



Cybersecurity Intelligence,
Protection, and Holistic
Enterprise Resilience

Annex 1 - Guide for Applicants

Open Call 1

Nov 2026



Funded by
the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Disclaimer

The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Copyright Notice

© CIPHER

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732.

Contents

1	What is CIPHER	4
2	What does CIPHER – OpenCall 1 offer?	4
3	Who can apply and how?	5
3.1	Types of applicants.....	5
3.1.1	Eligible applicants.....	5
3.1.2	Eligible countries.....	6
3.1.3	Multiple submissions.....	6
3.2	Types of projects.....	6
3.3	Funding conditions.....	9
3.4	Application process	10
	Application Documentation Package.....	10
	Guidance on the CIPHER FSTP Budget Template.....	12
3.5	Other application requirements and considerations.....	12
3.6	Technical/ feasibility assessment.....	13
3.7	Cut-offs or Open Call closure.....	13
4	How will applications be evaluated and selected?	14
4.1	Eligibility check.....	14
4.2	In/out challenge and ecosystem scope check.....	14
4.3	Expert evaluation.....	15
4.3.1	Evaluation criteria & scoring.....	15
4.3.2	Ranking & selection.....	17
4.4	Appeals.....	18
5	What happens after selection?	19
6	What is CIPHER - OC1 and what are its requirements?	20
6.1	Programme Sprints.....	20
6.1.1	Sprint 1: Onboarding and Pre-financing (Months M0–M1 Duration: 1 Month).....	20
6.1.2	Sprint 2: Technical Execution, Pipeline Integration & Initial Testing (Months M2–M5 Duration: 4 Months).....	20
6.1.3	Sprint 3: Full Validation, Refinement, Demonstration & Final Reporting (Months M6–M9 Duration: 4 Months).....	21
6.2	Programme review.....	21
6.2.1	Review summary.....	21
7	What else is important to know?	23
7.1	Intellectual Property Rights (IPR).....	23
7.2	Conflicts of interest.....	23

7.3	Ethical issues.....	23
7.4	Data protection.....	23
7.5	Confidentiality.....	24
7.6	Promotion of the action and ensuring visibility of the EU funding	24
7.7	Checks and reviews.....	24
7.8	Relevant links and contacts.....	25
8	Relevant Open Call definitions	26

Tables

Table 1: Challenges of CIPHER - OpenCall 1	7
Table 2: Application Process and Timeline	10
Table 3: 3.4.1.1 References and templates provided by CIPHER	10
Table 4: Submission Phase Documents (Mandatory at Proposal Submission)	11
Table 5: Contracting Phase Documents (Selected Beneficiaries Only)	11
Table 6: Scoring Criteria	15
Table 7: Target Applicants per Challenge	17
Table 8: Sprint Requirements	21
Table 9: Acronyms & Definitions	26
Table 10: Terms & Definitions	26

Figures

Figure 1: Evaluation and selection process	13
--	----

1 What is CIPHER

The CIPHER project (Cybersecurity Intelligence, Protection, and Holistic Enterprise Resilience) is a European initiative that aims to strengthen security and information assurance across critical infrastructure sectors like transport, telecommunications, and water management. To achieve this, the project is developing a collaborative, standardized, and "available-as-a-service" testing facility and experimentation laboratory. This platform allows operators and authorities to evaluate their cybersecurity risk governance, test cutting-edge solutions, and validate complex threat scenarios in a secure, production-like cyber-range environment.

The platform dynamically integrates multi-attribute risk assessments, automated penetration testing, and AI-driven threat forecasting to continuously monitor asset vulnerability surfaces and detect anomalies. Backed by a €4.32 million cascade funding scheme, CIPHER actively engages external startups, SMEs, and security consultants through open calls to deploy, refine, and validate these advanced capabilities in real-world settings.

For more information, please visit the official project website at <https://cipher-eu.com/>.

2 What does CIPHER – OpenCall 1 offer?

The *Open Call* is the competitive process by which eligible applicants seek admission to the CIPHER programme.

Applications to the Open Call will be accepted from 26th October 2026 until 6th January 2027. After the selection is completed, successful applicants will be invited to sign the sub-grant agreement and enter the CIPHER Programme.

The CIPHER Programme is organised in 3 sprints, as follows:

- Sprint 1 from Apr 2027 to May 2027
- Sprint 2 from Jun 2027 to Sep 2027

- Sprint 3 from Oct 2027 to Dec 2027.

During these phases, beneficiaries will be assigned a mentor to support and monitor project progress and facilitate communication with technical partners. Each selected project may receive up to 60,000€ in funding, distributed in three instalments:

- 20% (€12,000) upon first onboarding report completion at M1 (Sprint 1),
- 40% (€24,000) upon completion and approval of second deliverable at M5 (Sprint 2)
- 40% (€24,000) upon completion and approval of third and final deliverable at M9 (Sprint 3)

Relevant links and contacts

- Project website: <https://cipher-eu.com/>
- Open call application form: www.f6s.com/cipher-opencall1
- Contact us: info@cipher-eu.com

3 Who can apply and how?

3.1 Types of applicants

CIPHER – OpenCall 1 is looking for Technology Adopters/ Developers/ Integrators to develop/ adopt/ test innovative cybersecurity solutions, components, or experiments in the framework of the CIPHER project.

Additionally, OpenCall 1 is looking for Certified Auditors with demonstrable NIS2 compliance-assessment experience in critical sectors to assess CIPHER's toolset against the Article 21(2) risk-management measures (OT-prioritised sectors).

3.1.1 Eligible applicants

Eligible applicants for CIPHER - OpenCall 1 are:

- Legal entities or consortia of legal entities, which can be startups and micro-SMEs; SMEs; mid-caps; research organisations, higher education institutions (RTOs or academia) established in EU Member States (including overseas countries and territories) or EEA countries (Norway, Iceland, and Liechtenstein).
- In the case of consortium-type applications, the consortium must be composed of maximum 3 (three) independent legal entities representing complementary roles:
 - Technology Provider (Mandatory): Startups, Tech SMEs, Research Centres, or Academia responsible for technical developments.
 - End-User / Technology Adopter (Mandatory): SMEs, Infrastructure Operators, or Associations responsible for validating developments in real-case settings.
 - Certified Cybersecurity Auditor / Compliance Assessor (Optional): Certified auditing bodies responsible for assessing tools, testing methodology, NIS2 alignment, and governance frameworks.

Relevant notes:

- Please consult the [EU SME Definition](#) for details on what constitutes an SME.
- A signed version of the Declaration of Honour and the SME Declaration will be requested during the contract preparation phase.
- All applicant's (consortium partners) are required to have a **PIC number**. PIC is a 9-digit Participant Identification Code. Please see [here](#) to register and consult further.

Ownership and Control Restrictions: In accordance with EU Financial Regulation Article 136 and Eligibility restrictions under Articles 12(5) and (6) and 18(4) of the Digital Europe Regulation, CIPHER OpenCall 1 enforces strict ownership and control restrictions to protect EU strategic security interests.

