised and operational data are potentially accessible. 2. Through the compromised supplier environment, the attacker introduces malicious code that enables passive reconnaissance (credential harvesting, system mapping, telemetry access) without disrupting normal operations. Confidentiality is compromised after data access and credential exposure. Unauthorised code is executed. 3. In parallel, the attacker compromises a sector-specific website (e.g., RES vendor support portal or industry association website) and uses it as a water-holing site, exposing engineers, operators and market analysts to browser-based exploitation when accessing documentation or updates. 4. Credentials and system information collected from RES operators and aggregators allow the attacker to map interconnections between RES assets, market platforms and grid operators, without triggering security alerts. Sensitive system mapping and unauthorized access paths established.	• No interruption of electricity supply. • RES operators and aggregators continue normal operations but their ICT environments are partially compromised without detection. • Market-facing processes (e.g., forecasting, availability declarations, flexibility offers) remain operational, but their integrity can no longer be fully trusted. • TSOs and DSOs are not immediately affected, but are unknowingly exposed through trusted data exchanges with compromised RES platforms.

Risk scenario 2 – Medium stress level

Scenario 2: Ransomware attack affecting RES aggregators and grid operations Compromise of trusted third-party suppliers and RES market platforms leads to operational disruption and loss of availability of key ICT systems supporting electricity market participation and grid operations. Electricity supply is maintained but uncoordinated reductions in renewable generation – combined with degraded market data and system availability – significantly stress grid operations and electricity market processes, requiring manual interventions and emergency procedures.	
Scenario steps	**Impact**
1. Using credentials obtained via a compromised third-party RES platform supplier, a Cybercriminal group	• No widespread power outages, but grid operations are significantly stressed due to

[39] The compromised platform is also used by several electricity market participants for forecast submission, availability reporting, and flexibility aggregation, creating a shared attack surface across multiple organisations

deploys ransomware into the ICT environments of several RES aggregators and market service providers operating across the region. Unauthorised access and execution. 2. The attacker configures the ransomware to avoid immediate impact on OT but maintains persistence and command-and-control access, while deliberately preserving OT and control system integrity, enabling further escalation at a later stage. Integrity is undermined after unauthorized persistence, there is a latent disruption risk. 3. In parallel, the attacker exploits trusted IT/OT integration points (e.g., aggregator control gateways, remote access and maintenance channels) within RES aggregator environments to manipulate operational parameters, including: 3.1. Temporarily disabling remote control functions for selected RES assets; 3.2. Forcing repeated safety-related shutdowns or fail-safe modes in inverter- and controller-managed installations. 4. The ransomware spreads through shared cloud services and remote management tools, encrypting: 4.1. Asset management systems used to control RES installations; 4.2. Forecasting and bidding platforms used for electricity markets. 5. System and data are no more available. 6. To delay detection, the group launches Distributed Denial-of-Service (DDoS) attacks against RES aggregator customer portals and electricity market transparency and reporting websites to indirectly impact on trust in information.	reduced visibility and the presence of unreliable or incorrect data on RES availability and flexibility. • RES aggregators experience loss of availability of key ICT systems supporting forecasting, bidding, and flexibility management. • Electricity market processes are disrupted, leading to delays, incomplete submissions, increased imbalances and price volatility. • TSOs and DSOs are forced to switch to manual procedures and conservative operating assumptions to maintain grid stability. • Public communication becomes challenging as customers and stakeholders experience conflicting information regarding RES availability and market outcomes.

Risk scenario 3 – High stress level

Scenario 3: Supply-chain–enabled destructive attack on RES platforms and grid-supporting systems A coordinated, supply-chain–enabled cyberattack escalates into destructive actions against ICT systems supporting RES, grid operations, and market coordination. The incident causes regional electricity supply disruptions, prolonged recovery times, and cross-border effects, including the activation of crisis management mechanisms	
Scenario steps	**Impact**
1. Leveraging persistent access established through compromised RES platform suppliers and cloud service providers, a highly capable State-nexus threat actor deploys destructive wiper[40] malware across:	• Regional power supply disruptions occur, including forced load shedding and preventive disconnection of RES installations.

[40] The wiper malware permanently deletes, configuration files for RES installations, control logic and historical data used for forecasting and dispatch as well as system backups required for rapid restoration.

