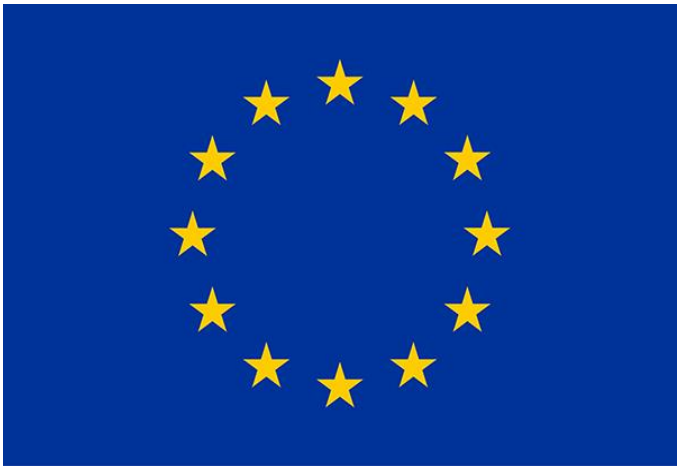

Digital Europe Programme (DIGITAL)

Call for proposals

Deployment Actions in the area of Cybersecurity

(DIGITAL-ECCC-2024-DEPLOY-CYBER-06)

Version 1.0
18 December 2023

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	18.12.2023	▪ Initial version (new MFF).	
		▪	
		▪	
		▪	

EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

CNECT.H– Digital Society, Trust and Cybersecurity
CNECT.H.1 Cybersecurity Technology and Capacity Building

CALL FOR PROPOSALS

TABLE OF CONTENTS TABLE OF CONTENTS

0. Introduction

This is a call for proposals under the **Digital Europe Programme (DIGITAL)**.

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

- Regulation 2018/1046 (EU Financial Regulation)
- the basic act (Digital Europe Regulation 2021/694[1]).

The call is launched in accordance with the 2023-2024 Work Programme[2] and will be managed by the **European Commission, Directorate-General for Communication, Networks, Content and Technology (DG CONNECT) on behalf of the European Cybersecurity Competence Centre (ECCC), until the ECCC has the capacity to implement its own budget.**

The call covers the following **topics**:

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres**
- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations**

[1] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe programme for the period 2021-2027 (OJ L166, 11.05.2021).

[2] Commission Implementing Decision C(2023) 8620 of [15.12.2023] concerning the adoption of the work programme for 2023-2024 and the financing decision for the implementation of the Digital Europe Programme.

- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-SEC-CRATOOLS - Tools for compliance with CRA requirements and obligations**
- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors**
- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD - Standardisation and awareness of the European transition to post-quantum cryptography**
- **DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS - Roadmap for the transition of European public administrations to a post-quantum cryptography era**

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.

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)*.

1. Background

Digital technologies are profoundly changing our daily life, our way of working and doing business, the way we understand and use our natural resources and environment and the way we interact, communicate and educate ourselves. The critical role of digital technologies and infrastructures, and the interdependencies in our societies and economies, have recently been demonstrated by disruptive events such as the COVID-19 crisis and Russia's war of aggression against Ukraine. These crises have confirmed how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world. Malicious cyber activities not only threaten our economies but also our way of life, our freedoms and values and even try to undermine the cohesion and functioning of our democracy in Europe.

The second Work Programme (WP) Cybersecurity of the Digital Europe Programme 2023-2024 responds to a two-fold challenge. It ensures the continuation and evolution of actions started in the first Work Programme Cybersecurity 2021-2022 (notably the support for National Coordination Centres), while simultaneously introducing actions that further develop the EU's cybersecurity capabilities and enhance its resilience in the context of the EU Cybersecurity Strategy.

Actions included in this call document will in particular support the objectives indicated below.

- Actions in order to create an advanced (state of the art) threat detection and cyber incident analysis ecosystem by building capacities of Security Operation Centres (SOCs), in particular by supporting enabling technologies.
- Actions to support the implementation of the proposed Cyber Resilience Act (CRA)[3], in particular with regards to strengthen their cybersecurity capacities of European SMEs.
- Actions enabling the adoption to post-quantum cryptography (PQC) in industrial sectors, strengthening Europe's efforts on the transition to PQC by supporting European and international standardisation activities and developing a roadmap for the transition of public administrations to post-quantum cryptography PQC.
- All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation. Those topics cover EU capacities in quantum communication, an emerging field that will be of high strategic value in the development and deployment of secure communication and secure data, applications and services, and which will enable the EU and its Member States to safeguard sensitive governmental data and critical infrastructures against potential interference.