- **Mandatory Declaration:** All applicants (whether applying as a single entity or as a consortium partner) must complete and submit the Ownership Control Declaration (Annex 4) as part of their proposal application.
- **Qualified electronic Signature Requirement:** The declaration must be signed by an authorized legal representative using a qualified electronic signature (QES) recognized under Regulation (EU) 910/2014 (eIDAS)
- **Public Body Exemption:** Public bodies formally validated as such in the EC Funding & Tenders Portal Participant Register are automatically considered EU-controlled and are exempt from submitting the Ownership Control Declaration.
- **Definition of Control:** "Control" is defined as the possibility to exercise decisive influence over the applicant, directly or indirectly through intermediate entities (*de jure* or *de facto*), notably regarding strategic business decisions (e.g., senior management appointments, budget approval, IPR, technology transfer, or veto rights).
- **Continuity of Requirement:** Ownership and control conditions must be fulfilled at the proposal submission deadline and maintained throughout the entire project implementation. Any changes in ownership or foreign shareholding during the project must be reported immediately to the CIPHER Consortium. Non-compliance or unauthorized foreign control acquired during the project will lead to termination and grant reduction.
- **Ownership and Control Assessment Procedure:** All submitted Ownership Control Declarations will be subject to an ownership and control assessment conducted by the CIPHER Consortium in accordance with the Ownership and Control Assessment (OCA) Procedure. The procedure establishes the methodology, assessment criteria, supporting evidence requirements, review process, and decision-making framework used to determine applicants' compliance with the ownership and control restrictions applicable to this Open Call. Applicants may be requested to provide additional supporting documentation, clarifications, or evidence where necessary to enable the assessment.

3.1.2 Eligible countries

Legal entities from following eligible countries may receive funding through this Open Call:

- European Union Member States (including overseas countries and territories), with a valid VAT number.
- EEA countries (Norway, Iceland, and Liechtenstein)

- CIPHER - OpenCall 1 follows the rules applied by the EC for the DIGITAL-ECCC-2024-DEPLOY-CYBER-07 Europe in terms of geographical coverage, eligibility, and exclusions, which take precedence.

3.1.3 Multiple submissions

CIPHER - OpenCall 1 will accept a maximum of one application per entity, whether submitted individually or as part of a consortium. In case an entity submits more than one application, only the FIRST submitted application will be considered.

3.2 Types of projects

CIPHER - OpenCall 1 aims to fund applications that assess, validate, or expand CIPHER's capabilities across six open challenges in Knowledge, Testing, Range/ Environment and DevSecOps modes, focusing on NIS2 regulatory compliance, pentesting, vulnerability management, XDR onboarding, risk monitoring, domain cyber-range contributions and platform automation. Applicants are required to select one of the challenges/ topics presented in Table 1 and further detailed in Annex 2 (Technical Requirements).

Table 1: Challenges of CIPHER - OpenCall 1

Challenge Title	Challenge Description	Expected Outcomes
K1: Regulatory capability gap assessment	A certified NIS2 auditor assesses CIPHER's toolset against the Article 21(2) risk-management measures (OT-prioritised sectors), maps where the platform does and does not support each obligation and identifies prioritised gaps that scope next project phases. Documentation only — no active testing. Output is owned by CIPHER.	(a) Map CIPHER capabilities against NIS2 Article 21(2)(a)–(j) and relevant IEC 62443 requirements; (b) identify and severity-rate compliance-coverage gaps; (c) translate gaps into actionable requirement statements for inclusion in the scope of subsequent project phases
K2: Pentest methodology & CIPHER gap assessment	An OT / critical-infrastructure offensive-security expert documents a best-practice identify-and-validate pentest methodology (EU-regulation-aware) and benchmarks CIPHER's T4.3 automated pentesting against it, identifying prioritised technical gaps that scope next project phases. Documentation only — no active testing	(a) Document a repeatable methodology — process, tools, techniques — for the pre-exploitation kill chain through safe validation of exploitable vulnerabilities in OT / critical infrastructure (exploitation confined to a controlled range); (b) benchmark CIPHER's current coverage against it; (c) severity-rate technical gaps and translate them into requirement statements to be included in next project phases; map the

	against CIPHER. Output is owned by CIPHER.	methodology to NIS2 Article 21(2)(e)/(f) and IEC 62443-3-3 / 4-2.
T1: Vulnerability management validation	A vulnerability-management practitioner exercises CIPHER's existing VM toolchain end-to-end across three views (SBOM, endpoint, network/host), pushes conformant scan proofs to project storage, validates the ingestion pipeline through to DefectDojo, and reports performance and integration friction. Active scanning runs only in the cyber range. Output is owned by CIPHER.	(a) Run the CIPHER baseline toolset against range targets across all three views; (b) push each scan as a reproducible bundle to WORM storage; (c) verify pipeline pickup from storage → Dependency-Track (SBOM) → DefectDojo aggregation and deduplication; (d) measure pipeline performance and surface integration friction; (e) map findings to NIS2 Article 21(2)(f) and CRA vulnerability-handling / SBOM obligations.
T2: CIPHER XDR onboarding & data-collection validation	A detection / SOC practitioner onboards their environment to CIPHER XDR (Wazuh-based, CIPHER-hosted SaaS) by deploying the full range of agent types and SIEM inputs (EDR + IDS/IPS + OT security appliances), exercises the platform's data-collection and detection capabilities, and reports coverage, fidelity and integration friction. Output is owned by CIPHER. The activity validates whether CIPHER can ingest high-volume cybersecurity events, combine them with infrastructure- and application-level monitoring data, suppress low-impact alerts and generate higher-level risk alerts across organisational, network or geographical domains.	(a) Deploy agents across diverse host / OS types reporting to the CIPHER XDR SaaS; (b) integrate SIEM inputs from IDS/IPS and OT appliances; (c) exercise the full breadth of agent capabilities (FIM, SCA, inventory, log collection, vulnerability detection, rootcheck, active response) and collect security-event facts; (d) validate detection against known scenarios (range); (e) map to NIS2 Article 21(2)(b) incident handling and (f) effectiveness, and CRA monitoring / reporting obligations; (g) assess performance, integration effort, applicability across critical sectors and opportunities for extending CIPHER with applicant-provided risk-analysis capabilities.
R1: Domain cyber-range contribution	Invite partners to contribute a cyber-range / sector-emulation solution (open-source preferred) that enables NIS2 readiness assessment for a real operational domain, deployed into or federated with CIPHER so the consortium can run comparable assessments across	(a) Deploy / federate the range with CIPHER; (b) provide domain-realistic scenarios that assess NIS2 readiness (not CTF / training-only); (c) map scenarios and measurements to NIS2 Article 21(2) measures so readiness is assessable;

	competing solutions and produce evidence-based recommendations. Generic capture-the-flag ranges are out of scope — readiness value, not training alone.	(d) enable comparable evaluation against other CIPHER range environments to support consortium recommendations.
P1: DevSecOps & platform automation	Partners deliver DevSecOps automation for technologies on a CIPHER-provided list that lack proper automation — e.g. porting a monolithic, Docker-Compose-only tool such as MISP to a maintainable Helm chart, or authoring IaC and CI/CD where none exists. Applicants select from the list; CIPHER defines what needs doing. Work lands in CIPHER repositories under review; execution against a non-production environment. Reusable output, OSS-preferred, licensed to CIPHER.	(a) Codify deployment of a CIPHER-listed technology as idempotent, version-controlled IaC and/or a maintainable Helm chart; (b) build a CI/CD pipeline for build → test → deploy; (c) generate an SBOM, scan artifacts, and record a risk-management decision (accept / mitigate / compensate control) for findings in components CIPHER does not own — visibility and documented decision, not upstream remediation; (d) make the deployment portable / reproducible across ≥2 target environments (supporting proof-recreation independent of any single platform); (e) map pipeline supply-chain controls and risk decisions to NIS2 Article 21(2)(d)/(e) and CRA secure-development / SBOM obligations.