1.1. RES aggregator control systems; 1.2. Cloud-hosted RES management platforms; 1.3. Backup and recovery systems supporting grid-related ICT. 2. The threat actor uses trusted software update and management channels to distribute the wiper malware across multiple organisations and regions. Trusted channel is compromised and widespread system is impacted. 3. In parallel, selective ransomware attacks encrypt IT systems used by TSOs, DSOs, and market operators, preventing coordinated response and recovery. 4. A human error during system isolation unintentionally disrupts a backup communication interface used for RES monitoring and dispatch, reducing redundancy at a critical moment. 5. To further delay recovery and coordination, large-scale DDoS attacks target national cyber incident response platforms, energy-sector information-sharing systems, and cross-border electricity coordination platforms, disrupting real-time communication and situational awareness. 6. The attacker disables or corrupts control and telemetry interfaces of compromised RES platforms and aggregator systems by manipulating APIs and configuration services.	• Grid stability is significantly degraded due to loss of reliable generation and flexibility information. • Electricity markets, including trading and balancing, are temporarily suspended or significantly limited, with cross-border coordination relying on reduced-capacity communication channels and predefined emergency arrangements. • Restoration is prolonged as affected systems must be rebuilt and reconfigured, triggering national and cross-border crisis management procedures.

Similar past incidents

Date of reporting	***Incident***	***Source***
30 March 2022	Supply chain attack affecting wind energy infrastructures	**link**, **link**
30 January 2026	Coordinated cyberattacks on renewable energy plants	**link**

2. Transport sector: maritime and railway

MARITIME RISK SCENARIOS OVERVIEW:	**RAILWAY RISK SCENARIOS OVERVIEW:**
RS.1 – Low stress level Ransomware attack on port information technology (IT) systems	**RS.1 – Low stress level** Ransomware attack affects railway customer services
RS.2 – Medium stress level Operational technology/industrial control systems (OT/ICS) disruption affecting port equipment	**RS.2 – Medium stress level** Coordinated cyberattack against a railway operator, targeting both IT and OT systems used for rail traffic management

RS.3 – High stress level	**RS.3 – High stress level**
Coordinated multi-modal disruption including rail logistics	DDoS attack combined with physical attacks (sabotage) affecting train services

2.1 Maritime – Ports

Risk scenario 1 – Low stress level (baseline scenario)

Scenario 1: Ransomware attack on port information technology (IT) systems A ransomware group compromises port IT systems via spear-phishing, gaining access to internal networks and escalating privileges. They deploy ransomware targeting maritime single window and payment platforms. Encryption of critical data disrupts terminal operating systems and cargo management platforms. Container processing is affected forcing manual operations. There is congestion at berths and administrative overburden with operational and economic impacts.	
Scenario steps	**Impact**
1. A financially-motivated threat actor launches a spear-fishing campaign targeting port staff. 2. An unsavvy employee falls victim to the campaign by clicking on the fake link. 3. The malware (initial loader) infects and compromises the port office's IT network and the systems depending on it, namely the maritime single window and payment platforms. 4. This allows for the attackers to successfully infiltrate and escalate privileges. 5. With a foothold on the systems, attackers deploy ransomware against terminal operating systems, disrupting cargo tracking and billing IT systems.	• Delayed container processing, billing outages, manual procedures needed. • Queues at berths. • Port admin paralysis with economic loss. • Light disruption of some OT services.

Risk scenario 2 – Medium stress level

Scenario 2: Operational technology/industrial control systems (OT/ICS) disruption affecting port equipment An advanced persistent threat (APT) group steals the credentials of a third-party service provider used in the port's remote access maintenance platform. By abusing trusted remote administration capabilities, the attackers deploy malicious payloads and leverage the high-level privileges granted by the stolen credentials to enter the OT networks and controls multiple port operation systems.	
Scenario steps	**Impact**
1. An APT group steals the credentials of a trusted vendor that performs equipment maintenance through a remote access platform. 2. The attacker pushes a legitimate update and the system automatically runs the update as part of routine maintenance. The malware is installed.	• Equipment unable to move containers, extended crane idle times. • Safety shutdowns, potential physical hazards. • Backlog of cargo building rapidly on premises. • Since the entry point is a vendor tool, other ports may be affected.