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

[3] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres

Objectives

This topic addresses enabling technologies (such as AI) for SOCs, including National SOCs which provide a central operational capacity and support other SOCs at national level and play a central role as a hub within a context of SOCs, and also Cross-border SOC platforms where such technologies can strengthen capacities to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats.

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

Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity, based on enabling technologies (such as AI), addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that indicate potential threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape.
- 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 and management of vulnerabilities.
- 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 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 and de-identification. Tool and service providers are welcome to apply to this topic, also when in a consortium with National SOCs. 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.

Tool and service providers are welcome to apply to this topic, also when in a consortium with National SOCs. Links with stakeholders in the area of High-Performance Computing should be made where appropriate. 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 licencing to National and/or Cross-Border SOC platforms under favourable market conditions.

These actions aim at creating or strengthening national and/or cross-border SOCs, which occupy a central role in ensuring the (cyber-)security of national authorities, providers of critical infrastructures and essential services. SOCs are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of SOCs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, SOCs must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt 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 relating to SOCs are subject to Article 12(5) of Regulation (EU) 2021/694, in consistency with WP 2021/2022.

Outcomes and deliverables

- Deployment of Artificial Intelligence and Advanced Key Technologies as enablers for SOCs
- Tools for creation, analysis and processing of CTI that allow for faster and more scalable SOC operations
- Original European CTI feeds or services

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of entities benefitting from funded entities.
- Intensity of exchange of information between funded entities.
- Number of AI services and enabling technologies deployed for rapid detection of cybersecurity incidents and more effective decision making.
- Number of activities organised for collaboration, communication, awareness raising or knowledge exchange and training (on the implementation of the AI tools and services).

Targeted stakeholders

- The target stakeholders are public and private actors, as well as consortia of either kind or combining them, which can support cyber threat detection and CTI sharing.

- National authorities may associate themselves with private providers of technology services or equipment, in particular European SMEs, possibly in cooperation with network and technology providers, to pilot and develop security and interoperability aspects of innovative solutions, such as open, disaggregate and interoperable solutions.

Type of action and funding rate

Simple grant — 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-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations

Objectives

The objective of this topic is to support European SMEs, with a focus on micro and small enterprises, to strengthen their cybersecurity capacities and to support the implementation of the proposed Regulation on the Cyber Resilience Act (CRA).

Scope

In synergy with other actions launched under this WP which will be developing compliance tools for the CRA, the action should distribute cascade financing grants to European SMEs, with a focus on micro and small enterprises, though remaining open to other stakeholders, to support achieving compliance with requirements and obligations stemming from the CRA.

Applicants are encouraged to identify categories of cascade financing recipients, including at least the following:

- Manufacturers of products with digital components, including software developers.

- Providers of tools and solutions that facilitate compliance with CRA obligations.
- Other well-justified categories in line with CRA (e.g., distributors, importers, open-source community).

For each identified stakeholder category, a dedicated set of activities should be devised taking into consideration the specific needs of target consumers, business users, and other relevant stakeholders.

The proposed project should include actions addressing the following:

- Awareness raising, dissemination and other stakeholder engagement actions with the focus on the cascade financing to European SMEs, with a focus on micro and small enterprises.
- Managing an open call process to distribute cascade funding, including impartial evaluation of proposals and monitoring the implementation of grants.
- Establish an openly available platform providing links to CRA-related resources that the proposed project itself would collect or develop or which would be available from external sources and supporting community building and upskilling. This includes for example a dedicated central repository website to allow easy finding of internal and external resources, step-by-step guidelines, compliance tools, training materials, free and open-source code implementations, and other relevant resources to achieve CRA compliance. This should include, amongst others, tools procured for this purpose under this work programme.
- In close coordination with the EU Cybersecurity Skills Academy, perform trainings and upskilling of stakeholders to achieve CRA compliance, i.e. organise workshops, training sessions, and events, draft guidelines, supporting actions to facilitate interaction among European SMEs, including drafting reports or other material discussing the implementation of CRA compliance requirements and promoting awareness, including by contributing to relevant deliverables of standardisation bodies e.g. through a sectoral perspective and informed by the needs of companies on the ground.
- Facilitate and share CRA compliance best-practices and use-cases.
- Contribute to standardisation efforts, as appropriate, considering the activities of European and international standardisation that are directly relevant to the CRA implementation.