CIPHER - OpenCall 1 will look to ensure a balanced distribution of applications among challenges. Specific rules are defined in Section 4.

3.3 Funding conditions

Any entity, applying individually or as part of a consortium, will only be considered for funding once.

Each application may receive a maximum of up to €60,000. The total amount requested must represent 50% of the project costs (including indirect costs), with the remaining 50% as co-financing. All applications will be required to provide a justification of the planned costs and resources of the project. This will be explicitly evaluated under the "Quality of implementation and operational capacity" criterion, which directly assesses the total eligible costs presented and justified in the submitted proposal, compliance with the project's objectives and the expected impact of the proposed activities and finally the scope, scale, and maturity of the activities to be implemented.

Funding is foreseen to support the following categories of costs:

- Personnel costs (direct costs);
- Equipment costs (direct costs);
- Travel costs (direct costs);
- Other goods, work and services (licenses costs; Communication, promotion, and exploitation; Services for meetings, seminars, workshops; etc) (direct costs)
- Indirect costs - 7% of direct costs.

The type of costs that may be reported include human resources, equipment, other direct costs, and indirect costs (7% of personnel and other direct costs). Subcontracting is not eligible for this open call. Summary of funding rules:

- Cumulative Ceiling: No single legal entity may receive more than €60.000 in total FSTP funding across the lifetime of the CIPHER project. This includes:
 - Co-Funding Rate: The grant represents a maximum of 50% of total eligible project costs.
 - Cost Categories & Flat Rate: Eligible costs include Personnel, Travel, Equipment, and Other Direct Costs. Indirect costs are calculated as a flat rate of 7% of total direct eligible costs (personnel and other direct costs).
- Ineligible Costs: Subcontracting is strictly ineligible under this Open Call.
- Disbursement: Grants are paid as a Lump-sum upon completion of three milestones (20%, 40%, 40%) upon approval of Sprint1, Sprint 2 and Sprint 3 deliverables. First payment is planned to be paid at M1 followed by the onboarding report which is considered as pre-financing support.

During the programme funds will be disbursed in lump sums at the end of each Sprint and pending the achievement of agreed milestones and deliverables.

3.4 Application process

The F6S platform will be the single-entry point for all applications to CIPHER - OpenCall 1. Interested applicants should register at the CIPHER F6S page (www.f6s.com/cipher-opencall1). The relevant links and timings for the application process are provided in Table 2 but are subject to change (Table 2).

Table 2: Application Process and Timeline

Phase	Description	Timeline
Application	Fill in and submit application including: ● Application form on F6S [link]. ● Proposal Supplement [link]	Launch date: 26/10/2026 Submission deadline: 06/01/2027 (17h00 CET)
Eligibility & Technical check	CIPHER Consortium performs internal checks of the eligibility criteria of the applications	13/01/2027 to 23/01/2027
Application evaluation	An evaluation board reviews the received applications, scoring them based on the evaluation criteria. The evaluators rank the applications and select the top-ranked projects in online interviews.	24/01/2027 to 13/02/2027
Announcement of the results	All applicants receive a written letter about approval or rejection of their project. The successful projects start the onboarding phase in the CIPHER Programme.	17/03/2027

The submission date for applications is final. All other dates, including those of the programme, may be subject to change.

Application Documentation Package

To apply for the CIPHER Open Call 1, applicants must complete and submit a defined documentation package via the single-entry F6S platform (www.f6s.com/cipher-opencall1) prior to the call deadline. The documentation package is divided into documents required at proposal submission and administrative documents required from selected beneficiaries during the contracting phase.

Table 3: 3.4.1.1 References and templates provided by CIPHER

Annex 1 (current document): Guide for Applicants	Reference PDF	Comprehensive guideline on how to apply, call requirements (general, financial and technical), important dates, scope and limitations, programme details, evaluation process.
Annex 2: Technical Requirements	Reference PDF	Comprehensive call specifications detailing the open challenges, technical touchpoints, KPIs, and scope boundaries.
Ownership and Control Assessment (OCA) Procedure	Reference PDF	Reference

All applicants must complete and submit the following documents during the open submission window:

Table 4: Submission Phase Documents (Mandatory at Proposal Submission)

Document Name	File Format	Mandatory / Optional	Description
Application Form (F6S / EC Portal Template)	Online Form	Mandatory	Administrative and legal identification questions completed directly on the F6S submission portal.
Annex 3: Technical Proposal Template	Word Document	Mandatory	Technical proposal template (12 pages maximum for Sections 1–5, excluding cover, summary, and Section 6 Ethics/Security Annex) detailing alignment, excellence, impact, work plan, team, and budget rationale.
CIPHER FSTP Budget Template	XLSX	Mandatory	Excel workbook detailing cost categories, person-months, purchase expenses, requested grant, and co-financing
Annex 4: Ownership Control Declaration (OCD)	Word Document (QES signed)	Mandatory (<i>Exempt for validated public bodies</i>)	Declaration enforcing EU strategic security restrictions under Digital Europe Regulation. Must be signed via Qualified Electronic Signature (QES) by each applicant entity (and consortium partner).

Applicants selected for funding will be invited to the contracting phase and required to provide signed administrative and legal documentation prior to grant agreement execution:

Table 5: Contracting Phase Documents (Selected Beneficiaries Only)

Document Name	File Format	Requirement	Description
Annex 5: Sub-Grant Agreement (SGA)	Word (e-signed)	Mandatory	Formal tri-party sub-grant contract executed between the Lead Beneficiary, CIPHER Coordinator (EVIDEN), and Treasurer (F6S)
Annex 6: Declaration of Honour (Non-Individuals)	Word (e-signed)	Mandatory	Legal declaration confirming non-exclusion, absence of double funding, and availability of operational capacity.
Annex 7: Consortium Declaration of Honour	Word (e-signed)	Mandatory for Consortia	Declaration signed by all consortium partners designating the Lead Beneficiary, defining roles, and agreeing on budget shares.
Annex 8: SME Declaration Form	Word (e-signed)	Mandatory for SMEs	Self-assessment form establishing SME qualification (autonomous, partner, or linked) under Commission Recommendation 2003/361/EC.
Annex 9: Bank Account Information Form	PDF (e-signed)	Mandatory	Official bank details form accompanied by a recent bank statement (< 2 months) or bank stamp.
Administrative Proofs & KYC	PDF / Scans	Mandatory	Official proof of legal existence (commercial register extract, VAT proof), EC Participant Register PIC validation, and Know Your Customer (KYC) proof of ID and residence for legal representatives.