3. The remote access to the network allows the attacker to establish persistence and proceed to harvest credentials and tokens using in-mem tooling. 4. The high-level privileges of the vendor's credentials allow the attacker to move to the port's OT environment unnoticed and gain control of critical PLC controllers. 5. Several port operation systems (crane control systems, terminal operating systems, gate automation systems) are now in control of the APT group, allowing for unsafe/hazardous operation or halt.	• Media attention – Public concern –reputational impact. • Financial loss due to operation halt.

Risk scenario 3 – High stress level

Scenario 3: Coordinated multi-modal disruption including rail logistics In the context of geopolitical tensions, a state-nexus threat actor known to target the transport sector conducts initial reconnaissance on port and connected railway network systems. After identifying an unpatched vulnerability on the port ERP / logistics platform, the group disrupts the logistics dispatch IT layer, moving then to port ICS and rail signalling/CCTV/dispatch servers. There is major port standstill with blocked containers and connected railway freight left idle or stranded.	
Scenario steps	**Impact**
1. A state-nexus threat actor conducts initial reconnaissance on port and connected railway network systems. 2. The actor identifies an unpatched vulnerability on the port ERP and gets a foothold on both the port logistics platform and the rail freight management system. 3. The actor launches an attack which floods systems with DDoS & malware and simultaneously disrupts port ICS (cargo systems, terminal controls) and rail signalling/CCTV/dispatch servers. 4. Intermodal transfer coordination platforms suffer major stalls, with significant impacts on freight movement.	• Major port standstill with blocked containers. • Connected rail freight disrupted — left idle or stranded. • Broader supply chain shock with backlog at inland depots. • Economic losses, congestion at other hubs, extended delivery delays.

Similar past incidents

Date of reporting	***Incident***	***Source***
07 December 2024	Ransomware and data theft attack against port systems	**link**
25 March 2026	Ransomware attack disrupts operations at major port	**link**

2.2Railway

Risk scenario 1 – Low stress level (baseline scenario)

Scenario 1: Data exfiltration and DDoS attack affects railway customer services (ticketing systems, passenger information systems) A financially-motivated threat actor exploits a public-facing application to access the network, steal customer data and disrupt critical systems through a large-scale DDoS attack. This leads to widespread outages across ticketing, passenger information and customer service platforms.	
Scenario steps	**Impact**
1. A financially motivated threat actor exploits a vulnerability in a public-facing web application (e.g., ticketing portal) to gain access to the corporate IT network. 2. The threat actor exfiltrates customer data (e.g., names, emails, travel history, possibly partial payment data). 3. Once inside the network, the threat actor moves laterally across IT systems and identifies critical servers for ticket sales, station display boards, mobile apps and customer support centres. 4. The threat actor launches a large-scale DDoS attack targeting (ticketing website, mobile apps, passenger information services and customer service portals). 5. The threat actor makes unavailable the public ticketing website, mobile ticketing apps, passenger information services and customer service web portals. Services become slow or unavailable to users. 6. The threat actor publicly leaks or threatens to leak stolen data.	• Passenger-facing systems unavailable and customers service systems overwhelmed or degraded. • Trains continue running but delays occur due to passenger confusion. • Passengers unable to purchase or validate tickets. • Passengers experience confusion about platforms, departure times and delays. • Increased station crowding and queuing is observed, causing potential safety issues. • Call centres are overwhelmed with passenger inquiries. • Complaints and refund requests increase dramatically. • Risk of phishing and fraud using stolen data • Reputational and legal impact.

Risk scenario 2 – Medium stress level

Scenario 2: Coordinated cyberattack against a railway operator, targeting both IT and OT systems used for rail traffic management An advanced persistent threat (APT) uses compromised remote access credentials to infiltrate the corporate IT network and subsequently pivots into OT systems by exploiting a vulnerability in a management interface. The actor deploys ransomware or wiper malware on critical train control and scheduling systems, disrupting monitoring and signalling capabilities. As a result, rail operations shift to degraded modes with reduced speeds and manual controls to maintain safety.	
Scenario steps	**Impact**
1. An advanced persistent threat (APT) group gains an initial access in the corporate IT network by using compromised credential for remote access (VPN or remote maintenance portal). 2. Once inside the IT network, the threat actor performs network discovery and system mapping in order to locate systems used for train scheduling, traffic management and signalling supervision.	• Real-time scheduling tools unavailable. • Dispatchers rely on manual coordination. • Trains operate at reduced service and significant delays occur. Some routes are temporarily suspended. • Increased congestion at key stations. • Announcements must be made manually by staff. • Passengers switching to alternative transportation.