Third parties receiving grants should, in particular:

- Engage in testing, detecting and addressing vulnerabilities, producing documentation, carrying out conformity assessment and implementing other measures necessary to comply with the CRA.
- Participate in workshops, training sessions, and events that facilitate interaction among European SMEs, with a focus on micro and small enterprises, to discuss and implement CRA compliance.

- Contribute to the proposed project's efforts in collecting the needs and perspectives of SMEs towards CRA-related standardisation deliverables.

Priority should be given to solutions available to use free of charge or free and open-source software (FOSS) solutions both when setting up the openly available platform and when distributing cascading finance grants.

These activities should be carried out in close coordination, and where possible collaboration, with the European Cybersecurity Competence Centre (ECCC), the Network of National Coordination Centres (NCCs), the European Digital Innovation Hubs (EDIHs) network, other relevant European and National cybersecurity entities, and other projects of this work programme.

The operational involvement of NCCs in implementing and running such actions is strongly recommended.

Indicatively one proposal is expected to be financed via this topic. Proposed projects should foresee at least 75% of the budget to be distributed for cascade financing grants.

This action includes the creation of a central platform that serves as a reference point, and hence will enable interactions between providers of essential services and critical infrastructures, as well as other actors, regarding their cybersecurity measures and possible vulnerabilities. Also third parties receiving funding will engage in solutions for testing, detecting and addressing vulnerabilities. As such information could be exploited by malicious actors, the central entity handling such must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt 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 relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- Financial support for SMEs and other stakeholders for CRA compliance.
- Openly available platform with CRA-related resources (such as guidelines and supporting documents), providing supporting community building and upskilling.
- Workshops, events, networking and exchange of experience of stakeholders.
- Contributions to CRA standardisation.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of SMEs and other entities benefitting from cascade financing.
- Number of awareness raising, dissemination and other stakeholder engagement activities.
- Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs.
- Number of CRA implementation supporting white papers, discussion papers, audio-visual and/or training didactic material, step-by-step guidelines, compliance tools, free and open-source code implementations, and other relevant resources to support CRA compliance published.
- Number of risk assessment/monitoring services provided.
- Number of visitors of the online platform per month.
- Number of CRA related compliance use-cases identified and related best-practices developed and disseminated.
- Number of standardisation work items, contributions, discussion papers or others directly relevant for the development of harmonised standards for CRA.

Targeted stakeholders

- This topic targets in particular national cybersecurity authorities, national cybersecurity competence centres, National Coordination Centres (as defined in Regulation (EU) 2021/887), private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries, to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties by attracting SMEs. 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

Grant for Support to Third Parties — 100% funding rate for the consortium, co-financing of 50% by the supported third

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)*
- For this topic, financial support to third parties is compulsory *(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-2024-DEPLOY-CYBER-06-CRATOOLS - Tools for compliance with CRA requirements and obligations

Objectives

The objective of this topic is to support the implementation of the proposed Cyber Resilience Act (CRA) through tools that support, and where possible automate, internal compliance procedures, including testing and specification drafting with focus towards European SMEs, in particular micro and small enterprises.

Scope

This action aims at the design and development of tools to facilitate, and where possible automate, CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements and documentation obligations.

CRA compliance solutions are foreseen based either on technical specifications, training modules, and/or other relevant material. Tools for penetration testing, testing facilities and other cybersecurity practices, aligning with CRA requirements, are also in the scope.

Tools should be tailored towards needs of European SMEs, with a focus on micro and small enterprises, though also usable by broader stakeholder categories, such as:

- Manufacturers of relevant product categories falling within the scope of the CRA, including software developers.
- Others, such as distributors, importers, open-source community, etc.

CRA compliance tools should be made widely available on fair and reasonable terms and also take into consideration the specific needs of different stakeholders such as the behaviour of consumers, business users, and other relevant factors.

Priority should be given to solutions available to use free of charge or free and open-source software (FOSS) solutions.

These activities should be carried out in close coordination and, where possible collaboration, with the Network of National Coordination Centres (NCCs), the European Digital Innovation Hubs (EDIHs) network, the EU Cybersecurity Skills Academy, other relevant European and National cybersecurity entities, and other projects of this work programme.