Guidance on the CIPHER FSTP Budget Template

All applicants are required to complete and upload the **CIPHER FSTP Budget Template** alongside their Technical Proposal. This template structures the project budget, ensures compliance with financial ceilings, and automates co-financing calculations.

Workbook Overview & Sheet Structure

The budget workbook contains five pre-formatted sheets:

- **Instructions Sheet:** Outlines editable light-yellow cells, locked calculation formulas, currency rules (EUR), and partner setup guidelines.
- **Consortium Summary Sheet:** Consolidated master sheet that automatically aggregates totals across all partners, validates budget ceilings, and displays automated verification flags.
- **Partner 1, Partner 2, Partner 3 Sheets:** Individual partner breakdown sheets. Single applicants complete **Partner 1** only; consortia complete one sheet per partner (up to 3 partners).

Key Financial Rules & Conditions

- **Maximum Grant Ceiling:** The maximum CIPHER grant awarded per application is **€60,000**.
- **50% Co-Funding Rate:** The requested grant represents exactly **50% of total eligible project costs**. The remaining 50% must be co-financed by the applicant(s).

3.5 Other application requirements and considerations

- Submission: Applications must be submitted via www.f6s.com/cipher-opencall1. Any other submission method will not be accepted.
- Complete application: All mandatory questions must be answered, and all requested documents must be uploaded. Incomplete applications will be disqualified. A technical proposal that exceeds the maximum page limit may result in the disqualification of the proposal or of the specific section under evaluation
- Accept terms: Applicants must agree to the application's terms and conditions.
- English language: All applications and programme communication must be in English.
- Document format: Unless otherwise agreed, all documents in all phases must be submitted electronically in PDF format without printing restrictions.
- Document naming: All required documents, including the technical proposal (if applicable), should include the project acronym. Documents must not include any special characters (e.g. #!+<>^|*) as these may make it unreadable/ corrupt. In such cases, the application may be disqualified, and resubmission will not be accepted after the call closure.
- Deadline:
 - Failure to submit the application by the submission deadline, regardless of cause (e.g., network issues, multiple browsers or windows), is not acceptable as an extenuating circumstance. It is recommended to apply well before the deadline.
 - Resubmissions are possible provided the call deadline has not passed but are only guaranteed if requested at least 2 business days before the deadline via support@f6s.com.
 - The deadline may be extended only in case of unforeseen F6S platform technical issues. All applicants will be notified of the new deadline.
- Review future documents: Applicants are encouraged to get familiar with the documents that will be required in the contracting phase (see Section 5 - Contracting Phase)
- Notifications: Applicants are encouraged to enable F6S notifications and notifications by email for the programme in their profile settings to ensure communications regarding their application are received.
- Applicants list: A full list of applicants containing their basic information will be created for statistical and transparency purposes and shared with the European Commission.
- Binding information: In the unlikely occurrence of a contradiction between the information provided via the OC channels (e-mail, webinars or other means) and the information included in this Annex (Guide for Applicants), the latter is binding.

3.6 Technical/ feasibility assessment

Before proposals are passed to the independent external experts for scoring, a Technical Eligibility Check will be conducted by the CIPHER Technical Committee. This stage operates as a binary In/Out filter based on Section 4.2 parameters

3.7 Cut-offs or Open Call closure

Submission Deadline: The call will close strictly on 06/01/2027 at 17:00 CET/CEST (Brussels time).

Single-Stage Finality: There are no rolling selection cut-offs. All applications must be fully finalized and submitted through the F6S platform prior to this single closing date to be considered for evaluation.

Late Submissions: In strict compliance with the project's regulatory requirements, the F6S platform will automatically block updates and entries after the deadline; no late submissions via email or other alternative channels will be accepted.

4 How will applications be evaluated and selected?

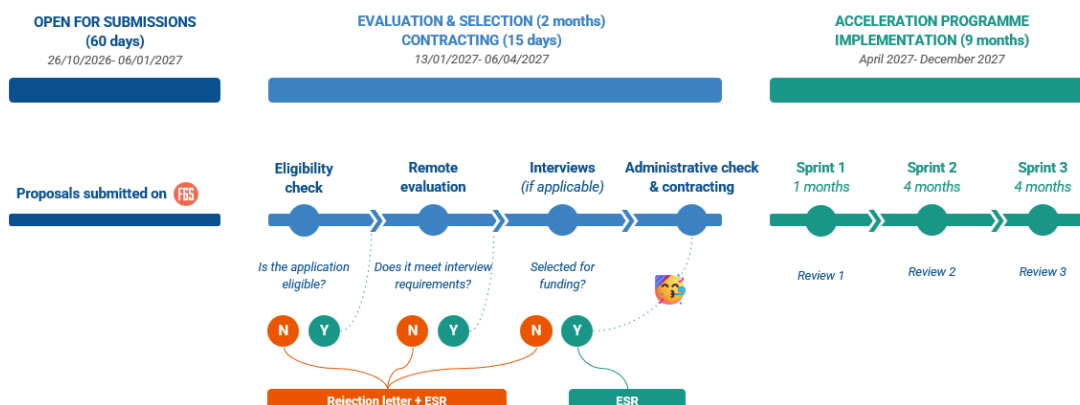


Figure 1: Evaluation and selection process

CIPHER reserves the right to request at any moment of the process additional information and/or documentation to clarify any doubts regarding the eligibility of the applicant(s) and/or the application.

4.1 Eligibility check

An initial eligibility verification will be performed to filter out and discard non-eligible applications. An application is only considered eligible if it meets all the eligibility criteria and requirements listed in Section 3, related with: type of applicant(s), consortium, countries, funding, and language.

The eligibility check enables the establishment of a shortlist of applications to be evaluated in the next step of the evaluation process. Applications marked as non-eligible (for not meeting one or more of the eligibility criteria) will receive a rejection letter with justification.

4.2 In/out challenge and ecosystem scope check

The in/out challenge and ecosystem scope check will be done to evaluate and discard applications that are not aligned and do not meet the baseline challenge and ecosystem requirements. The check will be carried out by CIPHER consortium partners.

An application is only considered within the challenge and ecosystem scope if the description, provided in the relevant section of the technical proposal and submitted with the application, clearly addresses and aligns with all baseline challenge and ecosystem requirements. Note that the full proposal will not be evaluated, even if it contains complementary information.

The challenge and ecosystem scope check will evaluate:

- **Challenge K1 (Regulatory Capability Gap Assessment):** Applicants should ensure their core team includes a certified auditor (e.g., ISO/IEC 27001 Lead Auditor or IEC 62443 Assessor) with a documented track record in NIS2 Annex I/II critical sectors or Operational Technology (OT) environments, as applications without verifiable compliance experience in these areas will not meet the baseline scope.
- **Challenge K2 (Pentest Methodology & Project Gap Assessment):** Applicants are expected to demonstrate practical offensive security experience in Industrial Control Systems (ICS/OT)

backed by relevant certifications (e.g., GICSP or OSCP), as proposals lacking proven critical infrastructure pentesting credentials will fall outside the challenge requirements.