3. The threat actor identifies a known vulnerability or misconfiguration in an OT management interface or a remote maintenance gateway. 4. By exploiting this vulnerability, the attacker gains access to operational systems, namely signalling systems and traffic management systems and the workstations in the operations control centre. 5. The threat actor deploys ransomware or wiper malware to critical operations systems (e.g., traffic management systems, train scheduling platforms, workstations at operations control centre). 6. Monitoring and signalling support systems become unavailable, so real-time train tracking is lost or degraded. 7. Safety mechanisms prevent unsafe operation, forcing rail operators to switch to degraded operating modes (reduced speed, manual dispatching, increasing headways).	

Risk scenario 3 – High stress level

Scenario 3: DDoS attack combined with physical attacks (sabotage) affecting train services A state-nexus threat actor plans a coordinated attack targeting both digital services and physical rail infrastructure during peak disruption periods. They combine a large-scale DDoS attack on customer-facing IT systems with simultaneous sabotage of signalling and communication equipment. This results in widespread service outages, degraded signalling, reduced train speeds and suspension of some routes due to infrastructure damage.	
Scenario steps	**Impact**
1. A state-nexus threat actor identifies critical IT services (ticketing, passenger information, mobile apps, web portals), physical infrastructure points (signalling cables, trackside equipment, communication nodes) and selects timing to maximize disruption (e.g., peak hours or major event). 2. The threat actor coordinated attacks: 2.1. High-volume DDoS attack targeting online ticketing systems, passenger information platforms, railway mobile applications, corporate/public web portals; 2.2. Simultaneous sabotage at multiple locations (e.g., cutting signalling and fibre-optic cables, arson damaging trackside switching units and signalling equipment, physical damage to communication equipment). 3. IT systems become slow or unavailable to users. Signalling systems degrade or revert to safe mode. Train speeds are reduced and traffic capacity decreases. Some routes are suspended due to infrastructure damage.	• Delays and cancellations across affected region. • Reduced train frequency. • Knock-on delays across wider network. • Passengers lose access to online ticketing or apps. • Inaccurate or unavailable passenger information. • Overcrowding at stations and increased confusion.

Similar past incidents

Date of reporting	*Incident*	*Source*
03 November 2022	Supply chain attack causing disruptions to train networks	**link**
17 November 2025	Cyber and sabotage attacks against rail infrastructures	**link**
19 February 2026	IT systems of rail operator disrupted due to DDoS attack	**link**

3. Public administration sector

RISK SCENARIOS OVERVIEW:

RS.1 – Low stress level

DDoS, Website Defacement and Phishing Campaign

RS.2 – Medium stress level

Supply Chain Compromise, Vendor Risk and Ransomware Attack

RS.3 – High stress level

State-Nexus Intrusion, Strategic Espionage and Wiper Attack

Risk scenario 1 – Low stress level (baseline scenario)

Scenario 1: DDoS, Website Defacement and Phishing Campaign

A known hacktivist group targets a regional public administration web portal. The primary external-facing website of the regional public administration becomes intermittently unavailable due to a DDoS. Simultaneously, a secondary, informational microsite is defaced with political messaging. In parallel, a broad-based phishing campaign targets administration staff, aiming to harvest credentials and increase operational pressure, without being the primary intrusion vector.

Scenario steps	**Impact**
1. A hacktivist group abuses a vulnerability in a public-facing web portal or uses automated probing to map the administration's public-facing IP ranges and identify API endpoints without rate limiting identifying the exposed assets. 2. The group leases a "DDoS-as-a-Service" botnet that consists of thousands of compromised devices (blending in with legitimate local ISP traffic) and begins an attack. The target is the web infrastructure. The attack affects availability by causing service disruption and intermittent outages. 3. While the administration's IT team is distracted by the DDoS, the attackers exploit a known low-severity vulnerability in a legacy CMS to swap the homepage with their "manifesto", which affects integrity because of content tampering. 4. The attackers then post screenshots of their defaced sites on Telegram to claim a total breach of the	• Systems supporting core day-to-day operations remain fully operational. However, citizens of the given region experience slow load times or timeouts when trying to access online forms or information available via the web portal. • Helpdesk becomes strained by increased inquiries from citizens unable to access services offered via the platform. • Reputation is affected as trust is in question– some confusion and social media chatter – speculation on what has happened and "the entire administration being down". • Misinformation causes public concern. • Potential credential exposure (if phishing successful), with no immediate visible service impact may have legal/regulatory consequences. The risk of future compromise arises.

administration (disinformation), in order to affect public perception. 5. In parallel a broad-based phishing campaign is taking place against staff via phishing emails aimed at credential harvesting from staff accounts.	