This action aims at the creation of tools that, amongst others, do penetration testing or document technical specifications with relation to cybersecurity, including for entities that are providers of essential services and critical infrastructures. As such

tools and information could be exploited by malicious actors, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt 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 relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- Tools to simplify and automate CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements.
- Tools to simplify and automate CRA compliance documentation obligations.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals should include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of tools to facilitate and automate CRA compliance.
- Number of CRA essential requirements fully covered by tools.
- Number of CRA essential requirements partially covered by tools.
- Number of tools to simplify and automate CRA compliance documentation obligations.
- Number of awareness raising, dissemination and other stakeholder engagement activities.
- Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs.
- Number of CRA compliance use-cases and best-practices.
- Number of prospective companies which will benefit from tools developed by the project, of which SMEs.
- Number of prospective products and end-users benefiting from the tools.

Targeted stakeholders

This topic targets in particular European SMEs but other applicants are not excluded.

Type of action and funding rate

SME support action grants — 50% of total eligible costs except for SMEs where a rate of 75% applies.

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 addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*
  - extent to which the project would reinforce and secure the digital technology supply chain in the Union*

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors

Objectives

The objective is to enable the adoption of PQC in industrial sectors like automotive, automation, finance, control systems or energy. The overarching aim is to seamlessly integrate PQC systems, equipment, components, protocols, and network technologies into existing digital security and communication networks.

Scope

Proposals should focus on the integration of a standardised PQC protocol into the digital security and communication networks in the automotive, automation, finance, or energy sector, while taking into account specific needs of the sector, such as necessary keys strength and keys management. Proposals should cover the development or adaptation of the required software/hardware and the validation of the solution in a large-scale demonstrator. This includes creating an inventory of assets requiring protection with a quantified level of risk, a migration plan[4] for both the migrating entities and their suppliers and customers, taking into account data protection policies, contributing to the development of standards and certification. Successful consortia are expected to raise awareness on the need to transition to PQC and share their experience and best practice.

This action aims at the creation of a technology that will be used to protect the cybersecurity of critical industrial assets with a new paradigm that is set to be a game changer in encryption. The control of such tools is of utmost importance for governments and industry alike, as they could be exploited by malicious actors. As such, they must be protected against possible dependencies and vulnerabilities in

[4] See for example https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

cybersecurity to pre-empt foreign influence and control. 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 relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- PQC system validation and PQC technology ready for wide-spread deployment in given industrial sectors
- Long-term protection of critical assets, long-term information security and operational continuity in the advent of quantum computers
- Migration checklists and plans for PQC in sectors where this has not yet taken place.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of entities benefitting from funded entities.
- Intensity of exchange of information between funded entities.
- Number of developed or adaptated PQC services.
- Number of activities organised for awareness raising and best practises on the need to transition to PQC.

Targeted stakeholders

- This topic targets Post Quantum Cryptography stakeholders, industrial players, including SMEs and start-ups, and relevant actors that play a role in the PQC integration and standardisation process.

Type of action and funding rate

Simple grant — 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-2024-DEPLOY-CYBER-06-PQCSTANDARD -Standardisation and awareness of the European transition to post-quantum cryptography

Objectives

Proposals should aim to strengthen Europe's efforts on the transition to PQC by supporting European and international standardisation activities, delivering a comprehensive European PQC industrial migration roadmap and raise awareness regarding PQC endeavours. This should be achieved in particular through the following strategic actions:

- Organisation of events, workshops, stakeholder consultations, and production of white papers to fostering the development of harmonised standards on PQC.
- Support for participation of relevant European experts in European and international standardisation fora relating to PQC.
- Community-Based PQC Migration Roadmap: Foster a collaborative process involving research and industry stakeholders to formulate a robust European PQC migration roadmap, which can be the basis for sector-specific roadmaps.
- Widespread Dissemination of PQC Outcomes: Promote broad awareness and understanding of European PQC achievements through extensive dissemination efforts spanning various platforms, including social media. This includes outreach events and structured dialogues with the general public, exploring ethical and societal dimensions of PQC, especially in terms of privacy, security, public trust, and acceptance.
- Research Dissemination Services: Provide specialised dissemination services targeting relevant communities, such as European cybersecurity providers and users, effectively sharing research insights.
- Identifying Training and Infrastructure Needs: Identify crucial requirements for training, education, and infrastructure to advance PQC development.