- Challenge T1 (Vulnerability Management Validation): Proposals should commit to executing all active vulnerability scanning strictly within CIPHER's isolated cyber range using OT-safe scan profiles and emitting scan proofs as S3 WORM bundles in DefectDojo-parseable formats to fulfil essential technical boundaries.
- Challenge T2 (CIPHER XDR Onboarding & Data-Collection Validation): Applicants must directly control a representative environment—comprising diverse OS types and active IDS/IPS or OT security appliances—capable of securely forwarding telemetry to CIPHER's XDR SaaS using strict data-minimization controls.
- Challenge R1 (Domain Cyber-Range Contribution): Applicants need to provide an operational, sector-emulation cyber range that generates quantifiable NIS2 Article 21(2) readiness assessment metrics—excluding pure Capture-The-Flag (CTF) or training-only platforms—along with the legal capacity to grant CIPHER sustainable deployment and operational licensing rights.
- Challenge P1 (DevSecOps & Platform Automation): Proposals require demonstrated engineering experience in Infrastructure as Code (Terraform/OpenTofu/Ansible), Helm packaging, and CI/CD automation, with a commitment to contributing all deliverables directly to CIPHER repositories via Pull Requests for non-production validation.

The check will establish the final list of applications that proceed to the expert evaluation stage. All applicants that are evaluated as out of scope will receive a rejection letter with justification.

4.3 Expert evaluation

The expert evaluation board is a collective body composed of individual members with relevant experience in the CIPHER domains, having signed and duly agreed in advance a written commitment of confidentiality and absence of any conflicts of interest that might influence the impartial and objective analysis and evaluation of all submitted proposals.

4.3.1 Evaluation criteria & scoring

Each application will be reviewed by a minimum of two experts from the expert evaluation board. Applications will be scored from 0 to 10 by *independent* experts, with final scores rounded according to the approved call guidelines and will be scored against the following criteria:

Table 6: Scoring Criteria

Criteria Name	Description
Excellence (weight: 30%)	Assessment of the overall technical quality and methodology of the proposed solution or testing activity across Knowledge (K1, K2), Testing (T1, T2), Range/Environment (R1), or Platform/Enablement (P1) challenges
Sub-criterion 1.1	1.1 Technical Concept & Objectives: Clarity, precision, and feasibility of the proposed technical objectives and minimum deliverables mapped to the selected challenge scope (e.g., gap assessment, VM pipeline, XDR & Risk Monitoring telemetry, domain range, or DevSecOps automation).
Sub-criterion 1.2	1.2 Soundness & Methodology: Quality and rigor of the methodology, testing frameworks, and tools used (e.g., NIS2/IEC 62443 audit frameworks, EU-regulation-aware pentest kill-chains, OT-safe scan profiles, custom risk-analysis tools, or DevSecOps/IaC automation pipelines)

Sub-criterion 1.3	1.3 Testing & Execution Scenarios: Feasibility, realism, and rigor of proposed threat, risk, or validation scenarios (e.g., executing at least 2 distinct threat/analysis cycles, multi-site/multi-system data correlation, NIS2 readiness domain scenarios, or reproducible clean-environment deployment tests).
Relevance to the objectives of CIPHER project (weight: 30%)	Evaluation of alignment with CIPHER core capabilities (automated pentesting, XDR SaaS, Risk Monitoring Bundle, WORM storage, NBI, DevSecOps automation) and targeted critical infrastructure sectors
Sub-criterion 2.1	2.1 Component Integration: Technical feasibility and seamlessness of integrating third-party tools/feeds with CIPHER touchpoints (S3 WORM, Dependency-Track, DefectDojo, Wazuh manager, NBI, Federated Risk Monitoring Agents, or Git/CI-CD repositories and Secret Store)
Sub-criterion 2.2	2.2 Pilot & Sector Value Added: Tangible domain applicability and value delivered to NIS2 Annex I/II critical sectors (with explicit prioritization for OT, energy, healthcare, telco, and industrial infrastructure).
Sub-criterion 2.3	2.3 Technical Maturity & Data Readiness: Maturity of the applicant's environment/product (TRL 6–8) and readiness to deploy agents, host isolated K8s capacity, or feed representative/synthetic event sources and telemetry.
Impact and scalability (weight: 20%)	Potential of the solution to scale across critical infrastructure sectors, contribute to EU cybersecurity resilience, and ensure post-project sustainability.
Sub-criterion 3.1	3.1 EU Cybersecurity Resilience: Direct contribution to European digital supply chain security, EU-native intelligence sharing, and compliance with NIS2 Article 21(2), Article 12, and CRA obligations
Sub-criterion 3.2	3.2 Scalability & Cross-Sector Benefit: Potential for methodologies, scan proofs, contributed domain ranges, or automation blueprints to scale across multiple administrative domains, geographic sites, and critical sectors.
Sub-criterion 3.3	3.3 Exploitation, Licensing & Sustainability: Alignment with IP/licensing terms (CIPHER ownership for challenge outputs; applicant IP retention; or grant of sustainable deployment/extension licenses for contributed ranges (R1) and DevSecOps tooling (P1), with open-source preference).
Quality of implementation and operational capacity (weight: 20%)	Evaluation of the work plan, risk management, applicant track record, and objective budget breakdown.
Sub-criterion 4.1	4.1 Coherence of Work Plan: Clarity and quality of the execution timeline, milestone structure, KPI delivery targets, failure recovery demonstrations, and technical risk management.
Sub-criterion 4.2	4.2 Budget Justification & Compliance: Objective rationale and detailed cost breakdown ensuring total project budget complies with financial ceilings (e.g., max grant ceiling per third party; indirect costs capped at 7% of Direct Costs / Other Direct Costs).

Sub-criterion 4.3

4.3 Operational Capacity & Team Credentials: Demonstrated qualifications, certifications, and operational track record of key personnel matching the required target profiles (e.g., ISO 27001 Lead Auditor, GICSP/OSCP pentester, SOC/detection engineer, or DevSecOps/Platform lead).

Table 7 (item 'Score, Expert') defines how individual criteria will be scored on a scale from 0 to 5. The minimum threshold for each individual criterion will be 3 (three) out of 5 (five), while the overall score threshold will be 10 (ten) out of 15 (fifteen). Applications that do not meet the minimum thresholds (per criterion or overall score) will be excluded from the programme.

After the individual scoring by the expert evaluation board, the Open Call Management Team [F6S, EVIDEN, I2CAT, ICCS, K3Y, EXZ] will:

- Check for large differences (over 2 points per criterion) between evaluators.
- If differences exist, evaluators meet to discuss and agree on scores.
- If an agreement isn't reached, another expert may be invited to provide a third assessment.

4.3.2 Ranking & selection

All applications will be ranked in a single list based on their overall score, which is calculated from the average scores given by the evaluators. If multiple applications have the same overall score, the following tie-breaking criteria will be applied in this order:

1. Excellence
2. Relevance to the objectives of the CIPHER project
3. Impact and scalability
4. Quality of implementation and operational capacity

Final ranking of applications:

- Evaluators discuss and agree on the scores.
- Projects are ranked by their overall score.
- Ties are broken by prioritising scores in Criterion 1, then 2, then 3 and then 4.

All applicants at all stages of the evaluation will be informed about the result of their evaluation along with an Evaluation Summary Report (ESR).

CIPHER expects 25 applications in total with specific applicant thresholds established for each challenge. Selection will be capped within the defined target ranges to maintain optimal capacity and resource allocation per challenge.

Table 7: Target Applicants per Challenge

Challenge Code & Name	Target (Min–Max)	Applicants
K1: Regulatory capability gap assessment (NIS2 auditor profile)	1 – 3	
K2: Pentest methodology & T4.3 gap assessment (offensive / OT profile)	3 – 5	
T1: Vulnerability management validation	8 – 10	
T2: CIPHER XDR onboarding & data-collection validation	8 – 10	

R1: Domain cyber-range contribution	1 – 2
P1: DevSecOps & platform automation	4 - 5

4.4 Appeals

Within three (3) working days of receiving (1) a rejection letter informing the application as non-eligible or (2) an ESR of non-acceptance, an applicant may submit a request for an appeal if they believe the results of the eligibility checks have not been correctly applied, or if they feel that there has been a shortcoming in the way their application has been evaluated.

All requests for appeal must be sent to F6S at info@cipher-eu.com and must:

- Focus on aspects concerning the evaluation of the application (e.g. admissibility or eligibility checks, evaluation procedure, etc), not their merits.
- Clearly describe the complaint.
- Be received within the time limit (3 working days) from the reception of a rejection letter considering the application as non-eligible or the ESR information letter delivered.
- Sent by the entities' legal representative that has also submitted the application.

Note that the evaluation is carried out by highly qualified experts. CIPHER will neither question nor interfere with their original evaluation. Mere repetitions of the content of the application or disagreements with the result or reasoning of the technical evaluation will not be considered.

5 What happens after selection?

Selected applicants will be invited to the contracting phase, where administrative and financial details and documents are verified and validated.

Furthermore, to carry out mandatory Know Your Customer (KYC) checks, proof of residency and proof of ID from one or more members of the organisation(s) is required.

The steps of this phase are listed below (also see Table 7 for complementary information):

1. Inclusion of comments (if any) provided in the Evaluation Summary Report as part of the sub-grant agreement (contract).
2. Validation of the entities based on the provision of the following documentation (for selected winning entities prior to grant agreement signature):
 - Formal proof of the entity's legal existence and tax activity and declaration of ownership.
 - [If applicable] Proof of the SME status, including the SME Declaration Form.
 - Declaration of Honour, for all participating entities, signed by the legal representative of the entity.
 - [If applicable] Consortium Declaration of Honour, signed by the legal representative of each consortium partner.
 - Bank Account Information.
3. Signing of the sub-grant agreement between CIPHER Consortium represented by its Coordinator (EVIDEN), the Treasurer (F6S) and the Lead Beneficiary.

Additional considerations:

- A valid VAT number is mandatory.
- PIC number is mandatory. Please see [here](#).
- The sub-grant agreement (contract) is final and cannot be altered.
- Electronic digital signatures are required for signed documents (unless otherwise agreed).
- Deadlines for document submission will be provided and will normally be concluded within two weeks.
- Failure to complete the negotiation in time will result in rejection.

6 What is CIPHER - OC1 and what are its requirements?

6.1 Programme Sprints

Selected third parties will participate in a 9-month programme structured across 3 consecutive Sprints. Participation and grant disbursement are strictly linked to achieving defined technical outputs and submitting milestone reports.

1. Sprint 1: Onboarding & Testing Framework (Months M0–M1 | Duration: 1 Month)
2. Sprint 2: Standalone Tool Development & Integration (Months M2–M5 | Duration: 4 Months)
3. Sprint 3: Production Testing, Refinement & Pilot Validation (Months M6–M9 | Duration: 4 Months)

6.1.1 Sprint 1: Onboarding and Pre-financing (Months M0–M1 | Duration: 1 Month)

- Objectives: Formally onboard the sub-grantee, establish execution agreements (NDA/DPA), set up isolated test environments or access credentials, and define technical execution architectures. The initial 20% release is triggered by completion of Sprint 1 (architecture definition, data-minimization rules, and deliverable framework setup).
- Activities: Receive scoped credentials, API keys, or SaaS tenant access from CIPHER; agree upon specific testing/gap-assessment scenarios, target assets, sector focus (OT-prioritized), and target KPIs; set up local compute, lab environments, or agent deployment infrastructure.
- Deliverable: *Deliverable 1: Onboarding & Architecture Definition Report* (including agreed architecture, scenario descriptions, target KPIs, data-handling plan, and failure recovery framework) due at the end of M1.
- Funding Released: 20% (€12,000).

6.1.2 Sprint 2: Technical Execution, Pipeline Integration & Initial Testing (Months M2–M5 | Duration: 4 Months)

- Objectives: Execute primary technical tasks according to challenge mode, conducting desk audits/gap assessments (Knowledge), running pipeline/XDR/Risk-Bundle integrations and range tests (Testing), or standing up/federating range and DevSecOps frameworks (Range/Enablement).
- Activities:
 - *Knowledge (K1/K2)*: Review CIPHER toolset/ architecture documentation, map capabilities against NIS2 Article 21(2) / IEC 62443 requirements, and benchmark technical kill-chain coverage.
 - *OR Testing (T1/T2)*: Deploy agents/connectors, push scan bundles across SBOM/endpoint/network views to S3 WORM storage, ingest telemetry into Dependency-Track/DefectDojo/XDR SaaS, or deploy Federated Risk Monitoring Agents and Northbound Security Interfaces.
 - *OR Range/Enablement (R1/P1)*: Deploy/federate domain cyber-range scenarios or build IaC/Helm/CI-CD pipelines for CIPHER-listed technologies.

- Participate in monthly CIPHER technical syncs and measure preliminary KPIs (latency, ingestion success, gap severity, coverage).
- Deliverable: *Deliverable 2: Mid-term Technical Execution & Integration Report* (detailing initial gap analyses, pipeline performance, integration friction, telemetry fidelity, and preliminary KPI metrics) due at the end of M5.
- *Funding Released: 40% (€24,000) (Cumulative: €36,000).*

6.1.3 Sprint 3: Full Validation, Refinement, Demonstration & Final Reporting (Months M6–M9 | Duration: 4 Months)

- Objectives: Complete end-to-end validation, execute failure recovery tests, finalize severity-rated requirement recommendations or integration artifacts, and present final results.
- Activities: Execute complex threat/risk scenarios (minimum 2 distinct cycles) or cross-domain correlation runs; demonstrate system failure recovery (e.g., storage bundle replay or agent re-buffering); map final technical outputs to NIS2 Article 21(2), Article 12, or CRA obligations; translate findings into scopeable next phase of project. Requirement statements or reusable pull requests in CIPHER repositories; participate in the official CIPHER Demo Day / Final Review.
- Deliverable: *Deliverable 3: Final Validation, Regulatory Mapping & Exploitation Report* (including full KPI results, severity-rated gap analyses and requirements for next phase of project, reproducible configuration packages, regulatory mapping, and live demo presentation) due at the end of M9.
- *Funding Released: 40% (€24,000) (Cumulative: €60,000).*

6.2 Programme review

6.2.1 Review summary

Each project will go through at least 2 reviews, each one highlighting the end of a phase/ stage/ sprint.

Table 8: Sprint Requirements

Stage	Item	Description
Sprint 1	Requirement	Onboarding Phase completion & submission of Deliverable 1 (Onboarding & Architecture Definition Report)
	Result	Payment of 20% of the grant.
	Timeline	End of Month 1
Sprint 2	Requirement	- Submission & Approval of Deliverable 2 (Mid-term Technical Execution & Integration Report) - Deliverable 2 must include the following: • Mid-term technical progress, tool integration, and architectural alignment • Initial gap assessments (K1/K2) or pipeline/telemetry integration results (T1/T2/R1/P1)

Sprint 3		• Preliminary KPI measurement data (latency, ingestion success, false-positive rates, telemetry fidelity, integration friction) • Summary of participation in monthly CIPHER technical syncs
	Result	Payment of 40% of the grant.
	Timeline	End of Month 5
	Requirement	- Submission & Approval of Deliverable 3 (Final Validation, Regulatory Mapping & Exploitation Report) + Live Demo Day presentation - Deliverable 3 must include the following: • Full end-to-end testing results, scenario execution evidence (minimum 2 distinct threat/risk cycles), and system failure recovery proof (e.g., storage replay or agent re-buffering) • Complete KPI evaluation metrics against baseline targets • Severity-rated gap analyses and actionability mapping of requirement for next phase of project. Statements (Knowledge mode) • Traceability mapping to NIS2 (Article 21(2), Article 12) and CRA regulatory obligations • Reusable code, IaC, Helm charts, connectors, or configuration packages contributed to CIPHER repositories via PR (where applicable) • Commercial exploitation plan, open-source sustainability roadmap, and live demonstration deck
	Result	Payment of 40% of the grant.
	Timeline	End of Month 9

Reports must be submitted at least one week in advance, so that the reviewers will have enough time to prepare. During the review, representatives of the beneficiary should present their work and answer questions.

After each successful review and within 5 working days, the beneficiary should send the relevant payment request document.

If at any of the project stages the quality of work demonstrated and/or reported does not correspond to what has been agreed, the CIPHER Coordinator may agree to a resubmission of a report and respective reassessment. If significant improvements are not delivered after the reassessment, the sub-project is therefore considered to be in breach of their contractual obligations.

7 What else is important to know?

7.1 Intellectual Property Rights (IPR)

Unless otherwise specified in the challenge description, all outputs, results, deliverables and developments generated under the funded challenges shall be owned by CIPHER. Applicants retain ownership of all pre-existing intellectual property, know-how, tools and assets brought into the project (background IP).

An exception applies to Challenge R1, where any cyber range infrastructure contributed by an applicant shall remain the property of the contributing applicant. In such cases, the applicant shall grant CIPHER the rights and licences necessary for the implementation, operation and exploitation of the challenge outcomes, as detailed in the applicable grant and licensing arrangements.

As a general rule, all active testing, validation and operational cyber-security techniques shall be executed exclusively within the CIPHER cyber range environment. Only where expressly defined in a specific challenge description may activities be carried out within an applicant-controlled environment, in which case the applicable access, security, ownership and usage conditions shall be governed by the provisions of that challenge. Regarding the evaluation and the review processes, each evaluator will sign an Agreement including confidentiality clauses before receiving access to the applications database to protect the applicants' intellectual property and sensitive non-disclosed information.

7.2 Conflicts of interest

Applicants must not have any actual and/or potential conflict of interest with the CIPHER selection process and during the project implementation. All identified or potential conflicts of interest will be assessed on a case-by-case basis.

7.3 Ethical issues

CIPHER complies with the fundamental ethical issues particularly those outlined in the “European Code of Conduct for Research Integrity”.

- All applicants must submit a self-assessment ethics questionnaire, available in the Proposal Template
- If the applicant confirms the existence of potential ethical issues, they must contact the CIPHER Helpdesk for guidance, as required.
- CIPHER will verify the declaration's consistency with the application contents and may contact applicants to resolve any ethical issues.
- Applications that fail to properly address ethical issues or inadequately deal with privacy aspects will be rejected.

7.4 Data protection

In order to process and evaluate applications, and manage project implementation, the CIPHER consortium will need to collect Personal and Industrial Data.

- F6S Network Ireland Limited will act as Data Controller for data submitted through the F6S platform for these purposes. Please see our privacy policy [here](#).
- A Data Protection Officer (DPO) has been appointed by F6S generally, to ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), and that personal data is collected, processed, and stored in a secure manner.
- The F6S platform's system design and operational procedures ensure that data is managed in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR).
- Each applicant will accept the F6S terms to ensure compliance. Please refer to <https://www.f6s.com/privacy-policy> to review the F6S platform's privacy and data security policy.
- Apart from the F6S platform, data will also be stored in the F6S Google Drive, and in the project repository on Teams managed by the project coordinator, EVIDEN.
- Note that the CIPHER consortium must retain generated data until five years after the balance of the CIPHER project is paid or longer if there are ongoing procedures (such as audits, investigations or litigation). In this case, the data must be kept until their conclusion.

7.5 Confidentiality

Confidentiality obligations:

- Selected applicants are required to maintain confidential any project data, documents, invoices and other materials (in any form) during the implementation of the activities and for 5 years after project completion.
- This confidentiality period can be extended by agreement with the EC and the CIPHER consortium.
- Participant's project related information shared during the project, whether written or spoken, is only considered confidential if CIPHER agrees and confirms it in writing within 15 days.
- Confidential information must only be used for project implementation, unless otherwise agreed upon.
- Any information shared during the application stage will be treated as confidential.

7.6 Promotion of the action and ensuring visibility of the EU funding

The beneficiary must promote their funded project, the CIPHER project and its results, by providing targeted information to multiple audiences (including the media and the public) in a strategic and effective manner and to highlight the financial support of the EC, including on the official third-party website. The CIPHER Communication team will guide and support these communication activities for selected beneficiaries.

7.7 Checks and reviews

The EC may, at any time during the implementation of the sub-project and up to five years after the end of the sub-project, arrange for a check and review activity to be carried out, by external auditors, or by the EC services themselves, including the European Anti-Fraud office (OLAF). The procedure shall be deemed to be initiated on the date of receipt of the relevant letter sent by the EC. The European Commission, OLAF, and the European Court of Auditors retain the right to audit, investigate, and verify the use of funds by third-party beneficiaries both during project implementation and after its completion. Beneficiaries must cooperate fully and provide all required information,

records, and documentation. Failure to comply may result in the suspension, reduction, or recovery of funding.

There will be no financial checks, reviews, or audits to check costs, since beneficiaries have no obligation to document the costs incurred for the action. Checks, reviews, and audits will focus on the technical implementation of the action.

Beneficiaries will be required to submit periodic technical and financial reports, and payments will be disbursed based on the achievement of milestones or deliverables. The Coordinator reserves the right to suspend, recover, or reduce funding in cases of mismanagement, irregularities, or breach of obligations.

7.8 Relevant links and contacts

The CIPHER Consortium will provide information to the applicants via the F6S page, so that all communication (questions and answers) is visible to all participants.

- Open call publication: <https://cipher-eu.com/open-call-1/#>
- Project website: <https://cipher-eu.com/>
- Open call application form: www.f6s.com/cipher-opencall1
- Contact us: info@cipher-eu.com
- Online Q&A/ discussion board: www.f6s.com/cipher-opencall1/discuss
- F6S platform support team: support@f6s.com (*For issues with the submission, resubmission, access to the platform, etc.*)

8 Relevant Open Call definitions

Table 9: Acronyms & Definitions

Acronym	Explanation/ Definition
AWU	Annual Work Unit
EC	European Commission
SME	Small and Medium Sized Enterprise
ESR	Evaluation Summary Report
KYC	Know Your Customer

Table 10: Terms & Definitions

Term	Definition
Applicant(s)	The legal entity or group of legal entities that intend(s) to submit or that submitted an application to the Open Call.
Application Eligibility Criteria	Criteria used to assess if an application can be considered for the open call. Possible values (Yes/No).
Application Eligible or Non-Eligible	Application that is or is not compliant with eligibility criteria.
Application Timestamp	Timestamp of the final submission of an application. If the application is reopened and resubmitted the last date will be considered.
Bank Account Information	Document(s) where the beneficiary provides information of the bank account to which payments will be made during the project implementation.
Beneficiary or 3rd Party	An entity or a consortium that submitted an application to the open call that was accepted to be funded, and have signed, or are in the process of signing, a sub-grant agreement.
Consortium	Set of legal entities that are cumulatively responsible to implement the project as defined in the Grant Agreement signed with the European Commission.
Consortium Declaration of Honour	Declaration where the applicants/ beneficiaries, participating as a consortium, declare they accept all conditions of the open call, acceleration process & programme; and agree - if applicable - on budget share. One CDoH is required for each sub-granted project.
Contract Deadline	Date and time until when the selected entities need to provide contractual information.
Declaration of Honour (DoH)	Declaration where the applicant/beneficiary declares they accept all conditions of the open call, acceleration process & programme. One DoH is required for each applicant/ beneficiary.
External Evaluator	Expert hired by the consortium to assist in the evaluation of the Open Call. External evaluators cannot have conflicts of interest and are bound by a confidentiality agreement.
F6S Application Form	Application form available in F6S Platform.

F6S Platform	Platform provided by F6S.
FSTP	Financial support to third parties. Payments made to entities that are not members of the consortium.
FSTP – Lump Sum	Payment made to the third party based on the achievement of a milestone.
Internal evaluation committee	Group of appropriately qualified persons of the consortium partners that are assigned the responsibility of performing evaluations or reviews at any stage of the open call implementation or programme.
Mentor	Person from the consortium that works closely with the beneficiary to foster communication with the consortium and assess progress of the project. The mentor may be part of an evaluation committee.
Open Call	Competitive process to access a Programme.
Open Call and Programme deadlines	The project has planned the programme carefully, but unexpected things can happen. The application deadline is fixed, and will only change if something unforeseen occurs. Other dates, including of the programme, are flexible and may be adjusted as needed, and communicated to all applicants.
Open Call close date	Date and time when applications close.
Open Call selection prioritisation	Rules used to order applications.
Proof of Legal Existence	Company/ organisation register, official journal or other official document per country showing the name of the organisation, the legal address and registration number and a copy of a document proving VAT registration (in case the VAT number does not show on the registration extract or its equivalent).
Proof of SME Status	Proof of the SME condition is required: • If the applicant has been fully validated as an SME on the Beneficiary Register of the EC Participant Portal, the PIC number must be provided. • Provision of the signed (with a valid e-signature) SME Declaration (Annex 8): in the event the beneficiary declares being non-autonomous, the balance sheet and profit and loss account (with annexes) for the last period for upstream and downstream organisations is required. A Status Information Form may be requested, which includes the headcount (AWU), balance, profit & loss accounts of the latest closed financial year and the relation, upstream and downstream, of any linked or partner company. • Supporting documents: In cases where either the number of employees or the ownership is not clearly identified: any other supporting documents which demonstrate headcount and ownership such as payroll details, annual reports, national regional, association records, etc.
Reserve List	Eligible applications that were not selected for funding which can be invited in case selected applications do not provide contractual data.

Schedule for payments to Beneficiaries	All payments to beneficiaries are dependent on the successful review of deliverables/ reports at the end of each Sprint, and reception by the consortium of the corresponding payment request. All payments will be made with undue delay preferably no later than 30 calendar days after the reception of the financial statement.
Score, Expert	Unless otherwise stated, experts will rank each criterion with marks between 0 and 5. Half point scores are not given. Score values will indicate the following assessments: • 0: Fail. The application fails to address the criterion under examination or cannot be judged due to missing or incomplete information. • 1: Very poor. The criterion is addressed in an unsatisfactory manner. • 2: Poor. There are serious inherent weaknesses. • 3: Good. While the application broadly addresses the criterion, there are significant weaknesses that would need correcting. • 4: Very Good. The application addresses the criterion well, although certain improvements are possible. • 5: Excellent. The application successfully addresses all relevant aspects of the criterion in question. Any shortcomings are minor.
Score, Per Committee	When the evaluation is made by a committee, the average score of each criterion is rounded to the nearest point or half point (1, 1.5, 2, ..., 4, 4.5, 5), before computing the overall score. Overall score is the sum of the scores of each criterion multiplied by the respective weight, rounded to the nearest integer value.
Selected application	Application that was selected to participate in the Open Call Implementation.
SME	An incorporated enterprise that complies with the rules defined by the European Commission to be qualified as an SME ¹
SME – Autonomous Enterprise	An autonomous enterprise is not a partner with or linked to another enterprise
SME – Linked Enterprise	Linked enterprises are those that form a group through the direct or indirect control of the majority of voting rights of an enterprise by another or through the ability to exercise a dominant influence on an enterprise.
SME – Partner Enterprise	The enterprise holds a minimum of 25% (Capital or voting rights in another enterprise, or 25% (Capital or voting rights) are owned by another enterprise.
SME Declaration Form	Declaration where the SME status is assessed.
Sub-grant Agreement	Signed between the Project Consortium, represented by its Coordinator and the beneficiary. The sub-grant agreement will also include the comments (if any) of the application's ESR to the work plan.