Risk scenario 2 – Medium stress level

Scenario 2: Supply Chain Compromise, Vendor Risk and Ransomware Attack A cybercriminal threat actor compromises the update mechanism of a widely used managed services platform, inserting malicious code into a legitimate software update distributed to multiple clients (including entities in the public administrations sector). Weak vendor management and insufficient third-party risk controls mean the update is pulled by many different public administrations. Once installed across environments, the embedded payload enables covert access, large-scale data exfiltration and subsequent ransomware deployment and extortion, leading to simultaneous compromise of numerous entities.	
Scenario steps	**Impact**
1. Cybercriminal group compromises a trusted software vendor and distribute a legitimate-looking, signed update containing a malicious loader/backdoor, abusing the trusted software supply chain. 2. The public administration's automated system retrieves and installs the signed (trusted) update as part of routine maintenance affecting endpoint systems by the software update service. 3. The malicious component executes within the context of the legitimate software, deploys a beacon into the host systems, it then establishes encrypted Command and Control Communication (C2) mimicking legit network traffic. 4. Via the C2 the cybercriminal group performs low noise recon before migrating to a "trusted process", establishes persistence and proceeds to harvest credentials and tokens using in-memory tooling. 5. Using the credentials, the group moves laterally to any systems accessible with available privileges (additional servers, file shares, backup infrastructure, Domain Controllers if accessible, cloud identity platforms). 6. The goal is broad expansion – not precision. If they can obtain domain-level access they do, but they can encrypt without it so they may proceed as such. 7. Accessible sensitive data is quickly identified (file repositories, databases) and exfiltrated in bulk via encrypted outbound channels. Confidentiality is compromised due to a data breach/leakage. 8. Backup and recovery mechanisms are targeted where possible in order to disable or corrupt backups (reduce recovery options before ransomware attack), to achieve disruption of availability by making recovery is not possible.	• Third-party risk: Dependence on vendor security posture amplifies impact and reduces direct control over the incident spread. • Exfiltrated data: Reputational damage/ media scrutiny etc./ Public trust corroded. • Ransomware: day-to-day operations impacted – service disruption potential slowing down or downtime (file servers unavailable, email systems may be disrupted, workstations locked, shared drives encrypted). • Response actions: IT resources overloaded (containment, rebuilding servers, password resets, reimaging endpoints etc.). • Since the entry point is a vendor tool, other connected administrations may be affected (cross-entity impact). • Mandatory incident reporting – post-incident audits policy reviews.

9. Once sufficient data has been exfiltrated, the group deploys ransomware widely across reachable systems using available tools (speed over precision). 10. A ransom demand is issued, in order to restore/ give back access to the stolen data which is currently unavailable due to encryption.	