Scope

Proposals are expected to engage in concrete standardisation efforts within both European and international standardisation forums, where PQC will play a pivotal role in the near future and where progress in standardisation will augment existing cybersecurity capabilities and create a competitive edge upon Europe. Also, in alignment with projects resulting from the topic "Transition to Quantum-Resistant Cryptography" (call HORIZON-CL3-2022-CS-01-03) and the topic Deployment of Post-Quantum Cryptography (PQC) systems in industrial sectors (in this work programme), the proposals will incorporate practical strategies to coordinate and

synergise European research and innovation endeavours with PQC standardisation initiatives.

To this end, proposals should establish a proactive presence and take on leadership roles in orchestrating and shaping international standards and regulations for PQC. This can either be in existing standardisation activities and bodies or, where relevant, by contributing to creating new standardisation activities in existing groups and/or creation of new groups.

Proposals should cultivate a cohesive European PQC community, fostering collaboration among academic and industrial stakeholders, and engage in a structured dialogue on various fora. This will entail harmonising activities across European, national, and regional programs and projects, and pave the way for synergetic innovation efforts in PQC to help unlock use-cases for practical cybersecurity applications in Europe.

Proposals should bring together key stakeholders across the entire PQC value chain. This holistic approach should encompass researchers, standardisation experts and representatives from industry sectors. A comprehensive outline should be provided in the proposal, detailing the stakeholders to be engaged and the methodologies to efficiently coordinate their efforts at the European level in order to achieve impactful outcomes that effectively promote European interests in PQC standardisation.

Furthermore, the proposals will strive to establish constructive dialogues with international PQC programmes and promote international cooperation activities. Emphasis should be placed on collaborative exchanges between key international participants, including the EU and countries such as the USA, exploiting complementary strengths and challenges and fostering mutually beneficial outcomes in standardisation efforts.

This action aims at supporting stakeholders dealing with technologies that will be used to protect the cybersecurity of critical industrial assets with a new paradigm that is set to be a game changer in encryption. The control of such tools is of utmost importance for governments and industry alike, as they could be exploited by malicious actors. As such, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. 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 relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

- Contributions to European and international standards and regulations in PQC.
- Workshops, white papers and other activities to support synergies between different sectors transition to PQC.
- A European PQC migration roadmap, which can be the basis for sector-specific roadmaps.
- Actions supporting the European PQC community.
- Development of standards for hybrid cryptographic systems (pre- and postquantum encryption systems) for encryption, key encapsulation mechanisms, digital signatures, etc. and for the PQC integration in the existing digital infrastructure.
- Support for participation of relevant European experts in European and international cross-topical standardisation bodies in order to integrate PQC

whenever new cryptographic standards are developed or existing ones are updated especially for critical sectors like energy, transport, health, and finance.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Number of events, workshops, stakeholder consultations, and white papers to fostering the development of harmonised standards on PQC.
- Number of European and international standardisation activities involved in.
- Number of awareness raising, dissemination and other stakeholder engagement activities.
- Number of Research Dissemination Services targeting relevant communities (such as European cybersecurity providers and users).
- Number of education and training activities to advance PQC development.
- Number of active collaborations implemented with other relevant initiatives or European players and projects.

Targeted stakeholders

- This topic targets PQC standardisation stakeholders (within both European and international standardisation forums), industrial players, including SMEs and start-ups, and relevant actors that play a role in the PQC standardisation process.

Type of action and funding rate

Coordination and support action grant — 100% 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 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-2024-DEPLOY-CYBER-06-PQCTRANS - Roadmap for the transition of European public administrations to a post-quantum cryptography era

Objectives

Proposals should foresee a leading role for national security agencies in developing a roadmap for the transition of public administrations to post-quantum cryptography PQC. This should take into account an inventory of systems to be replaced, the timeframe, and technical and legal aspects of the migration to PQC in public administrations. It should be achieved in particular through the following strategic actions:

- Foster a collaborative process involving stakeholders from national security agencies and other public administrations to discuss priorities, technical challenges, legal obstacles and other issues relating to the transition to PQC.
- Promote awareness among public administrations of the need to make the transition to PQC.
- Identify crucial requirements and establish a coordinated roadmap for the transition of European public administrations to PQC.

Scope

Proposals should bring together national security agencies, relevant public administrations and related stakeholders including experts in the area of PQC. Activities should be foreseen to engage stakeholders to efficiently coordinate their efforts at national and European level in order to achieve impactful outcomes leading to the adoption of PQC in European public administrations.

The roadmap should identify what encryption systems need to be replaced, what algorithms should be adopted, priorities for defending against quantum attacks across the spectrum of public administrations, and legal and technical aspects of the transition to PQC. It should foster collaborations and exchange of best practice.

This action aims at the transition of public administration towards a new paradigm that is set to be a game changer in encryption, which directly involves national security as it relates to information that must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control. 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 relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

Outcomes and deliverables

Proposals are expected to deliver on at least two of the following results:

- Roadmap for the transition of European public administration for PQC
- Workshops, white papers and other activities to support synergies between national security agencies and public administrations.

- Collaborations between public administrations regarding the transition to PQC.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- Roadmap for the transition of European public administration for PQC.
- Workshops, white papers and other activities to support synergies between national security agencies and public administrations.
- Number of collaborative activities involving stakeholders from national security agencies and other public administrations regarding the transition to PQC.
- Number of awareness raising, dissemination and other stakeholder engagement activities among public administrations of the need to make the transition to PQC.

Targeted stakeholders

- This topic targets in particular stakeholders from national security agencies and other public administrations in developing a roadmap for the transition of public administrations to post-quantum cryptography PQC.

Type of action and funding rate

Coordination and support action grant — 100% 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 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 84.000.000**. Specific budget information per topic can be found in the table below:

Topic	Topic budget
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH **Novel applications of AI and Other Enabling Technologies for Security Operation Centres**	**EUR 30.000.000**
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA **Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations**	**EUR 22.000.000**
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-CRATOOLS **Tools for compliance with CRA requirements and obligations**	**EUR 8.000.000**
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY **Deployment of Post Quantum Cryptography in systems in industrial sectors**	**EUR 22.250.000**
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD **Standardisation and awareness of the European transition to post-quantum cryptography**	**EUR 1.000.000**
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS **Roadmap for the transition of European public administrations to a post-quantum cryptography era**	**EUR 750.000**

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:	16 January 2024
Deadline for submission:	26 March 2024 – 17:00:00 CET (Brussels)
Evaluation:	April 2024
Information on evaluation results:	May 2024
GA signature:	November 2024

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 Search Funding & Tenders section). Paper submissions are NOT possible.

Proposals (including annexes and supporting 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 *(to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded)*
- **mandatory annexes and supporting documents** *(to be uploaded)*:
  - detailed budget table: not applicable
  - CVs of core project team: not applicable
  - activity reports of last year: not applicable
  - list of previous projects: not applicable
  - **ownership control declaration: applicable**

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 the 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**.

Proposals are limited to maximum

70 pages (part B) for topics:

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH - Novel applications of AI and Other Enabling Technologies for Security Operation Centres

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA - Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-SEC-CRATOOLS - Tools for compliance with CRA requirements and obligations

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY - Deployment of Post Quantum Cryptography in systems in industrial sectors

50 pages (part B) for topics:

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD - Standardisation and awareness of the European transition to post-quantum cryptography

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS - Roadmap for the transition of European public administrations to a post-quantum cryptography era

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[5] 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 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)*.

Specific cases

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[6].

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'[7]. ⚠ 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).

EU restrictive measures — Special rules apply for certain entities *(e.g. 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)[8] and entities*

[5] Except for entities that are validated as public bodies by the Central Validation Service.
[6] See Article 197(2)(c) EU Financial Regulation 2018/1046.
[7] For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.
[8] 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.

covered by Commission Guidelines No 2013/C 205/05[9]). 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).

Following the Council Implementing Decision (EU) 2022/2506, as of 16th December 2022, no legal commitments (including the grant agreement itself as well as subcontracts, purchase contracts, financial support to third parties etc.) can be signed with Hungarian public interest trusts established under Hungarian Act IX of 2021 or any entity they maintain.

Affected entities may continue to apply to calls for proposals. However, in case the Council measures are not lifted, such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties). In this case, co-applicants will be invited to remove or replace that entity and/or to change its status into associated partner. Tasks and budget may be redistributed accordingly.

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

Consortium composition

For all other topics:

- no restrictions.

Eligible activities

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)*.

Financial support to third parties is mandatory in DIGITAL-ECCC-2024-DEPLOY-CYBER-06- STRENGTHENCRA (Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations) 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

[9] Commission guidelines No 2013/C 205/05 on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

- 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.

For other topics, Financial Support to Third Parties is not allowed.

Your project application must clearly specify why financial support to third parties is needed, how it will be managed and provide a list of the different types of activities for which a third party may receive financial support. The proposal must also clearly describe the results to be obtained.

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[10] 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

[10] 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).

- 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
- 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 these 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[11]:

- 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)

11 See Articles 136 and 141 of EU Financial Regulation 2018/1046.

- guilty of grave professional misconduct[12] (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)
- 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).

Applicants will also be refused if it turns out that[13]:

- 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** (composed or 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:

[12] Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

[13] See Article 141 EU Financial Regulation 2018/1046.

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'. When these scores are equal, priority will be based on their scores for the criterion 'Implementation'.

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 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. 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 are 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. Retroactive

application can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration:

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH Novel applications of AI and Other Enabling Technologies for Security Operation Centres the indicative duration of the action is 36 months, but other durations are not excluded.

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations the indicative duration of the action is 36 months, but other durations are not excluded.

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-CRATOOLS Tools for compliance with CRA requirements and obligations the indicative duration of the action is 12 to 18 months, but other durations are not excluded.

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY Deployment of Post Quantum Cryptography in systems in industrial sectors the indicative duration of the action is up to 36 months, but other durations are not excluded.

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD Standardisation and awareness of the European transition to post-quantum cryptography the indicative duration of the action is up to 36 months, but other durations are not excluded.

For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS Roadmap for the transition of European public administrations to a post-quantum cryptography era the indicative duration of the action is 36 months, but other durations are not excluded.

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

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.

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 (maximum grant amount):

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH Novel applications of AI and Other Enabling Technologies for Security Operation Centres: indicatively between 3 and 5 million per project but other amounts are not excluded.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations: EUR 22 million per project.

- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-CRATOOLS Tools for compliance with CRA requirements and obligations: indicatively between 2 and 3 million per project but other amounts are not excluded.
- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY Deployment of Post Quantum Cryptography in systems in industrial sectors: indicatively between EUR 5 million and EUR 7 million per project but other amounts are not excluded.
- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD Standardisation and awareness of the European transition to post-quantum cryptography: EUR 1 million per project.
- For topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS Roadmap for the transition of European public administrations to a post-quantum cryptography era: EUR 0,75 million per project.

The grant awarded may be lower than the amount requested. **The minimum budget for each topic as listed above is strongly recommended.**

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 topics XX)
- 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): Yes
  - SME owner/natural person unit cost[14]: Yes
- travel and subsistence unit costs[15]: No (only actual costs)
- equipment costs:
  - depreciation (for topic DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD and DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCTRANS)
  - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH, DIGITAL-ECCC-2024-DEPLOY-CYBER-06-, DIGITAL-ECCC-2024-DEPLOY-CYBER-06-SECCRATOOLS, DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY)
- other cost categories:
  - costs for financial support to third parties: allowed for grants:
    - for topics DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA (Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations): maximum amount per third party EUR 150 000, unless a higher amount is required because the objective of the action would otherwise be impossible or overly difficult to achieve and this is duly justified in the Application Form.
      - Proposals should foresee at least 75% of the project budget for this cost category.
      - Recipients of financial support to third parties are required to co-finance the activity by minimum 50% of the total costs of the activity.
- internally invoiced goods and services (costs unit cost according to usual cost accounting practices): 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 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:

[14] 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)7715).

[15] 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).

- 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
  - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible
- 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 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 payments will be made to the coordinator.

 Please be aware that payments will be automatically lowered if 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

- limitations to transfers and licensing: Yes

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 communication activities: Yes
- special logo: both EU and Cybersecurity Competence Centre logo.

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

n/a

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 Search Funding & Tenders 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 might 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
- FAQs on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- 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.

Non-IT related questions should be sent to the following email address: CNECT-ECCC-DEP@ec.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 going 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).
- **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. If you would like to nonetheless benefit from different EU funding opportunities, 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*).

- **Transparency —** In accordance with Article 38 of the EU Financial Regulation, information about EU grants awarded is published each year on the Europa website.

  This includes:

  - beneficiary names
  - beneficiary addresses
  - the purpose for which the grant was awarded
  - the maximum amount awarded.

  The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection —** The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the Funding & Tenders Portal Privacy Statement.

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%

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)[16].

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[17] 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 DEP, HE, EDF and CEF-DIG restricted calls)*.

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.

Thus:

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

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

- 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[18].

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 DEP, HE, EDF and CEF-DIG restricted calls*.

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