Risk scenario 3 – High stress level

Scenario 3: State-Nexus Intrusion, Strategic Espionage and Wiper Attack A state-nexus threat actor conducts a targeted intrusion via spear-phishing to gain persistent access to critical systems. Following a period of covert strategic data exfiltration and prepositioning, the actor activates a destructive wiper payload, potentially triggered by a geopolitical or sector-specific event, causing significant system degradation, operational disruption and loss of critical data.	
Scenario steps	**Impact**
1. The state-nexus threat actor conducts reconnaissance (OSINT, profiling) on administration personnel (sources: public websites, social media, conferences), gathering information that can be used for further targeting. 2. The actor then prepares a spear-phishing email containing a weaponized attachment and sends it to a senior officer. 3. Once the senior officer downloads the malicious attachment, that drops a lightweight payload and creates an in-memory beacon which gives the attacker hands on keyboard. 3.1. The implant performs an internal reconnaissance before migrating to a legitimate process (LOTL-based execution); 3.2. Persistence is established in a low-noise manner. 4. The threat actor subsequently moves to broaden their access covertly, performing in-memory credential harvesting and limited lateral movement to shared file servers using that to identify and collect high-value information (SharePoint, mailboxes, document repos e.g., internal briefs, communications etc.). 5. The actor proceeds to stage data in small encrypted archives, in preparation for exfiltration which is anticipated to have a major impact on confidentiality. 6. Using a "slow and low" approach they proceed to siphon data out of the administration over a period of months, impacting confidentiality. 7. To ensure they maintain continuous access, the threat actors may decide to rotate their Command-and-Control domains and IPs.	• Strategic and geopolitical impact: sustained intelligence asymmetry, disadvantaging the compromised party. • Political and reputational impact when discovered (erodes public trust, raises questions about national security, invites scrutiny/inquiries etc.). • Recovery is harder as it is difficult to easily determine the extent of compromise, the precise root-cause, the breadth of systems and information impacted etc. • Long-term undetected presence of attackers within compromised systems may result in a prolonged exposure of sensitive data and systems. • Upon activation of destructive payload (wiper) the administration suffers system disruption and data loss.

8. Upon the occurrence of a geopolitical or sector-specific event, the threat actor triggers the execution of a wiper which causes data loss and wide service disruption.	

The scenario can be further extended by introducing either additional concurrent cyber incidents or non-cyber disruptions affecting systems within an all-hazards context, such as non-malicious technical failures. Adding multiple simultaneous events increases operational strain and further stretches incident response capacity. An example of such a scenario add-on could be: a parallel non-malicious outage affecting a critical supporting service (e.g., a cloud identity or authentication platform) caused by a faulty software update, disrupts user access to key systems and further compounds response efforts already underway due to the cyber incident.

Similar past incidents

Date of reporting	***Incident***	***Source***
07 October 2024	Large-scale breach of data related to police officers	**link**
05 June 2025	Fraud against tax office through phishing tactics	**link**
28 August 2025	Large-scale ransomware attack on IT supplier	**link**
17 December 2025	Confidential data compromised due to cyberattack	**link**
18 February 2026	Breach of data related to law enforcement agents	**link**

Annex 4

Registration in the European Cybersecurity Competence Community

(not mandatory)

Pursuant to Article 8 of Regulation (EU) 2021/887, entities participating in actions under this call are encouraged to contribute to the European Cybersecurity Competence Community (the Community). The Community brings together stakeholders from industry, including SMEs, academia, research organisations, public authorities, civil society organisations, European standardisation organisations and other entities with relevant cybersecurity expertise, with the objective of strengthening cooperation and cybersecurity capacities across the Union.

Entities established in an EU Member State may apply to become members of the Community by submitting an application through their respective National Coordination Centre (NCC)[41]. Following the assessment by the relevant NCC, successful applicants are registered as members of the Community by the European Cybersecurity Competence Centre (ECCC).

Information on the registration process, including the eligibility criteria, application procedure and the role of the National Coordination Centres, is available.

Even though membership to the Community is **not required**, applicants are encouraged to apply for membership through the National (NCCs) and attach proof of the request to the application.

In order to do so, applicants shall provide:

- A declaration signed by the Coordinator, confirming that they have submitted an application to join the European Cybersecurity Competence Community through their respective National Coordination Centres (NCCs).

Template Declaration on the submission of applications to the European Cybersecurity Competence Community

Declaration on the submission of applications to the

European Cybersecurity Competence Community

Proposal Acronym/Number: [Proposal Acronym] [Proposal Number]

Call Reference: [Call Identifier]

Declaration

I, the undersigned, acting as the authorised representative of the Coordinator of the above-mentioned proposal, hereby declare, on behalf of the consortium, that:

1. All beneficiaries participating in this proposal have submitted an application to join the European Cybersecurity Competence Community, in accordance with Article 8 of Regulation (EU) 2021/887.

[41] https://cybersecurity-centre.europa.eu/nccs-0_en

2. Each beneficiary has submitted its application through its respective National Coordination Centre (NCC), in accordance with the applicable registration process.

3. The information provided in this declaration is true, complete and accurate to the best of my knowledge.

Coordinator Organisation:
[Legal name]

Name of authorised representative:
[Full name]

Position:
[Job title]

Place and Date:
[City], [Date]

Signature: